

**RTCM 13900.0**

RTCM Paper 2025-SC139-0039-STD



## **RTCM STANDARD 13900.0**

**FOR**

# **Maritime Messaging Service Architecture and Protocol**

DEVELOPED BY  
RTCM SPECIAL COMMITTEE NO. 139

March 05, 2025

COPYRIGHT©2025 RTCM

Radio Technical Commission for Maritime Services  
1150 18<sup>th</sup> Street NW., Suite 910  
Washington, DC 20036 U.S.A.  
E-Mail: [info@rtcm.org](mailto:info@rtcm.org)  
Web Site: <https://www.rtc.org>

*The Radio Technical Commission for Maritime Services (RTCM) is an incorporated non-profit organization, with participation in its work by international representation from both government and non-government organizations. The RTCM does not work to induce sales, it does not test or endorse products, and it does not monitor or enforce the use of its standards.*

*The RTCM does not engage in the design, sale, manufacture or distribution of equipment or in any way control the use of this standard by any manufacturer, service provider, or user. Use of, and adherence to, this standard is entirely within the control and discretion of each manufacturer, service provider, and user.*

*For information on RTCM Documents or on  
participation in development of future RTCM documents contact:*

*Radio Technical Commission for Maritime Services  
1150 18<sup>th</sup> Street NW, Suite 910  
Washington, DC 20036 USA*

*Telephone: +1-703-527-2000*

*Telefax: +1-904-410-2109*

*E-Mail: [info@rtcm.org](mailto:info@rtcm.org)*



**RTCM 13900.0**

RTCM Paper 2025-SC139-0039-STD



## **RTCM STANDARD 13900.0**

**FOR**

# **Maritime Messaging Service Architecture and Protocol**

DEVELOPED BY  
RTCM SPECIAL COMMITTEE NO. 139

March 05, 2025

COPYRIGHT©2025 RTCM

Radio Technical Commission for Maritime Services  
1150 18<sup>th</sup> Street NW., Suite 910  
Washington, DC 20036 U.S.A.  
E-Mail: [info@rtcm.org](mailto:info@rtcm.org)  
Web Site: <https://www.rtcn.org>

This page intentionally left blank

## Maritime Messaging Service Architecture and Protocol

### Table of Contents

Introduction.....	1
1 Scope.....	2
2 Normative References .....	2
3 Terms and Definitions.....	2
3.1 Abbreviations .....	2
3.2 Definitions .....	4
3.2.1 Aid to Navigation .....	4
3.2.2 Broadcast Message .....	4
3.2.3 MRN-addressed Message.....	5
3.2.4 Subject-cast Message .....	5
3.2.5 Anonymity .....	5
3.2.6 Maritime Identity Registry (MIR) .....	5
3.2.7 Maritime Service Registry (MSR).....	5
3.2.8 MCP MRN .....	5
3.2.9 Navigation .....	5
3.2.10 Navigator.....	5
3.2.11 Service .....	5
3.2.12 Service Consumer .....	5
3.2.13 Service Provider .....	5
3.2.14 Technical Service .....	5
3.2.15 Time to Live.....	6
3.2.16 VDE-TER Network .....	6
3.2.17 VDE-SAT Network .....	6
4 General Considerations (Informative) .....	6
4.1 Motivation .....	6
4.2 The Maritime Connectivity Platform.....	7
4.3 The Maritime Messaging Service .....	7
4.4 Compliance with IMO requirements.....	7
4.4.1 Support of MSC.1/Circ.1595 .....	8
5 System Architecture (Informative).....	8
5.1 Architecture Overview .....	8
5.2 MMS Message types.....	9
5.2.1 MRN-Addressed Messages.....	10
5.2.2 Subject-cast Messages.....	10
5.3 Protocols .....	10
5.3.1 Maritime Message Transfer Protocol (MMTP) .....	10
5.3.2 Secure Maritime Message Protocol (SMMP) .....	11
5.4 Nodes .....	12
5.4.1 MMS Agent.....	12
5.4.2 MMS Edge Router .....	12
5.4.3 Router Network.....	13
5.5 Interfaces.....	13
5.5.1 Interface Agent - Edge Router .....	13
5.5.2 Interface System Actor - Agent .....	14

5.6	VHF Data Exchange System (VDES) .....	14
6	Functionality of System Components .....	16
6.1	Functionality of MMS Agent .....	17
6.1.1	Discover Edge Routers .....	24
6.1.2	ConnectAnonymously Edge Router .....	25
6.1.3	ReconnectAnonymously Edge Router Token .....	25
6.1.4	ConnectAuthenticated Edge Router .....	26
6.1.5	ReconnectAuthenticated Token .....	26
6.1.6	Status .....	27
6.1.7	Query .....	27
6.1.8	Subscribe subject .....	27
6.1.9	Unsubscribe subject .....	28
6.1.10	SubscribeMessages .....	28
6.1.11	UnsubscribeMessages .....	29
6.1.12	Send Recipient MRNs .....	29
6.1.13	Send Subject .....	30
6.1.14	Notify .....	30
6.1.15	Receive filter .....	30
6.1.16	Disconnect .....	31
6.1.17	Persistence .....	31
6.2	Functionality of MMS Edge Router .....	31
6.2.1	General Functionality Concepts .....	33
6.2.2	Specific Functions .....	38
6.3	Functionality of MMS Router .....	45
6.3.1	Interface to MMS Edge Routers .....	45
6.3.2	Routing Network Interface .....	47
6.4	Functionality of MMS Router Network .....	48
6.5	Functionality of a SMMP Client .....	48
6.5.1	EstablishSession Remote SMMP Client .....	49
6.5.2	Send SMMP Message .....	49
6.5.3	SegmentMessage .....	49
6.5.4	AssembleMessage .....	50
6.5.5	TerminateSession Remote SMMP Client .....	50
7	The MMS Transfer Protocol .....	50
7.1	Overview (informational) .....	50
7.2	Requirements .....	51
7.3	Definitions .....	51
7.3.1	MMTP messages .....	51
7.3.2	MMTP Message Types .....	51
7.3.3	MMTP Request Message Types .....	52
7.3.4	MMTP Response Message Types .....	52
7.3.5	MRN .....	53
7.3.6	Application message .....	53
7.3.7	MMTP Protocol Request messages .....	55
8	The Secure Maritime Messaging Transfer Protocol .....	58
8.1	Overview (informational) .....	58
8.2	Definitions .....	58
8.2.1	SMMP messages .....	58
8.2.2	SMMP message identifier (magic word) .....	60

8.2.3	SMMP Handshake .....	60
8.2.4	SMMP Message reception .....	61
8.2.5	SMMP session termination .....	64
9	The MMS Router Network Protocol .....	64
9.1	Overview (informational) .....	64
9.2	Requirements .....	65
9.3	Definitions .....	65
9.3.1	Connection Between MMS Routers .....	65
9.3.2	Establishment of MMS Router Network .....	65
9.3.3	Handling of Subscriptions .....	65
9.3.4	Routing of Messages .....	66
10	Binding .....	67
10.1	WebSocket binding .....	67
10.1.1	WebSocket Endpoints .....	67
10.1.2	Connection Management .....	67
10.1.3	Discovery of Endpoints .....	67
10.1.4	Status .....	67
10.1.5	Timeouts .....	67
11	Example Implementation of a use case (informative) .....	67
11.1	MUC 2.5 realization .....	67
11.1.1	Service Registration .....	68
11.1.2	Service provision and consumption .....	68
11.1.3	Subscription to a subject using MMTP over VDES .....	69
Annex A (informative)	MMS Motivational Use Cases (Informative) .....	70
A.1	MUC1: User group - Navigator .....	70
A.1.1	MUC1.1: Navigational Supplementary Information .....	70
A.1.2	MUC1.2: Route validation service .....	70
A.1.3	MUC1.3: Chat service .....	70
A.1.4	MUC1.4: Emergency Signalling .....	70
A.1.5	MUC1.5: Intention broadcast .....	70
A.1.6	MUC1.6: Multiple services .....	71
A.2	MUC2: User group - Maritime Service Provider .....	71
A.2.1	MUC2.1: Search and Rescue Coordination .....	71
A.2.2	MUC2.2: Priorities on Safety .....	71
A.2.3	MUC2.3: ATon monitoring .....	71
A.2.4	MUC2.4: Virtual Aids-to-Navigation .....	71
A.2.5	MUC2.5: Subject based service provisioning .....	72
A.2.6	MUC2.6: Network aware response to service request .....	72
A.2.7	MUC2.7: Automatic Information Exchange .....	72
A.2.8	MUC2.8: AIS Authentication .....	72
A.3	MUC3: User group - Pilot .....	72
A.3.1	MUC3.1: Pilotage .....	72
A.4	MUC4: User group - Ship Owner .....	72
A.4.1	MUC4.1: Mirroring of Messages .....	72
Annex B (informative)	Annex MMS Ship Equipment .....	74
B.1	Ship Equipment for utilizing internet connectivity .....	74
B.2	Ship Equipment for utilizing optional SMMP .....	74

B.3	Ship Equipment for utilizing VDES connectivity .....	74
B.4	Ship Equipment for utilizing optional NAVDAT .....	74
Annex C	(informative) MMS Binding for VDE-TER networks.....	75
C.1	Entities overview.....	75
C.1.1	VDE-TER Shore Base Station .....	75
C.1.2	MMS VDE-TER Gateway .....	76
C.1.3	VDE-TER Link .....	76
C.1.4	VDE-TER Mobile Equipment .....	77
C.1.5	VDE-TER enabled mobile MMS Edge Router .....	77
C.1.6	VDE-TER Shore Network .....	77
C.2	VDE-TER transport specific function details .....	78
C.2.1	MMS VDE-TER Gateway .....	78
C.2.2	VDE-TER enabled ship MMS Edge Router.....	80
C.3	VDE-TER Discover Protocol Message.....	82
Annex D	(informative) MMS Binding for VDE-SAT Networks .....	84
D.1	Entities overview.....	84
D.1.1	VDE-SAT Satellite Station .....	84
D.1.2	VDE-SAT Satellite Network.....	84
D.1.3	MMS VDE-SAT Gateway .....	85
D.1.4	VDE-SAT Link .....	85
D.1.5	VDE-SAT Mobile Equipment .....	85
D.1.6	VDE-SAT enabled mobile MMS Edge Router .....	86
D.1.7	VDE-SAT Satellite Network.....	86
D.2	VDE-SAT transport specific function details .....	86
D.2.1	VDE-SAT Satellite Edge Router .....	86
D.2.2	MMS VDE-SAT Gateway .....	88
D.2.3	VDE-SAT enabled ship MMS Edge Router .....	91
D.3	VDE-SAT Fragment Header .....	92
D.4	VDE-SAT Discover Protocol Message.....	93
Annex E	(informative) Annex MMS Binding for ITU-R M.2116 [29] .....	95
Annex F	(informative) Annex MMS Binding for NAVDAT .....	96
F.1	Introduction.....	96
F.2	Background and Notes.....	96
F.3	Entities Overview .....	96
F.3.1	NAVDAT Transmitter Station .....	97
F.3.2	NAVDAT Ship Receiver .....	97
F.3.3	MMS NAVDAT Gateway .....	97
F.3.4	NAVDAT enabled mobile MMS Edge Router .....	98
Annex G	(informative) Annex MMS Binding for SECOM .....	99
G.1	Entities Overview .....	99
G.1.1	SECOM Service.....	99
G.1.2	MMS SECOM Gateway.....	99
G.1.3	SECOM Ship Agent .....	100
G.2	SECOM specific function details .....	100
G.2.1	SECOM Gateway.....	100
Annex H	(informative) Annex Protobuf Definition of MMTP .....	101
Annex I	(informative) Annex Protobuf Definition of SMMP .....	104
Bibliography	.....	105

## Table of Figures

Figure 1 – Overview of MMS system architecture.....	9
Figure 2 – Example of MMS protocol layering for messages over IP. ....	11
Figure 3 – Example of MMS protocol layering for messages over IP with SMMP. ....	11
Figure 4 – Overview of MMS system architecture with VDES connection. ....	15
Figure 5 – Example of MMS protocol layering for messages over VDES without SMMP. ....	16
Figure 6 – UML diagram showing the components of the MMS. ....	17
Figure 7 – UML diagram showing the functionality of the MMS Agent.....	18
Figure 8 – UML MSC Diagram: MMS Agent connects anonymously to an MMS Edge Router from User/App point of view.....	19
Figure 9 – UML MSC Diagram: MMS Agent connects and authenticates to an MMS Edge Router from User/App point of view.....	20
Figure 10 – UML MSC Diagram: authenticated MMS Agent subscribes to messages from User/App point of view. ....	21
Figure 11 – UML MSC Diagram: non-authenticated MMS Agent subscribes to messages from User/App point of view. ....	22
Figure 12 – UML MSC Diagram: MMS Agent receives messages. ....	23
Figure 13 – UML MSC Diagram: authenticated Application is sends messages and receives response.....	24
Figure 14 – UML MSC Diagram: MMS Agent connects and authenticates to MMS Edge Router from User/App point of view.....	35
Figure 15 – UML MSC Diagram: authenticated MMS Agent subscribes to messages at an MMS Edge Router.....	36
Figure 16 – UML MSC Diagram: MMS Agent receives messages from an MMS Edge Router. ....	37
Figure 17 – UML Sequence Diagram Delivery Guarantee: The receiving SMMP client may bundle acknowledgements. ....	62
Figure 18 – UML Sequence Diagram Non-repudiation: The receiving SMMP client must provide proof of reception using his digital signature.....	64
Figure 19 – Use Case Implementation and signalling steps.....	68
Figure 20 – Service Subscription and Delivery. ....	69
Figure 21 – Overview of MMS system architecture with VDE-TER network. ....	75
Figure 22 – Overview of MMS system architecture with VDE-SAT network. ....	84
Figure 23 – Overview of MMS system architecture with NAVDAT.....	97

This page intentionally left blank



## Introduction

This standard specifies the architecture, operational aspects, performance requirements, and protocol of the Maritime Messaging Service System.

RTCM draws attention to the possibility that the implementation of this standard may involve the use of (a) patent(s). RTCM takes no position concerning the evidence, validity, or applicability of any claimed patent rights in respect thereof.

As of the date of publication of this standard, RTCM had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information which may be obtained from the latest version of the applicable standard. RTCM shall not be held responsible for identifying any or all such patent rights or claims.

# MARITIME MESSAGING SERVICE ARCHITECTURE AND PROTOCOL

## 1 Scope

The purpose of this document is to describe the protocol of the Maritime Messaging Service System. This description is the first step in order to create an internationally recognized protocol and system standard. It can further be referred to by a new IMO performance standard, which then can be referred to by SOLAS Chapter V as a permitted means to transport safety of navigation related e-Navigation services.

This document is not an equipment standard. These might be developed later referring to an IMO performance standard.

This document is a first edition towards a normative standard.

Wording is to be used as follows:

- the word “shall” indicates normative aspects of the System
- the word “may” indicates non-normative aspects of the System

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this chapter are to be interpreted as described in [RFC2119].

## 2 Normative References

None

## 3 Terms and Definitions

### 3.1 Abbreviations

#### 3.1.1

##### AtoN

Aids to Navigation

#### 3.1.2

##### EUT

Equipment under Test

#### 3.1.3

##### DHT

Distributed Hash Table

#### 3.1.4

##### GMDSS

Global Maritime Distress and Safety System

**3.1.5**

**MCC**

MCP Consortium

**3.1.6**

**MCP**

Maritime Connectivity Platform

**3.1.7**

**MIR**

Maritime Identity Registry

**3.1.8**

**MMS**

Maritime Messaging Service

**3.1.9**

**MMSI**

Maritime Mobile Service Identity

**3.1.10**

**MMTP**

Maritime Message Transfer Protocol

**3.1.11**

**MRN**

Maritime Resource Name

**3.1.12**

**MSR**

Maritime Service Registry

**3.1.13**

**SMMP**

Secure Maritime Message Protocol

**3.1.14**

**TCP**

Transmission Control Protocol

**3.1.15**

**TTL**

Time to Live

**3.1.16****TE**

Test Equipment

**3.1.17****VDE**

VHF Data Exchange

**3.1.18****VDE LL**

VDE Link Layer

**3.1.19****VDES**

VHF Data Exchange System

**3.1.20****VDES PI**

VDES Presentation Interface, referring to the application side interface of a VDES modem as defined in [1]

**3.1.21****VDE-TER**

The terrestrial VHF Data Exchange access as described by [2], Annex 4

**3.1.22****VDE-SAT**

The satellite VHF Data Exchange access as described by [2], Annex 5

**3.2 Definitions**

For the purpose(s) of this Standard, the following definitions apply:

**3.2.1 Aid to Navigation**

A device, System or Service, external to vessels, designed and operated to enhance safe and efficient Navigation of individual vessels and/or vessel traffic.

**3.2.2 Broadcast Message**

A message sent from one sender to all receivers within the propagation range of a radio transmitter. Due to physical propagation nature, the number of receivers in propagation range of a transmitter can be between zero and unlimited. Broadcast is only applicable in radio networks to achieve geographical coverage of a region around a transmitting station. Different receiver parameters can make the actual range larger or smaller than expected, dependent on interference, the signal path, the receiver performance, and antenna heights.

Multiple transmitters can be used to broadcast the same message to achieve a larger coverage area. Broadcast may include repetition of the same message until the given TTL in order to reach receivers that were outside range, shadowed or switched off during earlier transmissions.

### **3.2.3 MRN-addressed Message**

A message sent from a sender to one or more receivers based on a MCP MRN.

### **3.2.4 Subject-cast Message**

A message addressed to all receivers subscribing to a specific subject-tag. This subject-tag can be a reference to a certain geographical region and/or a certain service.

### **3.2.5 Anonymity**

Anonymity (in anonymous access) describes situations where an MRN or identity of a System Actor is unknown.

### **3.2.6 Maritime Identity Registry (MIR)**

The MIR is responsible for identity management and providing security functionality to the entities of the MCP. For more information, see

<https://maritimeconnectivity.net/mcp-documents/#MIR>.

### **3.2.7 Maritime Service Registry (MSR)**

The MSR does not provide actual maritime information but a specification of various services, the information that they carry, and the technical means to obtain it. An MSR instance contains service specifications according to a Service Specification Standard (which is identical to IALA Guideline 1128) and provisioned service instances implemented according to these service specifications. For more information, see

<https://maritimeconnectivity.net/mcp-documents/#MSR>.

### **3.2.8 MCP MRN**

A Maritime Resource Name as defined for the Maritime Connectivity Platform.

### **3.2.9 Navigation**

The process or activity of accurately ascertaining one's position and planning and following a route.

### **3.2.10 Navigator**

The person on board a ship responsible for its Navigation.

### **3.2.11 Service**

The application of competences (knowledge, skills and resources) by one entity for the benefit of another entity in a non-coercive (mutually agreed and mutually beneficial) manner.

### **3.2.12 Service Consumer**

A software application, or other type of software module that requires a connection to a (Technical) Service through MMS. The Service Consumer can either be authenticated as an entity authorized to use Services provided by Service Provider or unauthenticated for Services not requiring authentication.

### **3.2.13 Service Provider**

An entity providing a Service.

### **3.2.14 Technical Service**

A software functionality or a set of software functionalities with a purpose that different Service Consumers can reuse for different purposes, together with the policies that should control its usage.

Where there is no risk of confusion, the term 'Service' may be used instead.

### 3.2.15 Time to Live

Time to Live in MMS is a timestamp set by the sender of an MMS message after which the message is considered not worth transporting by the MMS anymore; in practice, the message will be deleted from all queues, independent of whether it was delivered or not.

### 3.2.16 VDE-TER Network

A network consisting of one or more VDE shore base stations that are interconnected with a shore MMS Edge Router to facilitate access to mobile VDES equipment through the VHF Data Exchange terrestrial access method described in [2].

### 3.2.17 VDE-SAT Network

A network consisting of one or more VDE satellites that are interconnected with a shore MMS Edge Router to facilitate access to mobile VDES equipment through the VHF Data Exchange satellite access method described in [2].

## 4 General Considerations (informative)

### 4.1 Motivation

Maritime digitalization will enable increased operational efficiency, improve productivity, and is needed today. A number of key digital services have been identified in the IMO e-Navigation Strategy Implementation Plan [3], including port call procedures, distribution of navigational warnings, and VTS services. However, the maritime sector is generally lagging far behind comparable terrestrial industries when it comes to the level of digitalization and automation.

The two main reasons for this are:

- Connectivity at sea is generally difficult and costly. In near-shore waters, vessels may rely on cellular networks from shore, but in the oceans the only option is a satellite connection, which is rather limited and expensive compared to fiber-optic cabling on land. In the high-end maritime segment, the cost and overhead of connectivity is not necessarily significant, but for the broader segment, it prevents the deployment of digital solutions.
- Safety at sea is a vital requirement. When a vessel leaves harbor, it will be in a state of potential emergency if anything goes wrong. This means that maritime digital services will necessarily be deployed on strictly certified hardware and be trustable. It should be easy to establish a high level of cyber security on board even using contemporary e-Navigation services. Even though solutions solving cyber security concerns exist, there are no established standards that enable smaller vessels to easily deploy a cyber secure system when connecting through existing solutions.

As a result, the maritime industry has fallen behind comparable land-based industries when it comes to the use of IT and communications, resulting in highly-manual, time-consuming procedures for services that could be digitalized and automated. For example, the Danish Meteorological Institute produces up-to-date ice charts for waters around Greenland, and shipping companies can subscribe to these. The production of ice charts has become increasingly automated, but the delivery today is via an email with an attached file. The ice chart can then be viewed on a separate monitor next to the ECDIS or printed on paper. It would be much more effective if ice charts were delivered periodically, in a form that could be visualized directly in the ECDIS. Data formats do exist in draft form (IHO S-411), but secure connectivity between the weather authority and the onboard ECDIS is not possible through the established standards. The Maritime Messaging System (MMS) solves the above challenges by proving means to transfer e- Navigation services over frequently changing connection speed and means, while also providing the security the Maritime Connectivity Platform (MCP) offers.

## 4.2 The Maritime Connectivity Platform

The MCP is a decentralized platform that facilitates secure and reliable information exchange within the maritime domain and beyond. Beyond – because the maritime world isn't isolated but needs to exchange information with other domains – for instance with other transport domains.

The information exchanged can be almost of any nature, ranging from private confidential information between a vessel and the shore office of the shipowner, to public information provided by authorities, such as the provision of navigational warnings.

As a decentralized platform, there is no single entity operating this. Several organizations are MCP service providers, and collectively they form “the Maritime Connectivity Platform”.

The central part of the MCP is to provide trust between its stakeholders: users and service providers. The key component of the MCP therefore is the Maritime Identity Register (MIR). Agreed vetting procedures are to be used to establish an identity in a MIR.

The MCP also provides means to register maritime services in the Maritime Service Register (MSR). The MSR is organized to allow maritime users to discover services based on many parameters, such as:

- region (e.g. Norway, NAVAREA XI - JAPAN)
- subject (e.g. ice chart)
- format (e.g. S-411)
- coordinates
- MRN

## 4.3 The Maritime Messaging Service

The Maritime Messaging Service (MMS) is a store-and-forward messaging service intended to offer transparent seamless information transfer across different communication links in a carrier agnostic and geolocation-context sensitive manner.

The MMS primarily addresses ship-shore communication based on internet connectivity, yet any number of alternative communication services may be connected to and utilized by the MMS via dedicated gateways. As an example, a message, sent by one specific ship using INMARSAT access to the MMS, may be received via a VSAT terminal on another ship, an VDES connection on yet another ship, or a VTS operator on a DSL landline internet connection. MMS enables the transfer by using the Maritime Resource Name (MRN) of an entity as an end-point address.

Each communication technology may impose situation specific limitations in terms of restrictions to capabilities, bandwidth availability, size of transferrable data packages, latencies, etc. But basic transfer of text or structured data (e.g. using XML) is possible with all supported communication technologies.

Annex A lists the motivational use cases that lead to the following architecture and requirements for the MMS.

## 4.4 Compliance with IMO requirements

In its draft performance standard for VDES (version 0.5), the Navigation Communication Search and Rescue Subcommittee (NCSR) formulates:

1.4 VDES should be able to provide the following functions:

- .1 exchanging data to improve safety, security and efficiency of navigation and protection of marine environment;
- .2 as a means for coastal States to request and obtain information about a ship and its cargo and/or passengers;

.3 as a means for providing maritime services in the context of e-navigation; and

.4 provide means for standardized and automated reporting in accordance with MSC.1/Circ.1595.

Among these, the MMS with its support for VDES, supports all in a trusted and secure way, over the supported communication channels the ship may have available to communicate.

The support of .4 is explained further in 4.4.1

#### 4.4.1 Support of MSC.1/Circ.1595

[3] defines in Table 2 the referred means for standardized and automated reporting as following sub solutions S2.1, S2.2, S2.3 and S2.4.

Where:

- S2.1 describes the maritime single window for all reportable information. Further work is needed to identify which maritime single window standards MMS can support.
- S2.2 describes the automated collection of internal ship data for reporting [to authorities], which is supported by MMS, but requires harmonized formats for information exchange.
- S2.3 describes automated or semi-automated digital distribution/communication of required reportable information, including both “static” and “dynamic” information; this requirement is already implemented by any VDES mobile station as part of the AIS standard. MMS can add safety to the position reports by providing transport for the maintenance of authentication certificate updates and revocations.
- S2.4 describes standardized digital reporting based on recognized internationally harmonized standards, such as IMO FAL Forms or SN.1/Circ.289. This is supported as MMS can support all digital formats transport from a ship to shore and vice versa to request such data and provide format specifiers.

## 5 System Architecture (informative)

The architecture of the MMS system is designed as a system to facilitate sending messages between users (ship crew, captains, pilots, personal equipment, services, etc.) in the maritime environment with an uncomplicated way to ensure message security (authentication, confidentiality, non-repudiation, etc.). The system will connect users working both on ships and shore-side locations. They are not necessarily stationary, meaning they can move between ships and/or shore-side locations. Ships are moving, and therefore connectivity at sea can be intermittent and changing between different connectivity speeds, qualities and protocols.

Providing a transport of maritime messages that is hardened against the unstable maritime communication environment, the MMS uses protocols that are built on known networking, security, and cryptography principles. MMS is implemented as a store-and-forward system.

### 5.1 Architecture Overview

The MMS system architecture defines the following components.

- MMS Agents,
- MMS Edge Routers, and
- MMS Router Network,

and the following protocols

- Maritime Message Transfer Protocol (MMTP), and
- Secure Maritime Message Protocol (SMMP).



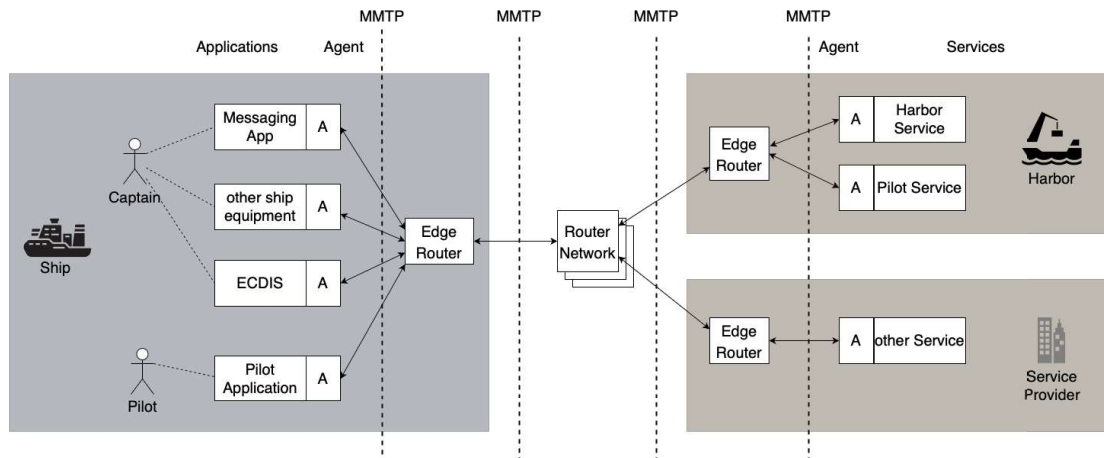
System Actors (short Actors) in this document are systems, personal devices and applications using the MMS. Actors run/use different applications, which interact with other Actors through an MMS Agent.

All MMS Agents that want to send messages and receive MRN-addressed messages, must be authenticated with an MMS Edge Router using a MCP certificate.

All messages from MMS Agents must be authenticated (signed) with a certificate from the sending MCP MRN. Such a certificate shall be issued in accordance with [4].

MMTP only provides message authentication. Messages between Actors may be sent via the SMMP to provide further security guarantees.

As an example of a system (see Figure 1), the different applications of a ship (e.g. ECDIS, captains messaging app, pilot function) can communicate securely with a service provided by a harbor or service provider.



**Figure 1 – Overview of MMS system architecture.**

The following sections describe the nodes and interfaces and their functions as a high-level introduction to each of the MMS architecture components.

Note, that we will make the distinction between

- MMS Edge Routers, and
- MMS Router Network.

An MMS Router Network consists of one or more MMS Routers. An MMS Edge Router shall perform domain specific operations needed in the intended installation location, such as supporting multiple communication links.

The MMS is designed to support message transfer between routers over different connection types, i.e. TCP/IP and VDES.

## 5.2 MMS Message types

The MMS defines the following two message types. All messages sent over the MMS must be authenticated (signed) by the sender with a MCP certificate associated to an MCP MRN.

### 5.2.1 MRN-Addressed Messages

MRN-addressed messages are messages sent from a specific MCP MRN to another specific MCP MRN. The receiver can be one or more agents.

### 5.2.2 Subject-cast Messages

Subject-cast messages are MMS messages published from a specific MCP MRN on a specific subject tag.

## 5.3 Protocols

The MMS defines the following two protocols.

### 5.3.1 Maritime Message Transfer Protocol (MMTP)

MMTP is the transfer protocol between MMS Agents via MMS Routers. This protocol handles three central aspects

- registration of agents based on MCP-MRNs,
- authenticated message transfer (send/receive), and
- message subscriptions based on subjects.

Senders are identified by authenticated MCP-MRNs. Recipients of MRN-addressed messages are specified using MCP-MRNs. Senders and Recipients of the MMTP are agents. The MCP-MRN that defines these agents, however, comes from the Actors as these are needed for authentication. Subject-cast messages are identified with a subject-string.

Note, that the MCP MRN used by an MMS Agent shall be MIR-authenticated.

For the example of a ship crew sending a message to the Danish Maritime Authority (DMA), DMA might have several MRNs in use to receive topic specific messages. Similarly, as today, when a user sends an e-mail to DMA, they would not just send it to the generic e-mail address like *info@dma.dk*, but instead to a specific address for their specific purpose e.g. *arctic\_wx-observations@dma.dk*. Thus, DMA may choose to have one (or more) Agent(s) running with a general DMA MCP MRN, but most MRNs would address specific purposes, like for example:

- *...:DMA:NW* for navigational warnings,
- *...:DMA:ArcticWxObs* for arctic weather observation reports from ships, or
- *...:DMA:GreenposReporting* for GREENPOS reporting, and so on.

For an example overview over MMS protocol layers in use, see Figure 2.

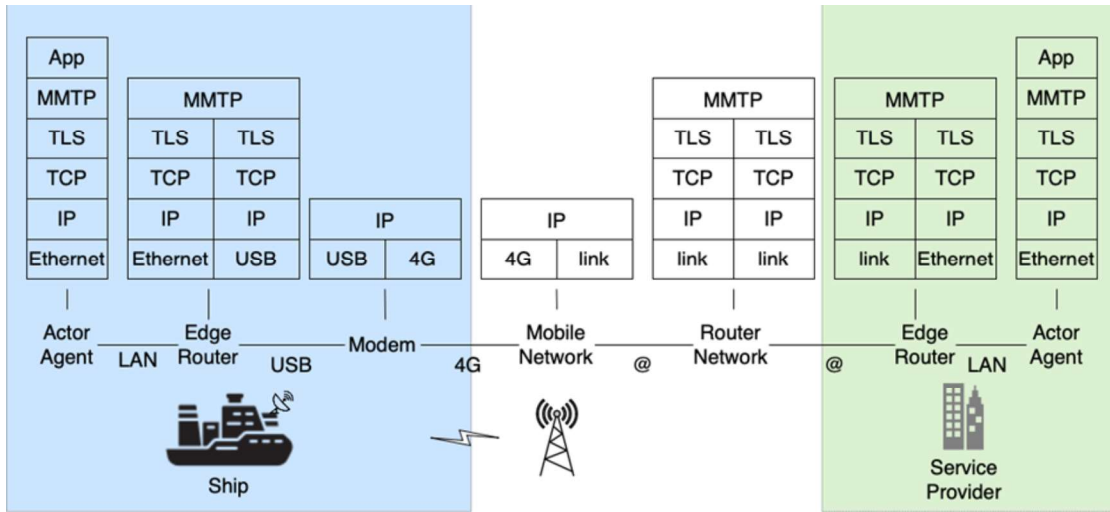


Figure 2 – Example of MMS protocol layering for messages over IP.

### 5.3.2 Secure Maritime Message Protocol (SMMP)

SMMP is an end-to-end protocol that provides security guarantees between System Actors. For an example protocol overview, see Figure 3.

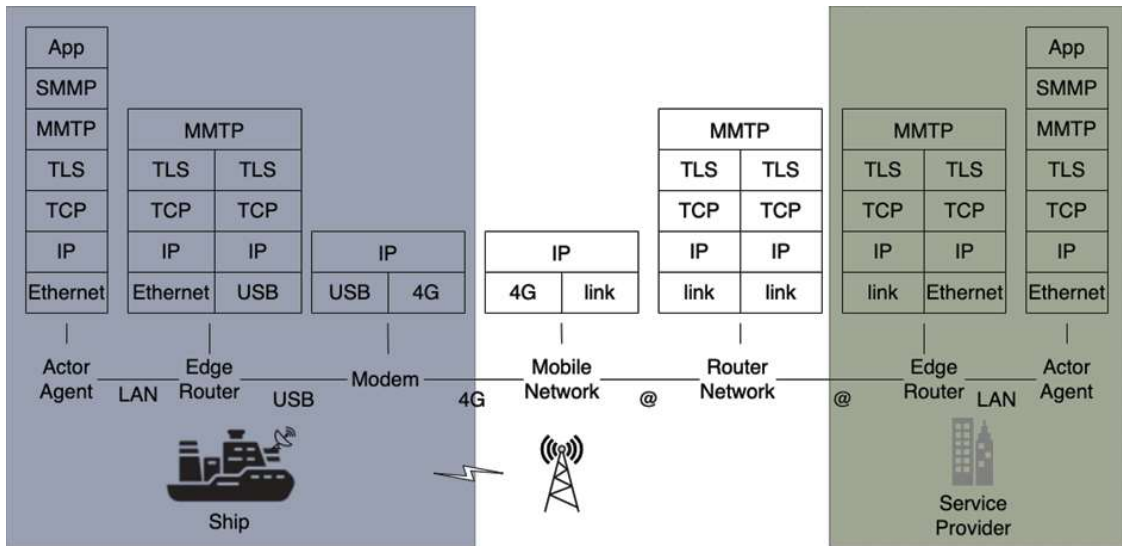


Figure 3 – Example of MMS protocol layering for messages over IP with SMMP.

The system provides the following end-to-end guarantees through the SMMP:

- Confidentiality: A message sent between users cannot be read by a third party.
- Integrity: The receiver of an authenticated message can be sure that for a given receiver the message has not been altered and it is guaranteed to come from the sender.
- Authenticity: Knowing who sent the message.

- Availability: In this case also called delivery guarantee. A message from a sender must either arrive at an available receiver within reasonable time or if the receiver cannot be found the sender must be notified of the failure to deliver.
- Non-repudiation: The receiver needs to give proof of reception.
- Segmentation of larger addressed messages.

To use the SMMP, Actors must authorize into the MMS with an MCP certificate.

Note: Authenticity is also included in the MMTP protocol. It may be that the two authentications are overlapping. However, there is not a requirement that the MMS Agent uses the same MCP certificate (and MCP MRN) as used for the SMMP.

## 5.4 Nodes

The MMS defines the following nodes.

### 5.4.1 MMS Agent

An MMS Agent is a client software that interfaces with System Actors and provides connectivity to the MMS. MMS Agents connect to MMS Edge Routers via the Agent-Edge Router interface using MMTP.

An MMS Agent is either MIR-authenticated, meaning that it

- has been assigned an MCP-MRN [5], in a MIR, and
- has been assigned an MCP certificate,

or

- operates anonymously.

An MIR authenticated MMS Agent may use the full functionality of the MMS.

An anonymous MMS Agent cannot receive MRN-addressed messages or send messages. This is however useful for System Actors that only need to receive subject-cast messages.

Informative Note: an MMS Agent may apply different priorities to messages by using different destination MRNs, which then in the Edge Router can be used to apply different routing policies based on local configuration.

### 5.4.2 MMS Edge Router

An MMS Edge Router handles the messages between a set of local MMS Agents and the MMS Router Network.

An MMS Edge Router authenticates the associated MIR-authenticated MMS Agents before these may receive MRN-addressed messages or send messages through the MMS Edge Router.

An MMS Edge Router is MIR-authenticated, meaning that it

- has been assigned an MCP-MRN [5], in a MIR, and
- has been assigned an MCP certificate

An MMS Edge Router may connect to one or multiple MMS Routers in the MMS Router Network. An MMS Edge Router may have a preferred MMS Router defined, but it also is able to find an MMS Router through a connection dependent lookup. An MMS Edge Router needs to authenticate for each MMS Router it connects to.

During the time an MMS Edge Router is not connected to an MMS Router of the MMS Router Network, it limits message forwarding to be between local MMS Agents only.

An MMS Edge Router provides message broker functionality to its local set of MMS Agents.

Message broking includes:

- local transport of MMS messages between Agents in the same set,
- store and forward of MMS messages between the Router Network and the local Agents,
- store and forward of MMS messages between the Router Network and the local Agents,
- subscription to Router Network provided subjects on behalf of the local Agents, and
- distribution of subject-cast messages received from the Router Network to the local Agents.

Message broking allows the distribution of a single received message to multiple subscribed MMS Agents and thus reduces traffic over the link between MMS Agents and the MMS Router Network. The message broker may discard messages that are not fetched by a subscribed MMS Agent within a configured timeout.

The MMS Edge Router may implement priority handling e.g. based on the destination MRN of messages to be sent. Local configuration on the MMS Edge Router would be used to define MRN destinations and associated allowed transports that are specifically installed for this Edge Router.

#### 5.4.3 Router Network

The MMS Router Network consists of one or more MMS Routers. The Router Network shall handle message routing and forwarding between MMS Edge Routers. The Router Network shall have the capability to exchange the knowledge about subscribed MMS Agents, and subjects between each other.

An MMS Router handles MMS message transport for a set of connected MMS Edge Routers, that subscribe to a set of specific subjects and/or specific MRNs on behalf of their subscribed MMS Agents. An MMS Router queues messages that an MMS Edge Router has subscribed to until they are fetched by that MMS Edge Router. An MMS Router may delete stored subscriptions and queued messages after a configured timeout occurs.

The MMS Router Network may handle the transfer of stored subscriptions and queued messages between the MMS Routers in case an MMS Edge Router roams from one MMS Router to another.

The MMS Router Network may support the lookup of an MMS Router by request from an MMS Edge Router, according to its current connectivity situation.

### 5.5 Interfaces

For the MMS the following interfaces are defined.

#### 5.5.1 Interface Agent - Edge Router

The Agent - Edge Router Interface uses the MMTP.

The MMTP facilitates the transfer of messages from MMS Agents through MMS Edge Routers and the MMS Router Network to one or multiple receiving MMS Agents.

For this purpose, the MMTP facilitates the exchange of information to support:

- authentication of an MMS Agent to an MMS Edge Router,
- the subscription to messages of a specific subject,
- the subscription to messages to a specific MRN,
- the transport of subscribed messages from the MMS Router Network to the MMS Agent, and

- the transport of MRN-addressed messages from the MMS Agent to the MMS Router Network.

The normative details about the MMTP are explained in Section 7.

The MMTP may give up on delivery attempts after a timeout, and therefore no delivery guarantee is given by the MMTP itself.

### 5.5.2 Interface System Actor - Agent

The MMS System Actors send/receive messages to/from other MMS Actors. The other MMS Actors can be locally connected to the same MMS Edge Router, or with remote MMS Agents at shore or on other ships. Remote MMS Agents are connected through e.g. IP or VDES connectivity.

For this purpose, the MMTP facilitates the exchange of information to support:

- authentication of an MMS Actor to an MMS Agent,
- the subscription to messages of a specific subject,
- the subscription to messages to a specific MRN,
- status querying,
- the transport of subscribed messages from the MMS Router Network to the MMS Agent, and
- the transport of MRN-addressed messages from the MMS Agent to the MMS Router Network.

Additionally, the Secure Maritime Messaging Protocol can invoke MMTP over a MIR authenticated Actors in order to facilitate:

- integrity (no alteration of the message),
- confidentiality (encryption),
- authenticity (origin of message),
- non-repudiation (message received by receiver).

### 5.6 VHF Data Exchange System (VDES)

The VDES may be used as means to transport MMS traffic by connecting the MMS ship Edge Router with other MMS Edge Routers over a VDES Network.

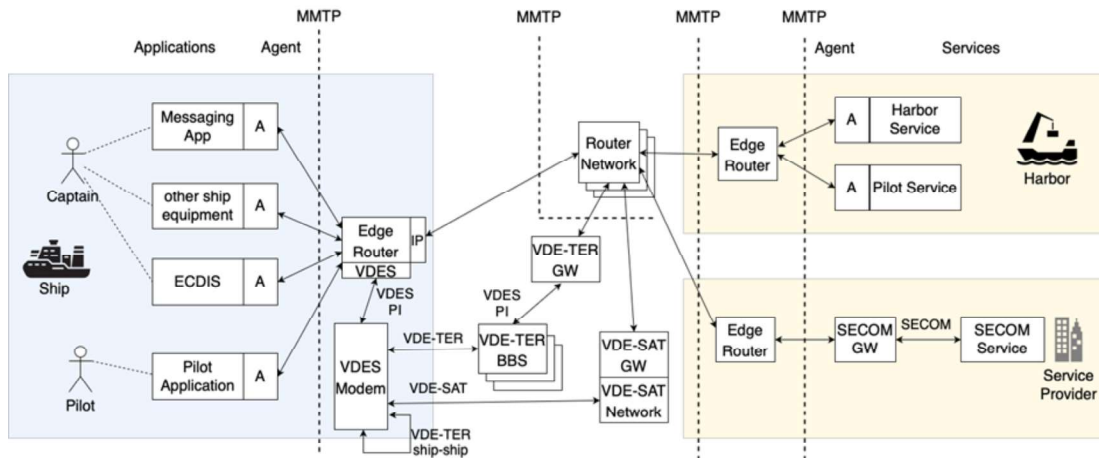
VDES provides AIS, ASM, VDE Terrestrial (VDE-TER) and VDE Satellite (VDE-SAT) services.

VDE-TER and VDE-SAT provide resources to route MMS traffic, as described in this specification.

Note: AIS and ASM data channels are reserved for small payload sizes and therefore not considered for the MMS.

In order to allow MMS transport (see 4) over VDES,

- the ship shall be equipped with a VDES enabled MMS Edge Router,
- the ship shall be equipped with a VDES Modem according to [2] and [1], and
- the ship has VDES connection with another MMS enabled ship, or
- the ship shall be within an MMS enabled VDES Network (terrestrial or satellite) coverage area, i.e. the current available VDES Network shall provide MMS routing services into the MMS Router Network.



**Figure 4 – Overview of MMS system architecture with VDES connection.**

Also, 4 shows how VDE bridges the MMS VDE-TER and VDE-SAT Gateways on the shore, through a VDE-TER or VDE-SAT network to the ship Edge Router, seen from the MMS Router Network. For the MMS Router Network, the MMS VDE-TER and VDE-SAT Gateways provide the same functionality, as the ship Edge Router when connected with the Router Network through a direct IP connection.

A VDES enabled ship Edge Router shall take into account:

- that an arbitrary VDES Network may or may not provide MMS capabilities, and therefore needs to be interrogated before use for each new VDES Network the ship roams into,
- that an arbitrary VDES Network may provide access to selected MMS services only, to be interrogated before use,
- that terrestrial VDE (VDE-TER) provides coverage along coastlines where the distance between ship and coast station reduces the connection quality and speed,
- that other ships might be directly reachable through ship-to-ship VDE-TER transfers, if the other ship is equipped with a VDE enabled ship Edge Router,
- that satellite VDE (VDE-SAT) provides world-wide satellite coverage over open water, which is expected to be available only for a few minutes at a time with coverage gaps of several hours in-between,
- that VDE-SAT based VDES Networks may not have direct connectivity with the Router Network over all territories, resulting in transport delays of up to 90 minutes.

An overview of the different protocols used between two Actor Applications on ship and shore, when using VDE-TER or VDE-SAT as a means of MMS transport, is shown in 5 for the case without SMMP.



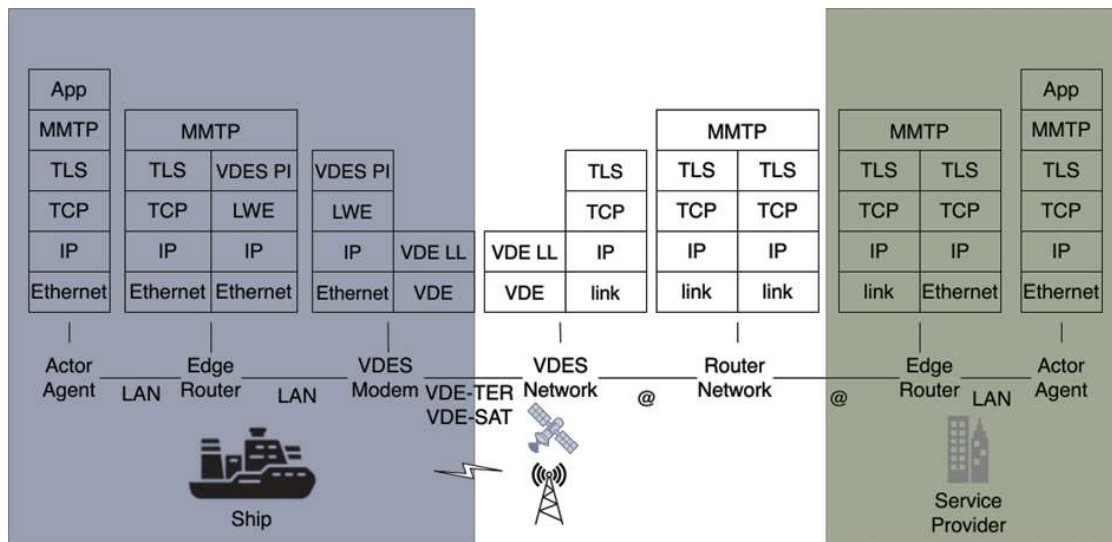


Figure 5 – Example of MMS protocol layering for messages over VDES without SMMP.

MMS over VDES shall also support SMMP as described in 5.3.2.

## 6 Functionality of System Components

This section describes the functionalities of the different system components that comprise the MMS. In Figure 6 a UML class diagram shows the connections between the components of the MMS, which will be described in detail on the following.

The following text refers to:

- ERROR for cases where the cause for the failed operation is known by the system,
- FAILURE for cases where the cause for the failed operation is unknown.



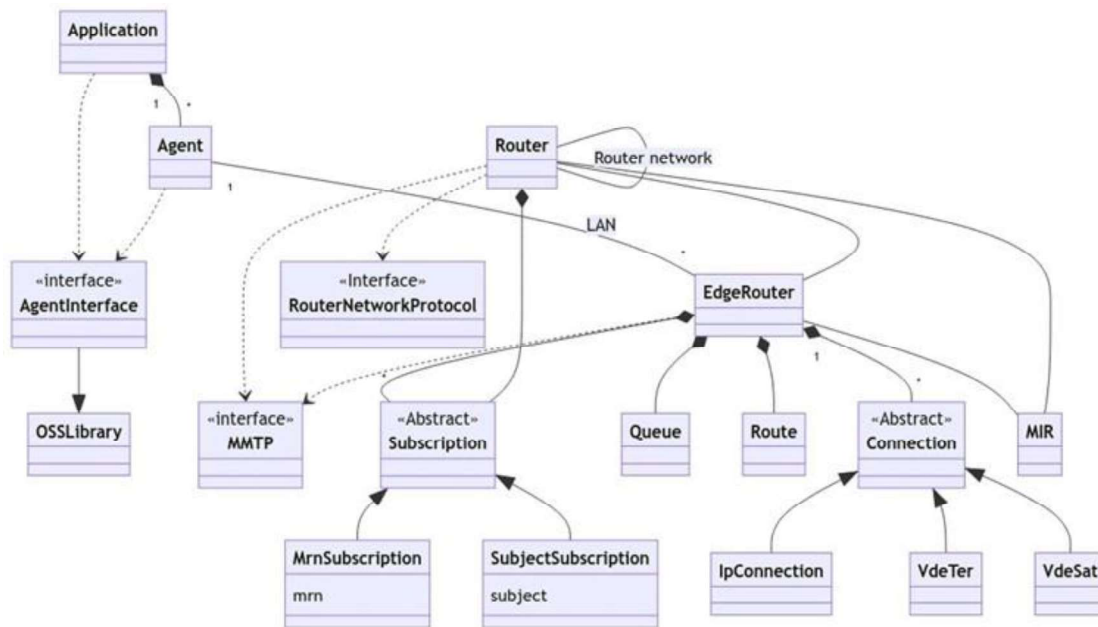


Figure 6 – UML diagram showing the components of the MMS.

### 6.1 Functionality of MMS Agent

An MMS Agent enables an Actor to be connected to MMS by establishing a connection with an MMS Edge Router using the MMTP. Sending and receiving of messages and subscribing to subjects are the basic functionalities of an MMS Agent.

An MMS Agent shall have three overall states:

- **Not Connected.** The MMS Agent has been started but is not connected to an MMS Edge Router.
- **Connected.** The MMS Agent has been anonymously connected to an MMS Edge Router.
- **Authenticated.** The MMS Agent has been connected and authenticated with an MMS Edge Router using an MCP certificate.

The overall functionality of an MMS Agent in one of the above states is described below. All functions shall be non-blocking.

- **Status.** Return the current status of the MMS Agent.
- **Discover.** When an MMS Agent connects to a Local Area Network, it should be able to lookup possible MMS Edge Routers. It is not a requirement that MMS Edge Routers announce themselves and MMS Agents can have predefined MMS Edge Routers.
- **ConnectAnonymous Edge Router.** An MMS Agent may connect anonymously to an MMS Edge Router enabling it to receive subject-cast messages.
- **ConnectAuthenticated Edge Router.** An MMS Agent may connect to an MMS Edge Router with authentication enabling it to send messages and receive MRN-addressed messages.
- **ReconnectAnonymous Edge Router Token.** An MMS Agent may reconnect anonymously to an MMS Edge Router to continue a previous anonymous connection.
- **ReconnectAuthenticated Edge Router Token.** An MMS Agent may reconnect to an MMS Edge Router with authentication to continue a previous authenticated connection.

- **Query.** During the connection process, an MMS Agent may query the MMS Edge Router for information on its connections and proof of authentication.
- **Subscribe Subject.** An MMS Agent may subscribe to subjects with the MMS Edge Router. Subscriptions are based on *subjects*, which are encoded as text strings.
- **Unsubscribe Subject.** An MMS Agent may unsubscribe to subjects with the MMS Edge Router. Subscriptions are based on *subjects*, which are encoded as text strings.
- **SubscribeMessages.** An MMS Agent may subscribe to MRN-addressed messages with the MMS Edge Router. This requires that the MMS Agent is authenticated.
- **UnsubscribeMessages.** An MMS Agent may unsubscribe to MRN-addressed messages with the MMS Edge Router.
- **Send Message.** When an MMS Agent is authenticated with an MMS Edge Router, it may send messages. These can be either MRN-addressed or subject-cast.
- **Notify.** An MMS Agent shall provide this function to an MMS Edge Router, it is triggered by receiving a protocol message from the MMS Edge Router to notify new arrived messages.
- **Fetch.** An MMS Agent shall provide this function to an MMS Edge Router to get list of available messages at an MMS Router.
- **Receive.** An MMS Agent shall fetch its received messages stored at a connected MMS Edge Router by this function.
- **Disconnect.** An MMS Agent shall disconnect from the MMS Edge Router by use of this function.

An MMS Agent shall implement the state transitions shown in Figure 7.

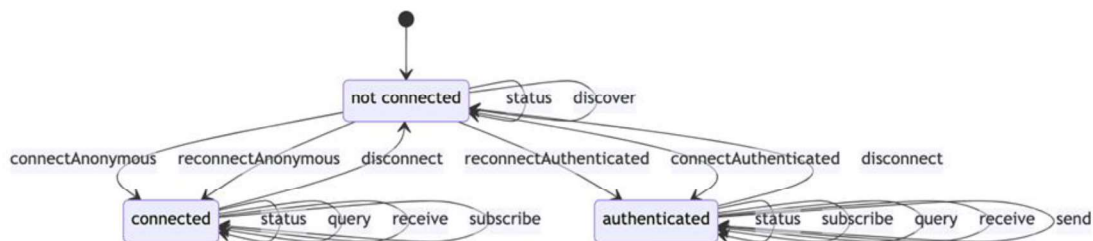


Figure 7 – UML diagram showing the functionality of the MMS Agent.

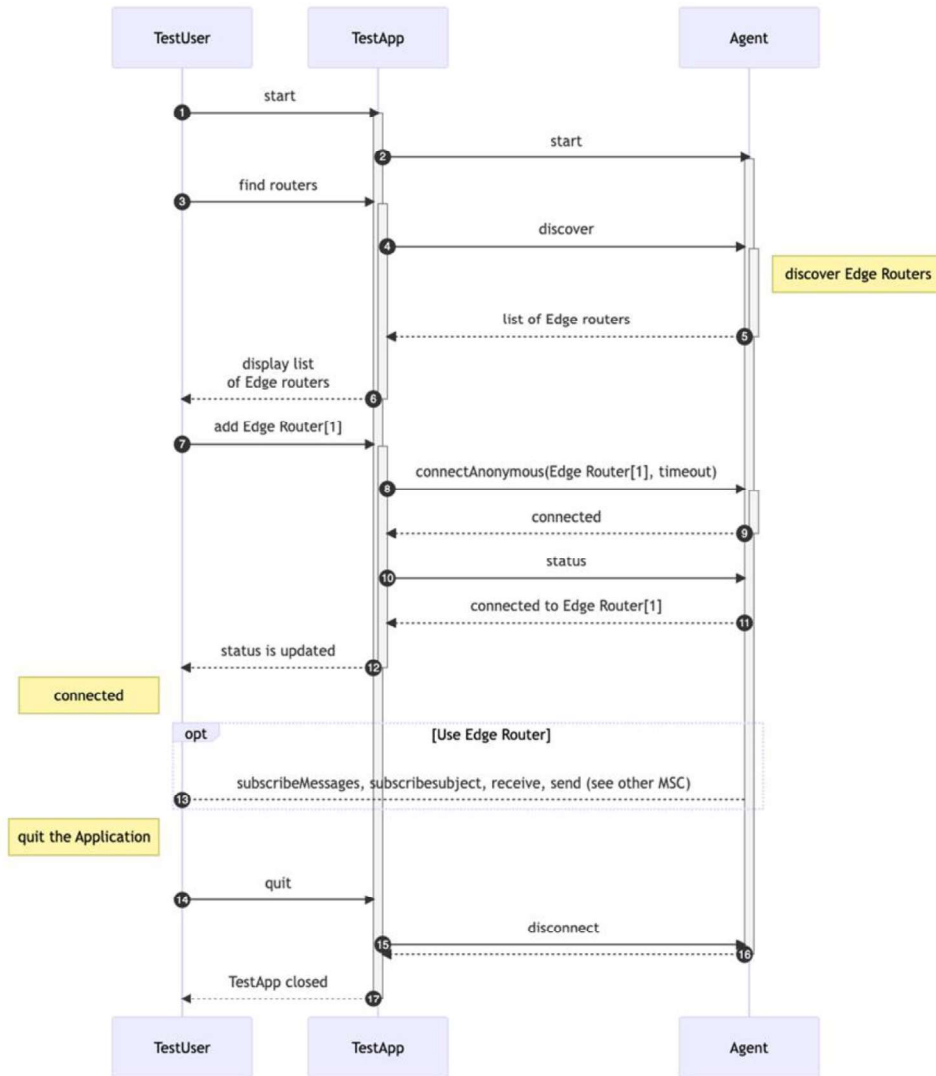


Figure 8 – UML MSC Diagram: MMS Agent connects anonymously to an MMS Edge Router from User/App point of view.

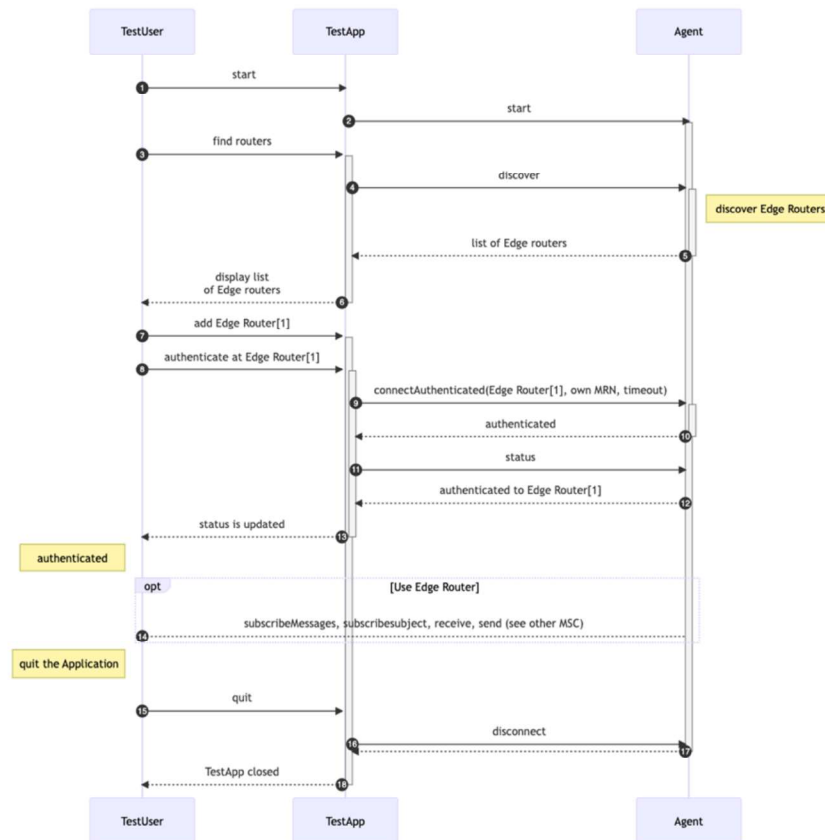


Figure 9 – UML MSC Diagram: MMS Agent connects and authenticates to an MMS Edge Router from User/App point of view.



Figure 10 – UML MSC Diagram: authenticated MMS Agent subscribes to messages from User/App point of view.

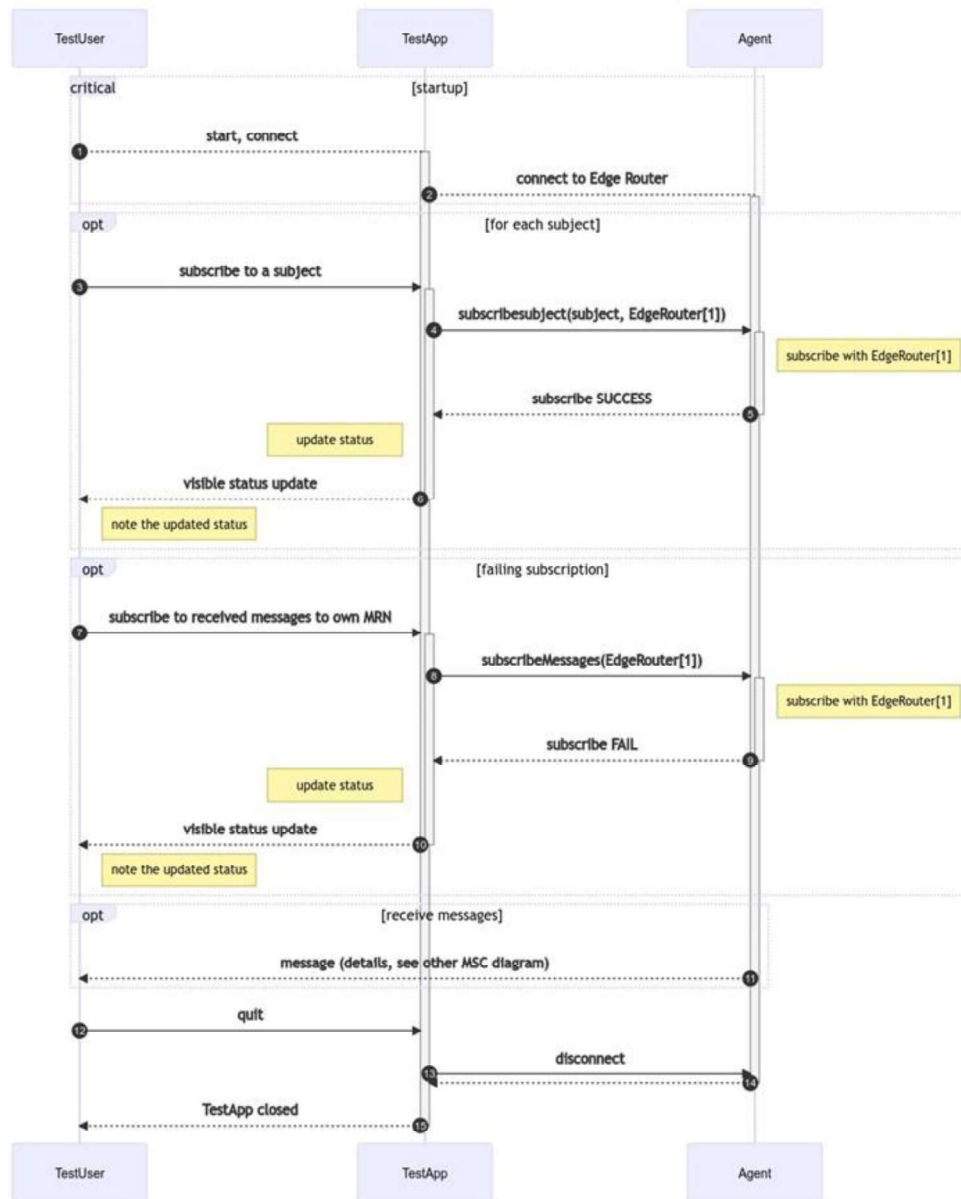


Figure 11 – UML MSC Diagram: non-authenticated MMS Agent subscribes to messages from User/App point of view.

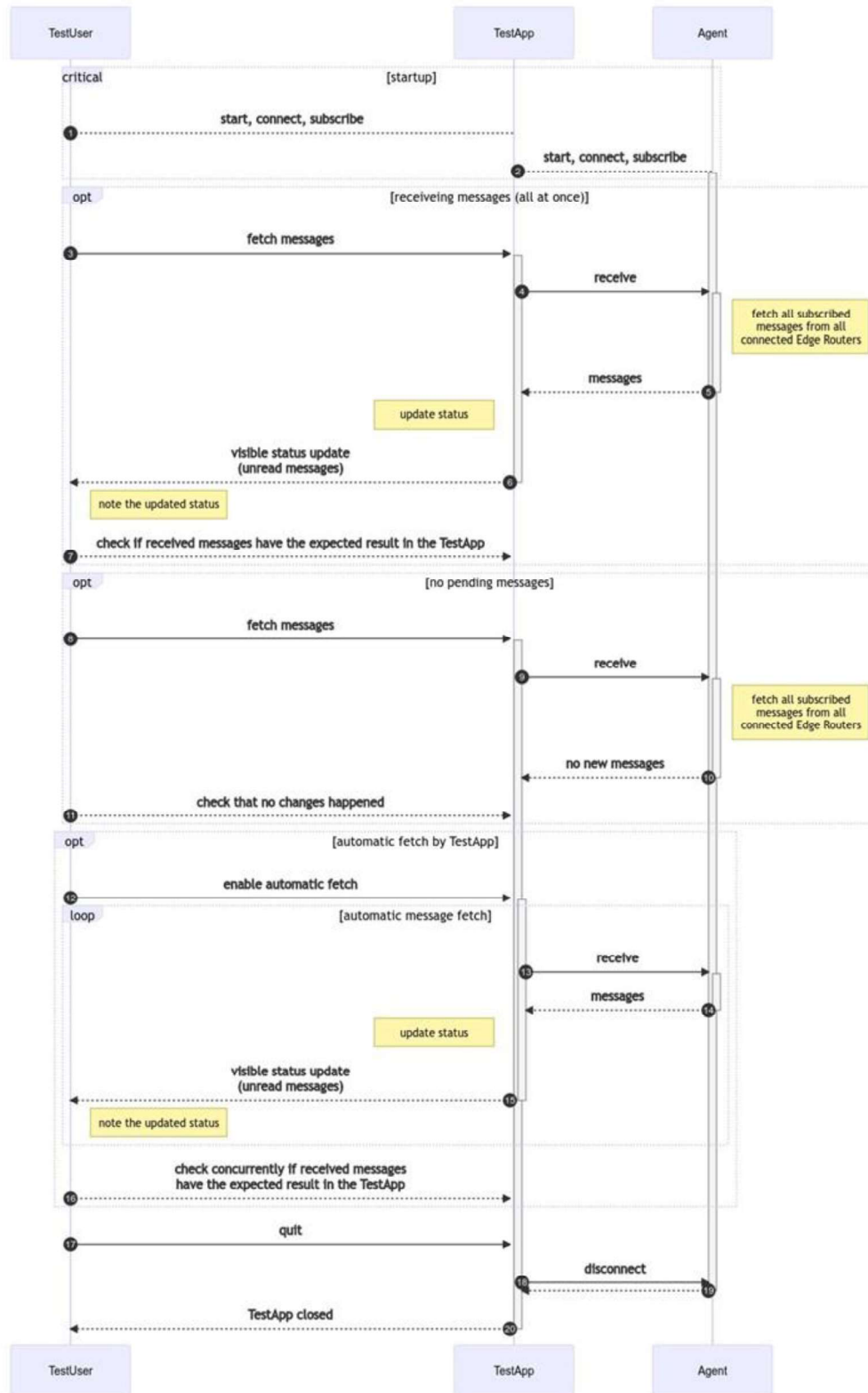
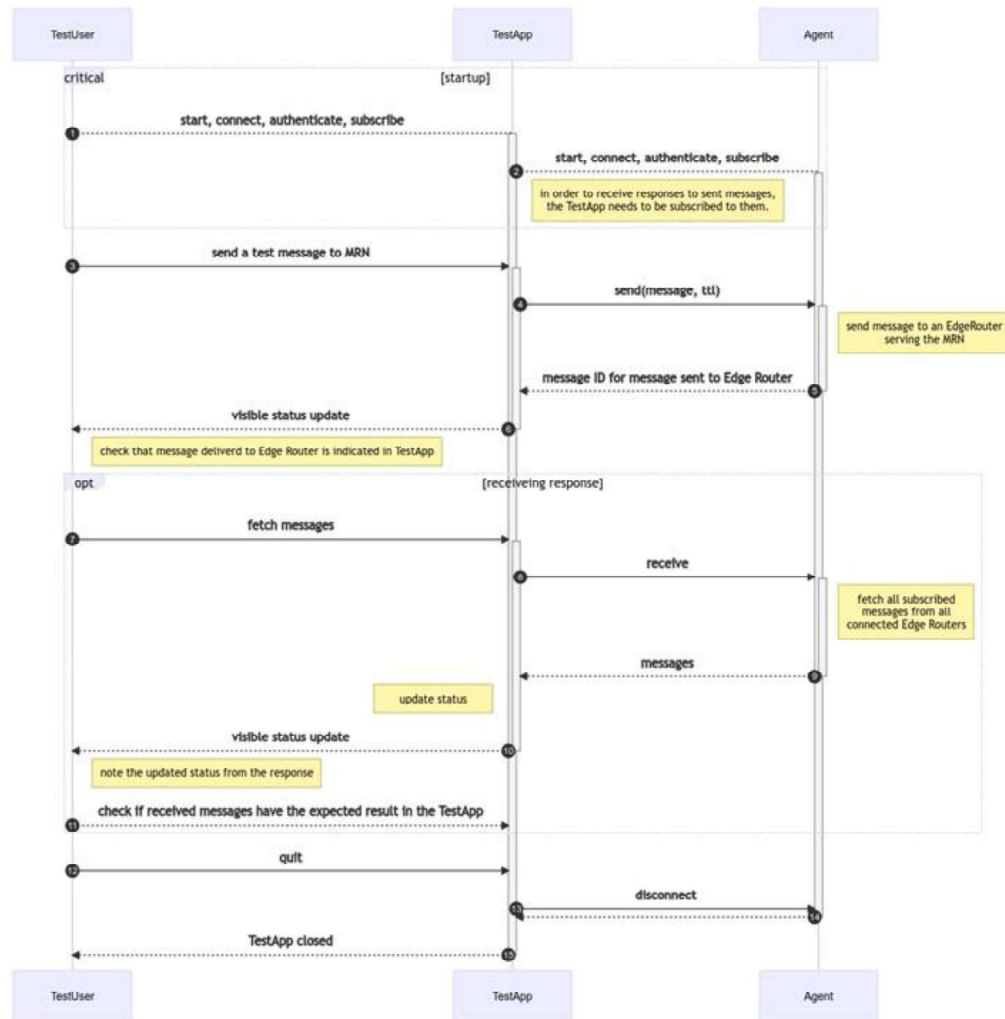


Figure 12 – UML MSC Diagram: MMS Agent receives messages.



**Figure 13 – UML MSC Diagram: authenticated Application sends messages and receives response.**

In the following, each function of the MMS Agent is described in more detail.

### 6.1.1 Discover Edge Routers

The Discover function may provide an alternative method to a statically configured Edge Router address.

If implemented:

1. the Discover function shall find MMS Edge Routers on the configured LAN using the mDNS [6] and DNS-SD [7] protocols,
2. the Discover function shall not accept any arguments, and
3. the Discover function shall return a list with the MRNs of all MMS Edge Routers that are found on the configured LAN.



### 6.1.2 ConnectAnonymously Edge Router

This function shall establish an anonymous connection to a specific MMS Edge Router using secure transport [NOTE:TLS V1.3 ][8] and shall keep it alive until disconnected or lost.

The function shall accept following arguments:

- the MRN of the MMS Edge Router, which may be discovered by the Discover function or known a priori (e.g. by local configuration) by the Application.

The function shall return:

- OK:<reconnection token> if connection to MMS Edge Router could be established, or was already established,
- ERROR if the connection was not possible, i.e. because the MMS Edge Router is not reachable.

If successful, the state of the MMS Agent shall be changed from NOT CONNECTED to CONNECTED, or it shall stay in CONNECTED if it was connected before calling the Connect anonymously function. If successful, the MMS Agent shall store the MRN of the connected MMS Edge Router and its IP address for later use in the other functions. The MMS Agent may store the anonymous reconnection token for a later reconnect.

### 6.1.3 ReconnectAnonymously Edge Router Token

This function shall re-establish an anonymous connection to a specific MMS Edge Router using secure transport [8] and shall keep it alive until disconnected or lost.

Note: the purpose of an Actor reconnecting is to attempt getting messages stored for the MMS Agent in the MMS Edge Router, that were not yet retrieved during disconnected state. See MMS Edge Router.

Prerequisites the function shall check before execution:

- the MMS Agent has been successfully connected anonymously earlier and stored the reconnection token received by the MMS Edge Router.

The function shall accept following arguments:

- the MRN of the MMS Edge Router, which can be discovered by the Discover function or known a priori by the Application,
- the reconnection token as received from the MMS Edge Router in the last successful connect.

The function shall return:

- OK:<reconnection token> if connection to MMS Edge Router could be established, or was already established,
- ERROR if the connection was not possible, i.e. because the MMS Edge Router is not reachable,
- TOKEN ERROR if the MMS Edge Router does not associate the required reconnection to a previous given connection token.

If successful, the state of the MMS Agent is changed from NOT CONNECTED to CONNECTED or AUTHENTICATED, or it stays in CONNECTED/AUTHENTICATED if it was connected/authenticated before calling the Connect function, respectively. If successful, the MMS Agent shall store the MRN of the connected MMS Edge Router and its IP address for later use in the other functions. The MMS Agent shall store the reconnection token and its associated authentication status (anonymous or authenticated) for later reconnect.

#### 6.1.4 ConnectAuthenticated Edge Router

This function shall establish an authenticated connection to a specific MMS Edge Router using secure transport [NOTE:TLS V1.3] [8] and an MRN based MCP certificate. The connection is kept alive until disconnected.

The function shall accept following arguments:

- the MRN of the MMS Edge Router, which can be discovered by the Discover function or known a priori by the Application,
- MRN based MCP certificate.

The function shall return:

- OK:<reconnection token> if the user was successfully authenticated with an MCP certificate on the MMS Edge Router,
- ERROR if the authentication failed,
- CONNECTION FAILURE if connection to the here specified MMS Edge Router is lost during processing of this function.

If successful, the state of the MMS Agent changes from NOT CONNECTED or CONNECTED to AUTHENTICATED, or it stays in AUTHENTICATED if it was authenticated before calling the Authenticate function. The MMS Agent shall store the reconnection token and its associated authentication status (anonymous or authenticated) for later reconnect.

#### 6.1.5 ReconnectAuthenticated Token

The function shall re-establish an authenticated connection to a specific MMS Edge Router and shall keep it alive until disconnected or lost.

Note: the purpose of an Actor reconnecting is to attempt getting messages stored for the MMS Agent in the MMS Edge Router, that were not yet retrieved during disconnected state. See MMS Edge Router.

Prerequisites the function shall check before execution:

- the MMS Agent has been successfully connected authenticated earlier and stored the reconnection token received by the MMS Edge Router.

The function shall accept following arguments:

- the MRN of the MMS Edge Router, which can be discovered by the Discover function or known a priori by the Application,
- reconnection token as received from the MMS Edge Router in the initial authenticated connect.

The function shall return:

- OK:<reconnection token> if connection to MMS Edge Router could be established, or was already established,
- ERROR if the connection was not possible, i.e. because the MMS Edge Router is not reachable,
- TOKEN ERROR if the MMS Edge Router does not associate the required reconnection to a previous given connection token.

If successful, the state of the MMS Agent shall change from NOT CONNECTED to AUTHENTICATED, or it stays in AUTHENTICATED if it was authenticated before calling the Connect authenticated function. If successful, the MMS Agent shall store the MRN of the connected MMS Edge

Router and its IP address for later use in the other functions. The MMS Agent shall store the reconnection token and its associated authentication status for later reconnect.

#### 6.1.6 Status

The function shall return the status of an MMS Agent.

The function shall not accept any arguments.

The function shall return:

- NOT CONNECTED if the MMS Agent is not connected to an MMS Edge Router,
- CONNECTED if the MMS Agent is anonymously connected to an MMS Edge Router,
- AUTHENTICATED if the MMS Agent is authenticated connected with an MMS Edge Router.

Calling the Status function shall not affect the internal state of the MMS Agent.

#### 6.1.7 Query

This function shall return the current information in relation to a query to a connected MMS Edge Router. This may be the MMS Edge Routers connection status, connection type, or other domain specific information.

The function shall accept following arguments:

- a query

The function shall return:

- NOT CONNECTED if not connected to an MMS Edge Router,
- CONNECTION FAILURE if connection to MMS Edge Router is lost during processing of this function.

The Query function shall not change the internal states of the MMS Agent.

#### 6.1.8 Subscribe subject

This function shall subscribe to a subject with the connected MMS Edge Router.

Note: subscription to a subject by an MMS Agent is expected to lead to receiving of messages that match the subject.

Prerequisites the function shall check before execution:

- the MMS Agent is connected to an MMS Edge Router, i.e. the MMS Agent is either in state CONNECTED or AUTHENTICATED.

The function shall accept following arguments:

- a subject to subscribe to as string.

Note: the connected MMS Edge Router is known to the MMS Agent.

The function shall return:

- OK if successfully subscribed to the subject with the MMS Edge Router, either as a result of this action or already before,
- ERROR if the MMS Edge Router does not accept subscriptions to the given subject,
- NOT CONNECTED if the MMS Agent is not connected to an MMS Edge Router,

- CONNECTION FAILURE if connection to MMS Edge Router is lost during processing of this function.

If successful, the state of the MMS Agent shall stay unchanged. If successful, the MMS Agent shall remember the subscription to the subject for later unsubscription or query reference.

#### 6.1.9 Unsubscribe subject

This function shall unsubscribe to a subject with the connected MMS Edge Router.

Prerequisites the function shall check before execution:

- the MMS Agent is connected to an MMS Edge Router, i.e. the MMS Agent is either in state CONNECTED or AUTHENTICATED.

The function shall accept following arguments:

- the subject to unsubscribe as string.

Note: the connected MMS Edge Router is known to the MMS Agent.

The function shall return:

- OK if successful unsubscribed, or if the subject was not subscribed at the MMS Edge Router,
- ERROR if the MMS Agent is not subscribed to the subject,
- NOT CONNECTED if MMS Agent is not connected to an MMS Edge Router,
- CONNECTION FAILURE if connection to MMS Edge Router is lost during processing of this function.

If successful, the connected/authenticated MMS Edge Router shall remove a prior existing subscription by that MMS Agent to the given subject. If successful, the MMS Agent shall remove an earlier remembered subscription to the subject in its own memory.

#### 6.1.10 SubscribeMessages

This function shall subscribe to MRN-addressed messages with an MMS Edge Router.

Prerequisites the function shall check before execution:

- the MMS Agent is authenticated with an MMS Edge Router, i.e. the MMS Agent is in state AUTHENTICATED.

The function shall not accept any arguments.

Note: the MMS Edge Router to which the subscription shall happen is connected and known the MMS Agent. The MRN is part of the earlier call to the Authenticate function.

The function shall return:

- OK if successful,
- ERROR if the MMS Edge Router does not accept delivery of MRN-addressed messages, e.g. if the MMS Agent is not authenticated with the connected MMS Edge Router,
- NOT CONNECTED if there is no connection to the MMS Edge Router,
- CONNECTION FAILURE if connection to MMS Edge Router is lost during processing of this function.

If successful, the MMS Agent shall stay in state AUTHENTICATED and registers for later query that it has subscribed to messages for the Application's MRN.

#### 6.1.11 UnsubscribeMessages

This function shall unsubscribe from MRN-addressed messages with an MMS Edge Router.

Prerequisites the function shall check before execution:

- the MMS Agent shall be connected to an MMS Edge Router, i.e. the MMS Agent is either in State CONNECTED or AUTHENTICATED.

The function shall not accept any arguments.

Note: the MMS Edge Router to which the unsubscription shall happen is connected and known the MMS Agent. The MRN is part of the earlier call to the Authenticate function and known to the MMS Agent.

The function shall return:

- OK if successful,
- ERROR if the MMS Edge Router does not accept delivery of MRN-addressed messages or the MMS Agent is not authenticated,
- NOT CONNECTED if there is no connection to the MMS Edge Router,
- CONNECTION FAILURE if connection to MMS Edge Router is lost during processing of this function.

If successful, the MMS Agent shall stay in its state and registers for later query that it does not receive messages to the Application's MRN.

#### 6.1.12 Send Recipient MRNs

This function shall deliver an MRN-addressed message from the Application to an MMS Edge Router.

Prerequisites the function shall check before execution:

- the MMS Agent is in AUTHENTICATED state.

The function shall accept following arguments:

- time to live (TTL),
- receiving MRN(s),
- binary message content in MMTP format.

The function shall return:

- OK:<unique message reference> if successful,
- ERROR if the MMS Edge Router does not accept delivery of MRN-addressed messages or the MMS Agent is not authenticated,
- NOT CONNECTED if there is no connection to the MMS Edge Router,
- CONNECTION FAILURE if connection to MMS Edge Router is lost during processing of this function.
- MAXIMUM MESSAGE SIZE EXCEEDED if the complete message exceeds the MMTP message size limit.

If successful, the MMS Agent shall stay in the same state AUTHENTICATED. The MMS Agent may store the reference to the message.

Note: The Application shall store the returned unique message reference for later query of the state.

If successful, the MMS Agent shall have delivered the message to the MMS Edge Router for further processing.

#### 6.1.13 Send Subject

This function shall deliver a Subject-cast message from the Application to an MMS Edge Router.

Prerequisites the function shall check before execution:

- the MMS Agent is in AUTHENTICATED state.

The function shall accept following arguments:

- time to live (TTL),
- subject string,
- binary message content in MMTP format.

The function shall return:

- OK:<unique message reference> if successful,
- ERROR if the MMS Edge Router does not accept delivery of Subject-cast messages or the MMS Agent is not authenticated,
- NOT CONNECTED if there is no connection to the MMS Edge Router,
- CONNECTION FAILURE if connection to MMS Edge Router is lost during processing of this function.
- MAXIMUM MESSAGE SIZE EXCEEDED if the complete message exceeds the MMTP message size limit.

If successful, the MMS Agent shall stay in the same state AUTHENTICATED. The MMS Agent may store the reference to the message.

Note: The Application shall store the returned unique message reference for later query of the state.

If successful, the MMS Agent shall have delivered the message to the MMS Edge Router for further processing.

#### 6.1.14 Notify

This function is triggered by receiving a protocol message from the MMS Edge Router to notify new arrived messages.

Prerequisites the function shall check before execution: none.

The function shall accept the following arguments:

- metadata of the unreceived messages.

The function shall return nothing.

The function shall trigger the Edge Router to receive relevant new messages from the Router.

#### 6.1.15 Receive filter

This function shall fetch all messages that are subscribed to and not yet received by the MMS Agent at the connected MMS Edge Router and deliver them to the Application.

Prerequisites the function shall check before execution:

- the MMS Agent is in CONNECTED or AUTHENTICATED state.

The function shall accept following arguments:

- filter to select certain messages to receive and leave the others on the Edge Router.

The function shall return:

- OK:<list of messages> if successful (the list may be empty if no new or filter matching messages were found),
- NOT CONNECTED if there is no connection to the MMS Edge Router,
- CONNECTION FAILURE if connection or authentication to MMS Edge Router is lost during processing of this function.

If successful, the MMS Agent shall stay in the same state. The MMS Agent shall have delivered the messages to the Application, that matched the filter condition, if there were any new.

#### 6.1.16 Disconnect

This function shall permanently disconnect the MMS Agent from an MMS Edge Router.

Prerequisites the function shall check before execution:

- the MMS Agent is connected/authenticated with the MMS Edge Router,
- the MMS Agent may have pending subscriptions on the MMS Edge Router.

The function shall not accept any arguments.

The function shall return:

- OK if successful,
- NOT CONNECTED if there is no connection to the MMS Edge Router,
- CONNECTION FAILURE if connection to MMS Edge Router is lost during processing of this function.

Note: If one or multiple subscriptions exist on the MMS Edge Router, the MMS Edge Router may unsubscribe them and delete all unfetched messages.

If successful, the MMS Agent shall be in state DISCONNECTED. If successful, the MMS Agent shall not accept any reconnect attempt to that connection again.

Note: only new connect authenticated or anonymous shall be accepted by the MMS Agent to the MMS Edge Router once it was disconnected by the disconnect function.

#### 6.1.17 Persistence

After a restart of the MMS Agent, it is the responsibility of the Application to bring the MMS Agent back into the required state for proper operation of the Application and ensure the necessary registrations to subjects and MRN messages is done. The MMS Agent is not required to persist its state across restarts. The Application may use the Status and Query function to check for the current state and subscriptions, respectively.

### 6.2 Functionality of MMS Edge Router

An MMS Edge Router is a special MMS Router which connects one or more MMS Agents with one or more Routers or MMS Edge Routers. An MMS Edge Router shall mutually authenticate with the Routers. An MMS Edge Router shall have one dedicated interface to connect to each type of network.

The MMS Edge Router shall handle authentication and registration of MMS Agents and subscriptions of connected MMS Agents.

If an MMS Edge Router provides a public MMS Agent interface, an MMS Edge Router shall authenticate MMS Agents appropriately, dependent on the connection technology.

An MMS Edge Router may be part of a ship or shore installation.

Store and forward messaging shall be facilitated by following main functional concepts of the MMS Edge Router:

1. buffering of messages for a connection in a queue until it is possible to forward them,
2. forwarding messages based on subject or destination MRN,
3. maintaining time-to-live (TTL) of queued messages, and
4. discarding messages where the TTL has been exceeded.

An MMS Edge Router shall maintain a mapping between the MRN and all Agents that have subscribed to that MRN. Multiple Agents may register on behalf of the same Entity to implement message forwarding, e.g. using different bindings or networks.

An MMS Edge Router shall maintain a mapping between subjects and Agents, it shall for each such subject notify all the Agents that subscribed to the subject.

An MMS Edge router shall have following states:

- **Starting** The MMS Edge Router has been started and shall be performing Startup.
- **Fault** The MMS Edge Router shall enter that state when encountered a fatal condition, and when MMS operations are disabled. No receiving of messages shall be allowed on any interface.
- **Ready** The MMS Edge Router has passed all startup tests and at least one of the configured interfaces initialized, is allowing for MMS Agents to connect and exchange messages. The MMS Edge Router is trying to contact one or multiple Routers as configured.
- **Connected** The MMS Edge Router is connected to at least one Router, is performing exchange with that MMS Router and is allowing for MMS Agents to connect and exchange messages.

The overall functionality of an MMS Edge Router in one of the above states is described below. All functions shall be non-blocking.

- **Startup** Perform tests, checks, and initialize all interfaces.
- **Connect ROUTER.** Connects to another MMS Router in the Router Network.
- **Send MRN(s) subject.** Send message addressed to one or more recipients or to a subject.
- **Fetch.** Get list of available messages at an MMS Router
- **Receive filter.** Receive messages.
- **Subscribe MRN.** Subscribe to receive messages for a certain MRN.
- **Subscribe subject.** Asks an MMS Router to deliver messages to the MMS Edge Router with a specific subject.
- **Shutdown.** Shuts down the MMS Edge Router.



## 6.2.1 General Functionality Concepts

### 6.2.1.1 System Concept

The MMS Edge Router shall:

1. implement the hardware and software requirements provided in IEC 60945 (ship equipment only),
2. provide an interface to exchange and edit local configuration with the administrative users, e.g. through a built-in web interface or file server,
3. provide the means to change all implemented timeouts through the local configuration,
4. provide a user management, at minimum providing two access levels to distinguish:
  - a. administrative users, and
  - b. normal users.
5. provide a default administrative user called “admin”, with a default password that is differing for each produced serial number, and where it is not possible to derive the password from the serial number,
6. provide means to the normal user to identify the internal states by means not requiring tools or equipment that is not part of the default fixed,
7. installation, e.g. through spatially differentiable positioned LEDs with clearly readable labels or a default installation display terminal,
8. provide interfaces through which MMS Agents can connect,
9. provide a certificate storage to authenticate MMS Agents, synchronized with MCP MIR instances at least for revocations once per month,
10. provide means to install certificates that can be used to authenticate MMS Agents,
11. provide means to upload its own certificate used to authenticate with the Router network,
12. provide means to the administrative users to add and remove MMS Agent and own certificates as necessary without requiring tools or equipment that is not part of the default installation, e.g. through a built-in web interface,
13. provide means to normal users to see the revocation states of all certificates and connection state of all MMS Agents without requiring tools or equipment that is not part of the default installation, e.g. through a built-in web interface,
14. have a message storage that is persistent across accidental power outages and restarts of the system,
15. provide means to detect functions that are not performing according to design and restart them accordingly to try to maintain operations
16. have an alerting system that informs users about changes in the states that indicate critical or faulty behavior, or local configuration inconsistencies,
17. have a log system that allows users and administrators to see all relevant events that are required to be logged according to this specification,
18. provide an mDNS service on all local interfaces, making it possible for MMS Agents to be discovered.
19. provide the means to manage the connections of both anonymous and authenticated MMS Agents, ensuring a clear distinction between the two.

### 6.2.1.2 Fraud Detection and Handling

The MMS Edge Router shall protect itself and the MMS network against excessive behavior by at minimum allowing configuration of following limits:

1. total requests per minute from a single MMS Agent: default = 10,
2. total requests per minute to a connected MMS Router: default = 100,
3. total number of subscriptions from a single MMS Agent: default = 5,
4. total number of subscription requests per minute from a single MMS Agent: default 5.

The given default shall be applied to default configuration (after factory reset), other values may be configurable.

In case one of the above limits is exceeded, the RATE EXCEEDED response shall be used.

### 6.2.1.3 MMS Agent Connection Concept

When MMS Agents are connecting to an MMS Edge Router, the MMS Edge Router shall:

1. handle one or multiple connections, where a connection is established over any network (LAN or WAN),
2. handle each MMS Agent connection individually.

### 6.2.1.4 MMS Router Connection Concept

An MMS Edge Router

1. may connect to one or more Routers over any available transport,
2. may monitor MMS Router connection status,
3. shall handle connection selection according to local configuration and connection status.

### 6.2.1.5 Message Exchange Concept

The MMS message exchange on an MMS Edge Router shall include:

1. store and forward of messages to an MMS Router or an MMS Agent,
2. checking authentication of the messages based on MCP certificates,
3. delay of messages until forward is possible,
4. caching of messages,
5. local subject-cast of received messages to relevant connected MMS Agents,
6. filtering of messages; this may include:
  - a. duplicated messages identified by UUID of the message,
  - b. subject of subscription, and
  - c. messages with a limited time until TTL.

### 6.2.1.6 Authentication of MRN-addressed messages

Agents shall authenticate with the MMS Edge Router before they may subscribe with their own MRN to MRN-addressed messages. The MMS Edge Router shall authenticate with MMS Routers.

Note: MMS Agents are not directly authenticated with the Router, but only with the MMS Edge Router. MMS Routers trust MMS Edge Router subscriptions and attempt to deliver messages for all subscribed subjects, connection limitations may require prioritisation.

### 6.2.1.7 Message Sequence Charts

The following non-normative UML message sequence charts may help understanding the MMS Edge Router behavior described in this specification.

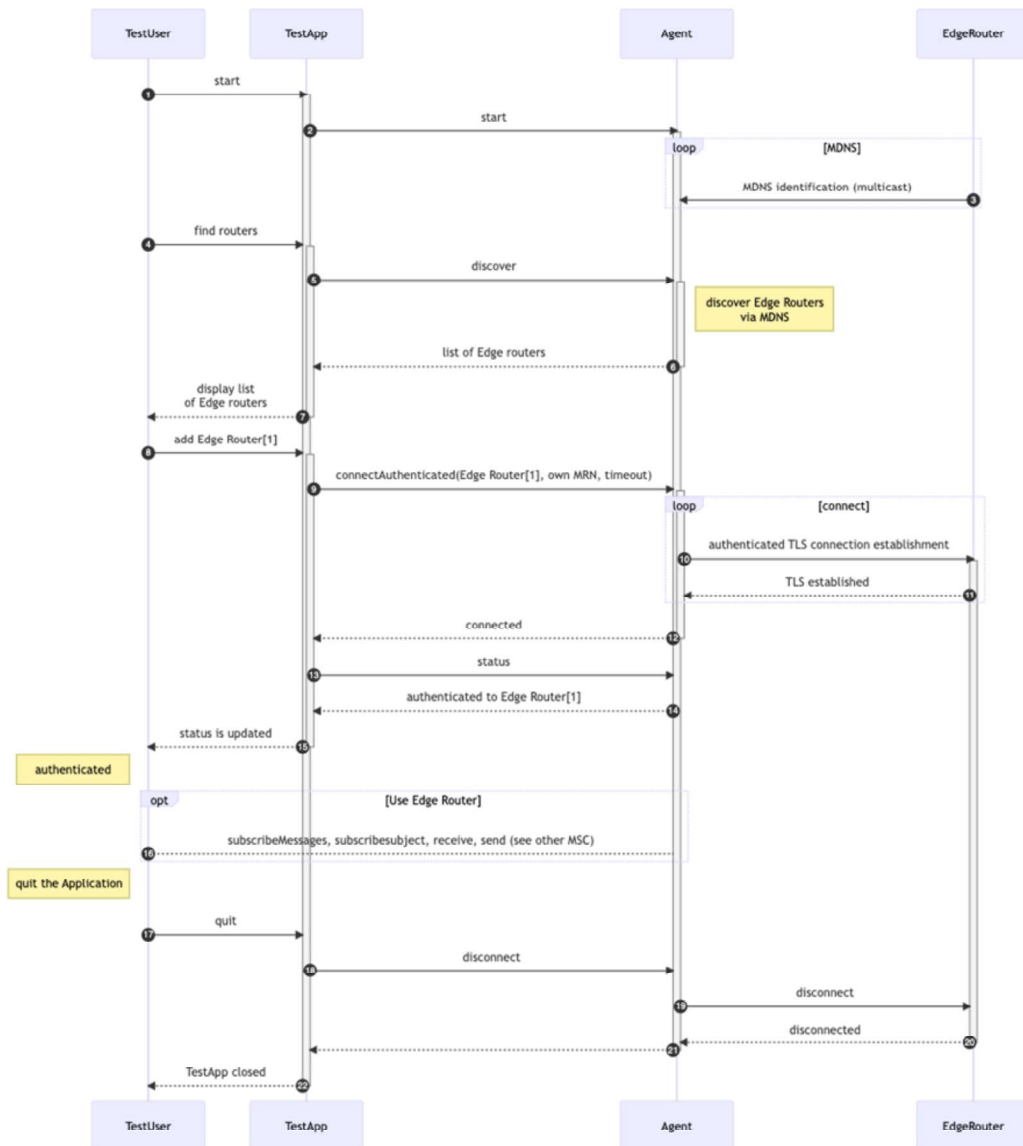


Figure 14 – UML MSC Diagram: MMS Agent connects and authenticates to MMS Edge Router from User/App point of view.

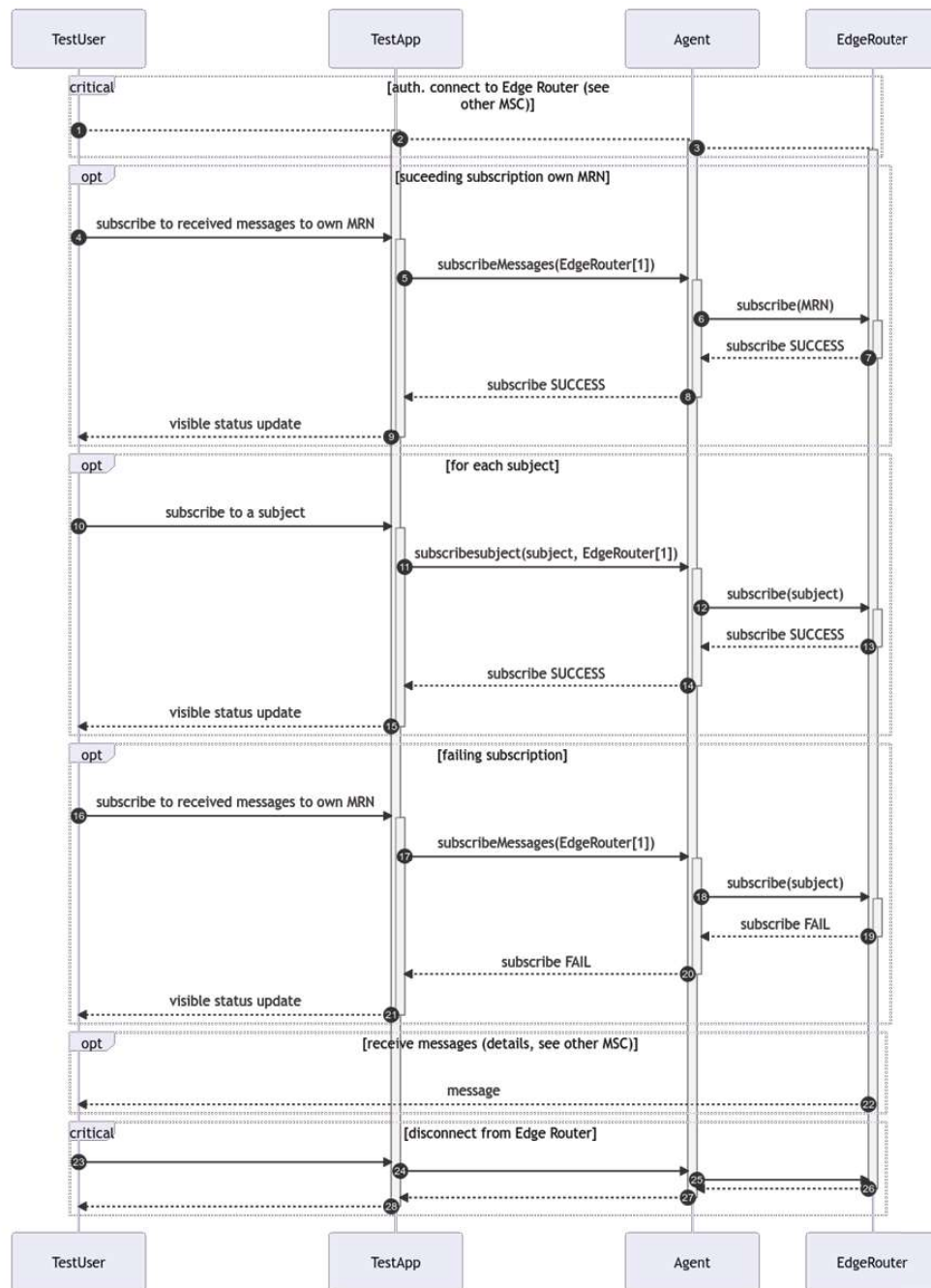


Figure 15 – UML MSC Diagram: authenticated MMS Agent subscribes to messages at an MMS Edge Router.

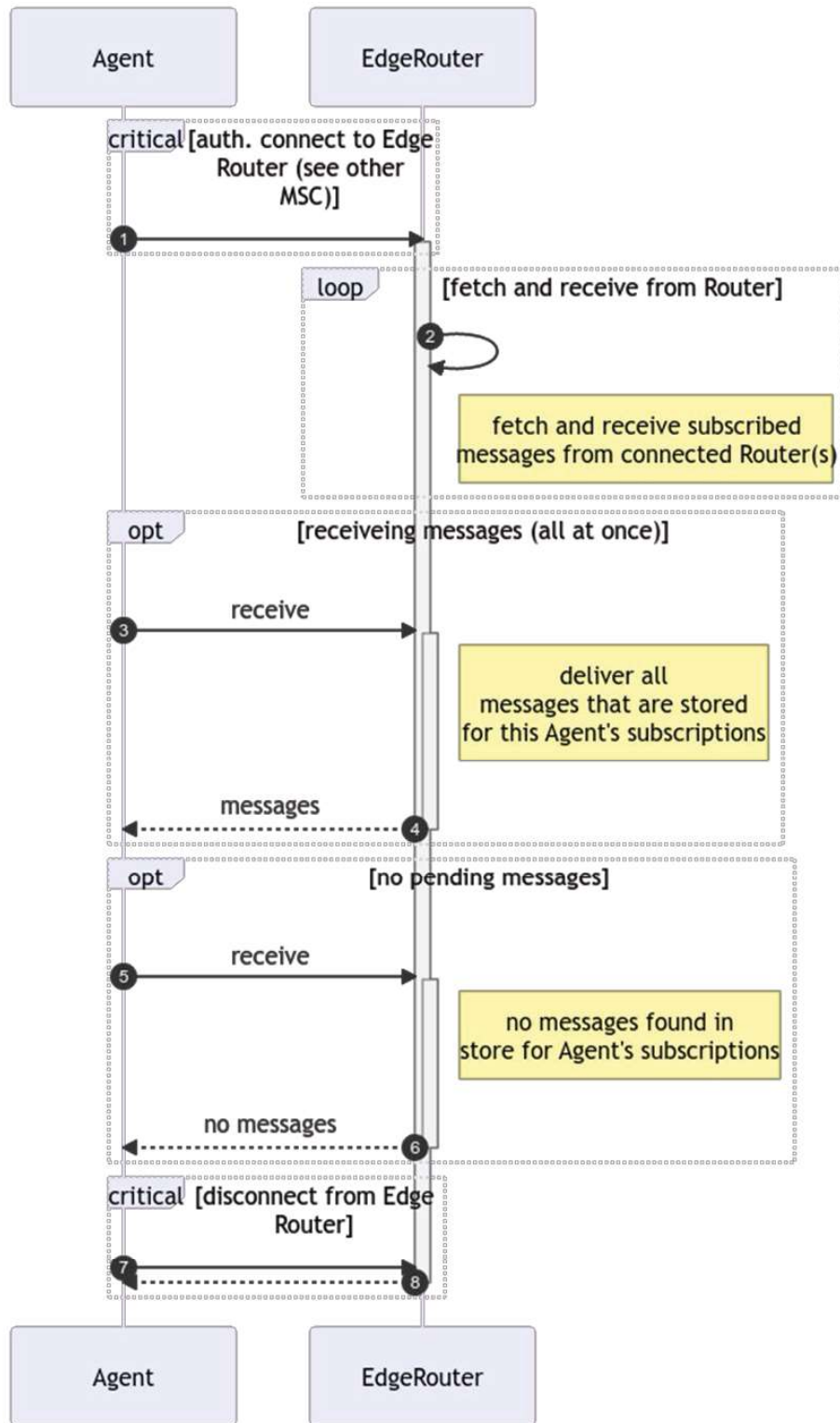


Figure 16 – UML MSC Diagram: MMS Agent receives messages from an MMS Edge Router.

### 6.2.2 Specific Functions

Functions noted in this section as “internal functions” shall not be available to external interfaces, while all other functions are available to MMS Agents.

Any of the following functions may encounter error conditions that shall be returned to the calling Agent using an ERROR response with a textual description of the type and reason for the error for analysis.

#### 6.2.2.1 Startup

This internal MMS Edge Router function shall start the MMS Edge Router interfaces and keep them alive for the entire time the MMS Edge Router is switched on.

This internal MMS Edge Router function shall continue operation, except if internal faults are detected by the BIST.

Prerequisites the function shall check before execution:

- the MMS Edge Router is connected to a power supply and is switched on.

The function shall not accept any arguments.

When executed, this function shall perform the following operations “startup procedure”:

1. run a built-in self test BIST to evaluate if all necessary hardware is operating as required for proper operation as described in this standard, classify problems into categories Warning, Critical and Fatal, and make these states known to the user by applicable means,
2. run a consistency check of the local configuration, classifying all problems into categories Warning, Critical and Fatal, and make the result of the check known to the user by applicable means,
3. decide if the first two steps allow for either:
  - a. normal operation as configured,
  - b. reduced operation limiting some configured functionality, or
  - c. no operation, indicated as fault state.
4. start all interfaces as configured,
5. start self-monitoring of all interfaces,
6. start the mDNS service to allow MMS Agents to discover the MMS Edge Router,
7. start all processes to handle the internal functions of the MMS Edge Router described in this specification,
8. start self-monitoring of all internal functions, with the purpose to
  - a. identify inconsistent states and behavior of functions, and
  - b. log and indicate such inconsistencies for momentary and later analysis by users and operators, and
  - c. restart processes and interfaces, or the system, in case that is indicated by the severity of an inconsistency,
9. start the router connect function.

The function shall return nothing.

If successful, the MMS Edge Router shall end in the operational state, performing all the other functions as specified in this specification.

#### **6.2.2.2 Built In Self Test**

This internal function is part of the Startup procedure and shall perform a self test.

It also shall be possible for any user to request the MMS Edge Router to run a BIST any time.

Execution of the BIST may not affect the message storage, no messages may be added or lost due to execution of the test.

#### **6.2.2.3 Configuration Check**

This internal function is part of the Startup procedure and shall perform a local configuration check.

The local configuration check function shall also be automatically called by the administrative interface whenever a local configuration parameter has been changed, giving direct feedback to the user after changing the local configuration.

#### **6.2.2.4 MMS RouterLookup**

Edge Routers shall lookup MMS Routers according to local configuration.

Routers may be discoverable by different means depending on the WAN connection type:

- for IP connections: DNS lookup, or
- for VDES connections: broadcast of shore MMS Edge Router MMSI.

#### **6.2.2.5 Connect ROUTER (internal)**

This internal MMS Edge Router function shall establish connection with the configured Routers and manage the connection as long as the MMS Edge Router is powered on.

#### **6.2.2.6 Disconnect ROUTER (internal)**

This internal MMS Edge Router function shall disconnect from an MMS Router. The MMS Edge Router shall:

1. send a disconnect message to the MMS Router, which is:
  - a. optionally containing a transfer MMS Router, taking over the MMS Edge Router's subscriptions, and
  - b. taking into account local configuration.

#### **6.2.2.7 Anonymous Connect (from MMS Agent)**

This function is requested by MMS Agents that want to connect to the MMS Edge Router. The function shall perform:

1. setup a connection to the requesting MMS Agent, and
2. maintain the connection to the connected MMS Agent until the MMS Agent disconnects.

#### **6.2.2.8 Authenticated Connect (from MMS Agent)**

This function is requested by MMS Agents that want to connect to the MMS Edge Router. The function shall perform:

1. setup and authenticate a connection to the requesting MMS Agent, and
2. maintain the connection to the connected MMS Agent until the MMS Agent disconnects.

**6.2.2.9 Send [MRNs subject] (from MMS Agent)**

This function is requested by an MMS Agent sending a message. The MMS Edge Router shall:

1. check that the requesting MMS Agent is authenticated,
2. check that the message is correctly authenticated by the MMS Agent's MCP certificate,
3. apply local forwarding rules according to local configuration, and
4. forward the message to:
  - connected MMS Routers that have subscribed to that message subject or MRNs, and
  - connected local MMS Agents that have subscribed to that message subject or MRNs.

This function shall return:

- OK if successful,
- ERROR if the MMS Edge Router does not accept delivery of MRN-addressed messages or the MMS Agent is not authenticated,
- RATE EXCEEDED: text if the Agent exceeded a rate limit, text describing which limit is exceeded, and its value,
- MAXIMUM MESSAGE SIZE EXCEEDED if the complete message exceeds the MMTP message size limit.

If successful, the MMS Edge Router shall have queued the message for transport to the MMS Router.

**6.2.2.10 Notify (to MMS Agent)**

This function shall be used by the MMS Edge Router to notify Agents of new messages.

Prerequisites the function shall check before execution:

- connected to the Agent.

The function shall accept the following arguments:

- list of new messages for this Agent arrived since the last notify sent to this Agent.

The function shall return nothing.

If successful, the function has notified the Agent about the newly arrived messages, and the Agent will actively poll these messages from the Edge Router, if relevant.

**6.2.2.11 Notify (from MMS Router)**

This function is triggered by receiving a protocol message from the MMS Router to notify new arrived messages.

Prerequisites the function shall check before execution: none.

The function shall accept the following arguments:

- metadata of unreceived messages.

The function shall return nothing.

The function shall trigger the Edge Router to receive relevant new messages from the Router.



#### 6.2.2.12 Fetch (from MMS Agent)

This function is requested by an MMS Agent fetching the list of unreceived message metadata for the requesting MMS Agent. The MMS Edge Router shall:

1. check that the requesting MMS Agent is authenticated, and
2. reply to the requesting MMS Agent delivering the metadata of the unreceived messages for this MMS Agent.

The function shall return:

- OK:<list of message metadata> if successful (the list may be empty if no new messages were found),
- RATE EXCEEDED: text if the Agent exceeded a rate limit, text describing which limit is exceeded, and its value.

If successful, the MMS Edge Router shall stay in the same state.

#### 6.2.2.13 Receive filter (from MMS Agent)

This function is requested by an MMS Agent to receive the filtered messages. The MMS Edge Router shall:

1. check that the requesting MMS Agent is authenticated,
2. apply the requested filter to the stored messages for this MMS Agent, and
3. return out of the stored messages for this MMS Agent the filtered ones.

The function shall return:

- OK<list of messages> if successful (the list may be empty if no new messages were found),
- RATE EXCEEDED: text if the Agent exceeded a rate limit, text describing which limit is exceeded, and its value.

If successful, the MMS Edge Router shall have cleared addressed messages that are successfully delivered to all receiving agents.

#### 6.2.2.14 Fetch (to MMS Router)

This internal MMS Edge Router function is invoked by the MMS Edge Router to fetch the list of unreceived message metadata for the requesting MMS Edge Router from the MMS Router. For each connected MMS Router, on intervals given in the MMS Edge Router local configuration, the MMS Edge Router shall:

1. send a fetch request to the connected MMS Router,
2. parse the response from the connected MMS Router, and
3. act on the received list based on local configuration policies.

This function shall return nothing.

If successful, the MMS Edge Router shall have acted on the received list based on local configuration policies.

#### 6.2.2.15 Receive filter (to MMS Router)

This internal MMS Edge Router function is invoked by the MMS Edge Router. For each connected MMS Router, on intervals or based on events given in the MMS Edge Router local configuration, the MMS Edge Router shall:

1. generate a filter based on the MMS Edge Router local configuration and/or received fetch responses,
2. send a receive request to the connected MMS Router,
3. parse the response with zero or more messages, and
4. act on the messages according to local configuration, which shall include as a minimum the possibility to:
  - store and forward received messages to connected MMS Agents that have subscribed to the message MRN or subject, and
  - storage of subject-cast messages until TTL.

This function shall return nothing.

If successful, the MMS Edge Router shall have acted on the received list based on local configuration policies.

#### **6.2.2.16 Subscribe (MRN-addressed messages to MMS Agent)**

This function is requested by an MMS Agent to subscribe to messages addressed to the requesting MMS Agents' own MRN. The MMS Edge Router shall:

1. check that the requesting MMS Agent is authenticated,
2. check if the MMS Edge Router already has subscribed to that MRN,
3. decide subscription actions according to local configuration and status of current MRN subscriptions,
4. send decided subscribe requests for this MRN to connected MMS Routers, and
5. store the subscription status for that MRN and requesting MMS Agent according to the above decision.

This function shall return:

- OK if successful,
- RATE EXCEEDED: text if the Agent exceeded a rate limit, text describing which limit is exceeded, and its value,
- ERROR if the MMS Edge Router does not accept delivery of MRN-addressed messages, e.g. if the MMS Agent is not authenticated with the MMS Edge Router.

If successful, the MMS Edge Router has updated the subscription status for that MRN and requesting MMS Agent.

#### **6.2.2.17 Unsubscribe (MRN-addressed messages to MMS Agent)**

This function is requested by an MMS Agent to unsubscribe to messages addressed to the requesting MMS Agents' own MRN. The MMS Edge Router shall:

1. check that the requesting MMS Agent is authenticated,
2. decide unsubscription actions according to local configuration and status of current MRN subscriptions,
3. send decided unsubscribe requests for this MRN to connected MMS Routers, and
4. update the stored subscription status according to the above decision.

This function shall return:

- OK if successful,
- RATE EXCEEDED: text if the Agent exceeded a rate limit, text describing which limit is exceeded, and its value,
- ERROR if the MMS Agent was not subscribed to MRN-addressed messages or is not authenticated with the MMS Edge Router.

If successful, the MMS Edge Router has updated the stored subscription status.

#### **6.2.2.18 Subscribe subject (from MMS Agent)**

This function is requested by an MMS Agent to subscribe to subject-cast messages. The MMS Edge Router shall:

1. check if the MMS Edge Router already has subscribed to that subject,
2. decide subscription actions according to local configuration and status of current subject subscriptions,
3. send decided subscribe requests for this subject to current and future connected MMS Routers, and
4. store the subscription status for that subject and requesting MMS Agent according to the above decision.

This function shall return:

- OK if successful,
- RATE EXCEEDED: text if the Agent exceeded a rate limit, text describing which limit is exceeded, and its value.

If successful, the MMS Edge Router has updated the subscription status for that subject and requesting MMS Agent.

#### **6.2.2.19 Unsubscribe subject (from MMS Agent)**

This function is requested by an MMS Agent to unsubscribe to subject-cast messages. The MMS Edge Router shall:

1. decide unsubscription actions according to local configuration and status of current subject subscriptions,
2. send decided unsubscribe requests for this subject to connected MMS Routers, and
3. update the stored subscription status according to the above decision.

This function shall return:

- OK if successful,
- RATE EXCEEDED: text if the Agent exceeded a rate limit, text describing which limit is exceeded, and its value,
- ERROR if the Agent was not subscribed to the given subject.

If successful, the MMS Edge Router has updated the stored subscription status.

#### **6.2.2.20 Query (from MMS Agent)**

This function is requested by an MMS Agent to query on MMS Router connection status of the MMS Edge Router. The MMS Edge Router shall:

1. parse the query, and
2. return the queried status information to the requesting MMS Agent.

This function shall return:

- OK:status if successful,
- RATE EXCEEDED: text if the Agent exceeded a rate limit, text describing which limit is exceeded, and its value,
- ERROR if the required status does not exist.

The MMS Edge Router internal states are not changed by this function.

#### **6.2.2.21 Disconnect (from MMS Agent)**

This function is requested by an MMS Agent that is disconnecting from the MMS Edge Router. The MMS Edge Router shall:

1. check subscription status for the requesting MMS Agent,
2. unsubscribe MRN-addressed messages according to the unsubscribe function descriptions above,
3. for each subscribed subject by the requesting MMS Agent, perform the actions as described in function unsubscribe subject above,
4. remove all relevant states for the requesting MMS Agent, which include at least:
  - a. stored messages,
  - b. stored subscription states, and
  - c. stored connection states,
5. close the connection to the requesting MMS Agent.

This function shall return:

- OK if successful,
- RATE EXCEEDED: text if the Agent exceeded a rate limit, text describing which limit is exceeded, and its value,
- ERROR if the MMS Agent was not connected.

If successful, the disconnecting MMS Agent is disconnected and all its subjects unsubscribed in the MMS Edge Router.

#### **6.2.2.22 Shutdown (internal)**

This internal MMS Edge Router function shall:

1. disconnect from all MMS Agents as described in the disconnect from MMS Agent section above,
2. disconnect from all connected MMS Routers according to the Disconnect MMS Router function description above,
3. purge all internal MMS Edge Router states,
4. purge all stored subject-cast messages, and
5. shut down the MMS Edge Router operations.

### 6.3 Functionality of MMS Router

An MMS Router stores and forwards messages with the goal to establish communication between two or multiple Actors in the system. In practice, an MMS Router maintains connections between MMS Routers and with MMS Edge Routers.

An MMS Router shall have:

1. An identity used to authenticate against other components in the system,
2. functionality for store and forward of messages,
3. a list of subscriptions,
4. a routing table of other MMS Routers,
5. a set of local configuration parameters to control its operations,
6. connections to MMS Edge Routers, providing routes to MMS Agents, and
7. connections to other MMS Routers, providing routes to MMS Agents via MMS Edge Routers, see 1.

An MMS Router shall perform:

1. authentication of MMS Edge Routers,
2. registration of MMS Edge Routers and Routers,
3. de-registration of MMS Edge Routers and Routers,
4. reception of messages from Edge Routers and other MMS Routers,
5. storage of messages to subscribed MMS Edge Routers that have no route at this time or where the connection is temporarily down,
6. deletion of messages beyond TTL,
7. forwarding of messages when routes become available,
8. subscription handling, [future: 1. transfer of stored subscriptions and queued messages to another MMS Router, if requested, and]
9. housekeeping.

Note: After a restart, an MMS Router is not required to perform any form of recovery of stored messages, routes and trust relations, because it handles the MMTP that does not give delivery guarantees. If delivery guarantees are required, the SMMP shall be used by the Actor, providing MMS Agent functionality ensuring delivery guarantees.

#### 6.3.1 Interface to MMS Edge Routers

An MMS Router shall provide the following functions to MMS Edge Routers.

##### 6.3.1.1 Authenticated Connect from MMS Edge Router

This function is requested by MMS Edge Routers that want to connect to the MMS Router. The Router shall:

1. setup and authenticate a connection to the requesting MMS Edge Router, and
2. maintain the connection to the connected MMS Edge Router until the MMS Edge Router disconnects.

### 6.3.1.2 Disconnect ROUTER

This function is requested by MMS Edge Routers that want to disconnect from an MMS Router. The MMS Router shall:

1. check authentication of the requesting MMS Edge Router,
2. unsubscribe on the MMS Router Network from the subjects and MRNs that were unique for the requesting MMS Edge Router, and
3. in case the optional transfer MMS Router is provided in the disconnect request:
  - a. transfer all subscriptions to the new transfer MMS Router,
  - b. transfer all messages that were stored for the requesting MMS Edge Router to the new transfer MMS Router,
  - c. taking into account local configuration,

### 6.3.1.3 Send [MRN subject]

This function is requested by an MMS Edge Router sending a message. The Router shall:

1. check that the requesting MMS Edge Router is authenticated,
2. check that subject-cast messages are correctly authenticated by the MMS Agent's MCP certificate,
3. apply local forwarding rules according to local configuration, and
4. forward the message to:
  - connected MMS Routers according to routing rules, and
  - connected MMS Edge Routers that have subscribed to that message subject or MRN.

### 6.3.1.4 Fetch (from MMS Edge Router)

This function is requested by an MMS Edge Router fetching the list of stored messages for the requesting MMS Edge Router. The Router shall:

1. check that the requesting MMS Edge Router is authenticated, and
2. reply to the requesting MMS Edge Router delivering a list of messages that were stored for this MMS Edge Router.

### 6.3.1.5 Receive filter (from MMS Edge Router)

This function is requested by an MMS Edge Router to receive the filtered messages. The Router shall:

1. check that the requesting MMS Edge Router is authenticated,
2. apply the requested filter to the stored messages for this MMS Edge Router, and
3. return out of the stored messages for this MMS Edge Router the filtered ones.

### 6.3.1.6 Subscribe [MRN subject]

This function is requested by an MMS Edge Router to subscribe to subject-cast or MRN-addressed messages. The Router shall:

1. check if the MMS Edge Router already has subscribed to that subject or MRN,
2. decide subscription actions according to local configuration and status of current subject subscriptions,

3. submit decided subscribes to the MMS Router Network, and
4. store the subscription status for that subject or MRN and requesting MMS Edge Router according to the above decision.

#### 6.3.1.7 Unsubscribe [MRN subject]

This function is requested by an MMS Edge Router to unsubscribe to subject-cast or MRN-addressed messages. The Router shall:

1. decide unsubscription actions according to local configuration and status of current subject subscriptions,
2. submit decided unsubscribe requests for this subject to the MMS Router Network, and
3. update the stored subscription status according to the above decision.

#### 6.3.1.8 Notify (to MMS Edge Router)

This function shall be used by the MMS Router to notify MMS Edge Routers of new messages.

Prerequisites the function shall check before execution:

- connected to the MMS Edge Router.

The function shall accept the following arguments:

- list of new messages for this Edge Router arrived since the last notify sent to this Edge Router.

The function shall return nothing.

If successful, the function has notified the Edge Router about the newly arrived messages, and the Edge Router will actively poll these messages from the Router, if relevant.

### 6.3.2 Routing Network Interface

#### 6.3.2.1 Connect to MMS Router Network

This internal function connects an MMS Router to an existing MMS Router Network. The Router shall:

1. connect to at least one other Router that is known to already be in the Router Network,
2. bootstrap routing table with routing information received from connected Routers,
3. query and connect to the  $k$  nearest Routers that advertise the route  $r$ , where the values of  $k$  and  $r$  are set to reasonable defaults,
4. update routing table with newly discovered and connected Routers,
5. advertise the route  $r$  to the network.

#### 6.3.2.2 Maintenance of Routing Table

This internal function shall be run by an MMS Router at a configured interval to do maintenance of the routing table. The Router shall:

1. query and connect to the  $k$  nearest Routers that advertise the route  $r$ , where the values of  $k$  and  $r$  are set to reasonable defaults,
2. update routing table with newly discovered and connected Routers,
3. advertise the route  $r$  to the network.

#### 6.3.2.3 **Subscribe [MRN subject]**

This function advertises the subscription of messages for a given MRN or subject in the MMS Router Network. The Router shall:

1. advertise the wish to receive messages published to the given MRN or subject in the MMS Router Network.

#### 6.3.2.4 **Unsubscribe [MRN subject]**

This function advertises the unsubscription of messages for a given MRN or subject in the MMS Router Network. The Router shall:

1. advertise the wish to no longer receive messages published to the given MRN or subject in the MMS Router Network.

#### 6.3.2.5 **Publish Message to [MRN subject]**

This function publishes a message for a given MRN or subject to the MMS Router Network. The Router shall:

1. publish the message in the MMS Router Network to Routers that are subscribing to the given MRN or subject.

#### 6.3.2.6 **Receive Message Published to [MRN subject]**

This function receives a message published to an MRN or subject that the Router has previously subscribed to. The Router shall:

1. receive the published message from the MMS Router Network,
2. store the message for connected Edge Routers that have previously subscribed to the MRN or subject of the message.

#### 6.3.2.7 **Housekeeping**

An MMS Router shall regularly:

1. remove sessions of Edge Routers that were not seen for more than 48 hours,
2. delete stored messages where the expiration time has been exceeded,
3. ...

### 6.4 **Functionality of MMS Router Network**

An MMS Router Network is defined as a set of MMS Routers that are interconnected in order to serve routing of messages based on destination MRNs and subject subscriptions.

### 6.5 **Functionality of a SMMP Client**

A SMMP Client enables an actor to send and receive SMMP Messages over MMTP. The SMMP Client interfaces with the MMS through an authenticated MMS Agent.

A SMMP Client shall have the following non-blocking functions:

- **EstablishSession Remote SMMP Client.** A SMMP Client may attempt to establish a SMMP session with a remote SMMP Client by performing a handshake.
- **Send SMMP Message.** When the MMS Agent used by the SMMP Client is in a connected state and at least one SMMP session has been established, the SMMP Client may send SMMP messages.
- **SegmentMessage.** When the SMMP Client is used to send a large message, this function shall be used to segment it into multiple SMMP messages.



- **AssembleMessage.** When the SMMP Client receives SMMP messages subject to segmentation, this function shall be used to reconstruct the original message.
- **TerminateSession Remote SMMP Client.** A SMMP Client shall end a SMMP session by the use of this function.

#### 6.5.1 EstablishSession Remote SMMP Client

This function shall establish a SMMP session with a Remote SMMP Client and keep it alive until terminated or lost.

Prerequisites the function shall check before execution:

- the MMS Agent used by the SMMP Client is in an AUTHENTICATED state

The function shall accept the following arguments:

- the MRN of a Remote SMMP Client
- a list of guarantees requested for the SMMP session

The function shall return:

- OK:<session guarantees> if a SMMP Session could be established with the Remote SMMP Client.
- ERROR if it was not possible to establish a SMMP Session with the Remote SMMP Client.

The MMS Client shall store the MRN of the Remote SMMP Client along with a list of the guarantees agreed for the session. If confidentiality is agreed, the MMS Client shall store the agreed session key.

#### 6.5.2 Send SMMP Message

This function shall deliver a single SMMP message to a Remote SMMP Client with whom a SMMP session has been established.

Prerequisites the function shall check before execution:

- the MMS Agent used by the SMMP Client is in an AUTHENTICATED state

The function shall accept the following arguments:

- receiving MRN,
- SMMP Message

The function shall return:

- OK:<smmp message reference> if successful
- ERROR if the MMS Agent used by the SMMP Client reports an error.
- NO SESSION if no SMMP session exists between the SMMP Client and the Remote SMMP Client.

The SMMP Client shall store the reference to the message when the session requires non-repudiation or delivery guarantee.

#### 6.5.3 SegmentMessage

This function shall segment a large message into multiple SMMP messages. The header of each SMMP Message should hold a 0-indexed *blockNum* indicating which segment in sequence the SMMP Message contains. The binary message content shall be segmented such that the first chunk of bytes

is assigned *blockNum 0*. The header of each SMMP Message should also hold a *totalBlocks* property indicating the total number of message segments.

The function shall accept the following arguments:

- receiving MRN
- binary message content

This function shall return:

- OK<list of SMMP messages> if successful.
- ERROR if the message could not be segmented.

If successful, the SMMP Client shall store the returned list of SMMP messages until they have been sent. The list may contain only a single entry if no segmentation was necessary.

#### 6.5.4 AssembleMessage

This function shall assemble a list of SMMP messages to the original message.

The function shall accept the following arguments:

- A list of SMMP messages that are the segments of a single message. All SMMP messages in the list should refer to the same *smmp uuid*.

The function shall return:

- OK if successful
- ERROR if the original message could not be reconstructed due to missing segments.

#### 6.5.5 TerminateSession Remote SMMP Client

This function shall permanently terminate a SMMP session between two SMMP Clients. Prerequisites the function shall check before execution:

- the MMS Agent used by the SMMP Client is in an AUTHENTICATED state

The function shall accept the following arguments:

- the MRN of a Remote SMMP Client

The function shall return:

- OK if successful,
- NO SESSION if no SMMP session exists between the SMMP Client and the Remote SMMP Client.
- ERROR if the MMS Agent used by the SMMP Client reports an error.

## 7 The MMS Transfer Protocol

### 7.1 Overview (informational)

The Maritime Messaging Transfer Protocol (MMTP) is the transfer protocol between MMS Agents via MMS Edge Routers and MMS Routers. This protocol handles

- registration of agents based on MCP-MRNs,
- authenticated message transfer (send/receive), and

- message subscriptions based on subjects.

Senders are identified by authenticated MCP-MRNs. Recipients of MRN-addressed messages are specified using MCP-MRNs. Senders and Recipients of the MMTP are agents. The MCP-MRN that defines these agents, however, comes from the Actors as these are needed for authentication. Multicast messages are identified with a subject-string.

## 7.2 Requirements

The MMTP shall provide a means of transport for sending and receiving protocol messages between MMS Agents via MMS Edge Routers and MMS Routers.

This chapter specifies the particular use of that transport, i.e. a *binding*.

The MMS Transfer protocol shall:

- allow for unsolicited transmission of protocol messages,
- ensure protocol message integrity and authenticity,
- enforce the proper processing order of protocol messages.

Unsolicited transmission of protocol messages shall allow for an MMS Edge Router to notify an MMS Agent of new messages.

Protocol message integrity and authenticity shall be ensured by specifying how to use the transport, if that transport provides integrity or authenticity; and if needed specify that protocol messages are *signed*. If a binding requires that protocol messages are signed, it is RECOMMENDED that messages are signed as specified in this chapter.

Bindings that each Router shall support are specified in 10.

## 7.3 Definitions

All messages listed here are defined in protobuf format [9] prefixed with

syntax = "proto3";

The complete protobuf definition of MMTP can be found in Annex H.

### 7.3.1 MMTP messages

Each MMTP message shall be categorized either to be a Protocol Message or a Response Message to a Protocol Message.

MMTP messages shall not exceed a maximum size of 50 KiB.

The following protobuf code does implement the required normative structure:

```
message MmtpMessage {
  MsgType msgType = 1;
  string uuid = 2;
  oneof body {
    ProtocolMessage protocolMessage = 3;
    ResponseMessage responseMessage = 4;
  }
}
```

### 7.3.2 MMTP Message Types

Each message in MMTP shall contain a *msgType* field of type enum with following different value.

The following protobuf code does implement the required normative structure:

```
enum MsgType {
  UNSPECIFIED_MESSAGE = 0;
  PROTOCOL_MESSAGE = 1;
  RESPONSE_MESSAGE = 2;
}
```

### 7.3.3 MMTP Request Message Types

MMTP shall provide the following protocol request messages:

1. *Subscribe*,
2. *Unsubscribe*,
3. *Send*,
4. *Receive*,
5. *Fetch*,
6. *Disconnect*,
7. *Connect*, and
8. *Notify*.

to implement a complete MMTP implementation.

The following protobuf code does implement the required normative structure:

```
enum ProtocolMessageTypes {
  UNSPECIFIED = 0;
  SUBSCRIBE_MESSAGE = 1;
  UNSUBSCRIBE_MESSAGE = 2;
  SEND_MESSAGE = 3;
  RECEIVE_MESSAGE = 4;
  FETCH_MESSAGE = 5;
  DISCONNECT_MESSAGE = 6;
  CONNECT_MESSAGE = 7;
  NOTIFY_MESSAGE = 8;
}
```

### 7.3.4 MMTP Response Message Types

MMTP shall provide a response message containing:

1. a UUID reference to the original message,
2. the response,
3. an optional reason text,
4. zero or multiple message metadata or zero or multiple message content, and
5. zero or one reconnect token, containing an UUID according to [10].

The following protobuf code does implement the required normative structure:

```
message ResponseMessage {
  string responseToUuid = 1;
  ResponseEnum response = 2;
  optional string reasonText = 3;
  repeated MessageMetadata messageMetadata = 4;
  repeated MessageContent messageContent = 5;
```

```

optional string reconnectToken = 6;
}

using

message MessageMetadata {
    string uuid = 1;
    ApplicationMessageHeader header = 2;
}

or

message MessageContent {
    string uuid = 1;
    ApplicationMessage msg = 2;
}

and

enum ResponseEnum {
    UNSPECIFIED_RESPONSE = 0;
    GOOD = 1;
    ERROR = 2;
}

```

### 7.3.5 MRN

All MRN references in this protocol definition shall comply with MCP MRN [5], which is a subdomain of MRN [11].

MRNs used in MMS are recommended to be no longer than 100 characters.

### 7.3.6 Application message

MMTP shall provide an application message which is a container transporting digital data of an MMS application from one sending Agent to one or multiple receiving Agents.

An MMTP application message shall contain the following elements:

1. An application message header containing:
  - a. A *subject* or *recipients* being:
    - i. The value of the *subject* property, if present, shall be an MRN no longer than 100 characters.
    - ii. The value of the *recipients* property, if present shall be a list with one or more MRNs. It is recommended to limit the number of recipients in this property to at most 10. For messages addressed to a larger number of recipients, it should be considered whether the subject cast concept can be utilized instead.
  - b. An *expires* property, value is seconds after the 1st of January 1970; shall be the timestamp when the message content is expected to be no longer relevant in seconds since the 1st of January 1970, 00:00:00 UTC. The timestamp may not be more than 30 days past the time of construction of the message.

- c. A *sender* property, value shall be the MRN of the Agent that constructed the message.
  - d. A *bodySizeNumBytes* indicating the size of the payload.
- 2. A *body* containing the binary data of the message in the protobuf bytes format.
- 3. A *signature* containing the bytes of a signed hash of the message header and body, signed with the MCP private key associated with the sender MRN in the context of the MCP MIR. Signing follows the following algorithm, where the byte encoding of a string is assumed to be UTF-8:
  - a. Allocate an empty list of bytes *B*,
  - b. Determine the value of *SubjectOrRecipient*:
    - If *subject* is set, encode the string value of *subject* as bytes and append the result to *B*,
    - If *recipients* is set, do for each recipient: encode the string value as bytes and append the result to *B*,
  - c. Encode the decimal string representation of the value of *expires* as bytes and append the result to *B*,
  - d. Encode the value of *sender* as bytes and append the result to *B*,
  - e. If *qosProfile* is set, encode the value of *qosProfile* as bytes and append the result to *B*,
  - f. Encode the decimal string representation of the value of *bodySizeNumBytes* as bytes and append the result to *B*,
  - g. Append the value of *body* to *B*,
  - h. Give *B* and private key as inputs to the signing algorithm defined by [12] Section 6.4.1 and store the output values *r* and *s*,
  - i. DER encode *r* and *s* using the ASN.1 structure defined by [13] Section 2.2.3 and return the result.

The signature shall be verified by the receiving agent, following the signature verification algorithm defined [12] Section 6.4.2

The following protobuf code does implement the required normative structure:

```
message ApplicationMessage {
  ApplicationMessageHeader header = 1;
  bytes body = 2;
  bytes signature = 3;
}
```

using

```
message Recipients {
  repeated string recipients = 1;
}
```

and

```
message ApplicationMessageHeader {
  oneof SubjectOrRecipient {
    string subject = 1;
    Recipients recipients = 2;
  }
}
```

```

}
int64 expires = 3;
string sender = 4;
optional string qosProfile = 5;
uint32 bodySizeNumBytes = 6;
}

```

### 7.3.7 MMTP Protocol Request messages

Each MMTP protocol request message shall be defined as a protobuf message, exchanged between connected nodes.

One MMTP protocol request message is sent in one encapsulating protobuf message.

The structure of each protocol message shall follow the following protobuf message:

```

message ProtocolMessage {
  ProtocolMessageType protocolMsgType = 1;
  oneof body {
    Subscribe subscribeMessage = 2;
    Unsubscribe unsubscribeMessage = 3;
    Send sendMessage = 4;
    Receive receiveMessage = 5;
    Fetch fetchMessage = 6;
    Disconnect disconnectMessage = 7;
    Connect connectMessage = 8;
    Notify notifyMessage = 9;
  }
}

```

An MMS Agent or MMS Router receiving a protocol message shall verify that the message complies with this specification and shall ignore messages that are not compliant.

#### 7.3.7.1 Subscribe

The *subscribe* protocol message shall be sent by either

1. An MMS Agent to an MMS Edge Router or
2. An MMS Edge Router to an MMS Router,

to inform about its interests in form of *subscriptions*.

The *subscribe* protocol message shall contain either:

- a *subject* string, value shall identify the MRN of the MCP service the sender subscribes to, or
- a *directMessages* bool, value shall identify a subscription to MRN-addressed messages to the Agent or Edge Router's own MRN.

The following protobuf code does implement the required normative structure:

```

message Subscribe {
  oneof subjectOrDirectMessages {
    string subject = 1;
    bool directMessages = 2;
  }
}

```

#### 7.3.7.2 Unsubscribe

The *unsubscribe* protocol message shall be sent by either

1. An MMS Agent to an MMS Edge Router or
2. An MMS Edge Router to an MMS Router,

to inform about its ending interests in form of *subscriptions*.

The *unsubscribe* protocol message shall contain:

- a *subject* string, value shall identify the MRN of the MCP service the sender subscribes to, or
- a *directMessages* bool, value shall identify a subscription to own MRN.

The following protobuf code does implement the required normative structure:

```
message Unsubscribe {
  oneof subjectOrDirectMessages {
    string subject = 1;
    bool directMessages = 2;
  }
}
```

#### 7.3.7.3 Send

The *send* protocol message shall be sent by either

1. An MMS Agent to an MMS Edge Router or
2. An MMS Edge Router to an MMS Router,

to send an application message.

The *send* protocol message shall contain:

- an Application message.

The following protobuf code does implement the required normative structure:

```
message Send {
  ApplicationMessage applicationMessage = 1;
}
```

#### 7.3.7.4 Receive

The *receive* protocol message shall be sent by either

1. An MMS Agent to an MMS Edge Router or
2. An MMS Edge Router to an MMS Router,

to receive message content.

The *receive* protocol message shall contain:

- an optional *filter*, containing an optional list of one or more message UUIDs.

The following protobuf code does implement the required normative structure:

```
message Receive {
  optional Filter filter = 1;
}
```

using



```
message Filter {
  repeated string messageUids = 1;
}
```

#### 7.3.7.5 Fetch

The *fetch* protocol message shall be sent by either

1. An MMS Agent to an MMS Edge Router or
2. An MMS Edge Router to an MMS Router,

to fetch a list of application message headers.

Note: this message triggers the receiver to send an MMTP response message.

The following protobuf code does implement the required normative structure:

```
message Fetch {
}
```

#### 7.3.7.6 Disconnect

The *disconnect* protocol message shall be sent by either

1. An MMS Agent to an MMS Edge Router or
2. An MMS Edge Router to an MMS Router,

to disconnect from the receiver of the message.

The following protobuf code does implement the required normative structure:

```
message Disconnect {
}
```

#### 7.3.7.7 Connect

The *connect* protocol message shall be sent by either

1. An MMS Agent to an MMS Edge Router or
2. An MMS Edge Router to an MMS Router,

to connect to the receiver of the message.

The *connect* protocol message shall contain:

- an optional *ownMrn*, subscribing to messages sent to own MRN, and
- an optional *reconnectToken*, containing an UUID according to [10], to continue a previous session, using the *reconnectToken* received in the Response Message to a previous connect.

The following protobuf code does implement the required normative structure:

```
message Connect {
  optional string ownMrn = 1;
  optional string reconnectToken = 2;
}
```

Note: a connect message triggers a response message from the receiver, containing a *reconnectToken*.

### 7.3.7.8 Notify

The *notify* protocol message shall be sent by either

1. an MMS Router to an MMS Edge Router or
2. an MMS Edge Router to an MMS Agent,

to notify about new queued messages.

The *notify* protocol message shall contain:

- zero or multiple message metadata.

The following protobuf code does implement the required normative structure:

```
message Notify {
  repeated MessageMetadata messageMetadata = 1;
}
```

## 8 The Secure Maritime Messaging Transfer Protocol

### 8.1 Overview (informational)

The Secure Maritime Messaging Transfer Protocol (SMMP) is an application layer protocol between SMMP Clients via MMS Agents. This protocol handles

- Confidential data exchange between SMMP Clients
- Segmentation of larger messages sent from one SMMP Client to another.

When using the SMMP, the MMS Agent acts as the interface between the SMMP Client and the Edge Router. The MMS Agent used by the SMMP Client must be in an authenticated state.

The SMMP is session based and does therefore only support MRN-addressed messages.

### 8.2 Definitions

All messages listed here are defined in protobuf format [9] prefixed with

syntax = "proto3";

The complete protobuf definition of SMMP can be found in Annex I.

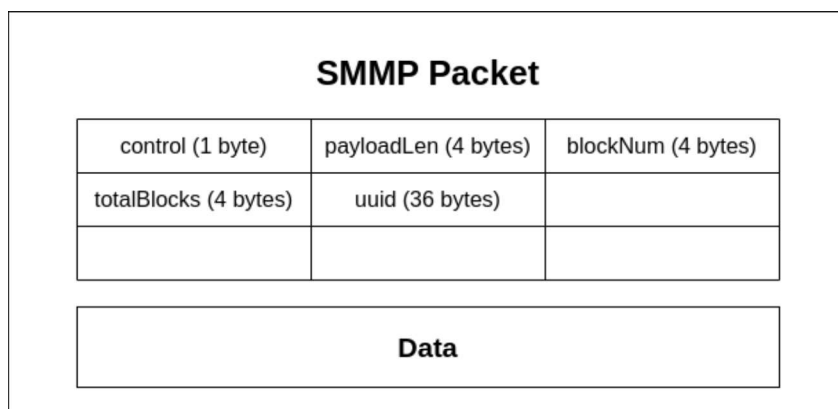
#### 8.2.1 SMMP messages

SMMP shall provide an SMMP message which is a container holding data to be sent from one sending SMMP Client to one receiving SMMP Client. If one *SmpMessage* is too large to be sent in one MMTP message (50 KiB), the data should be segmented into multiple SMMP messages referring to the same *SmpMessage* uuid.

An SMMP Message shall contain the following elements:

1. An SMMP message header containing:
  - a. A control byte, where the bits, starting from the least significant bit, indicates the following.
    - i. Bit 0 (Handshake) - Whether the *SmpMessage* is a part of the handshake procedure.
    - ii. Bit 1 (Acknowledgement) - Whether the *SmpMessage* is an acknowledgement of reception.

- iii. Bit 2 (Confidentiality) - Whether the *SmpmMessage* data is encrypted, and the agreed secret therefore should be used to decrypt the data.
  - iv. Bit 3 (Delivery Guarantee) - Whether a message acknowledgement is expected.
  - v. Bit 4 (Non-repudiation) - Whether the intended recipient should proof of message reception (non-repudiation).
  - vi. Bit 5 (Error) - Whether there was no valid SMMP session for a received message.
  - vii. Bit 6 (Finish) - Whether the sender is terminating the active SMMP session.
- b. An optional 0-indexed *blockNum* property indicating which number in the sequence of segmented blocks, the current SMMP message is. Shall only be used when segmentation is necessary.
  - c. An optional *totalBlocks* property indicating the total number of segments, the SMMP message has been divided into. Shall only be used when segmentation is needed.
  - d. A *uuid* property providing a unique identifier of the SMMP message or SMMP messages (if segmented).
2. A body containing the binary data of the message in the protobuf bytes format.



The SMMP header contains control bits indicating the operation of the SMMP message and optional block numbers for when SMMP messages are segmented. A uuid identifies the SMMP message.

The following protobuf code does implement the required normative structure:

```

message SmpmMessage {
  SmpmHeader header = 1;
  bytes data = 2;
}

using

message SmpmHeader {
  bytes control = 1;
  uint32 payloadLen = 2;
  optional uint32 blockNum = 3;
  optional uint32 totalBlocks = 4;
  string uuid = 5;
  repeated string responseToUuid = 6;
}
    
```

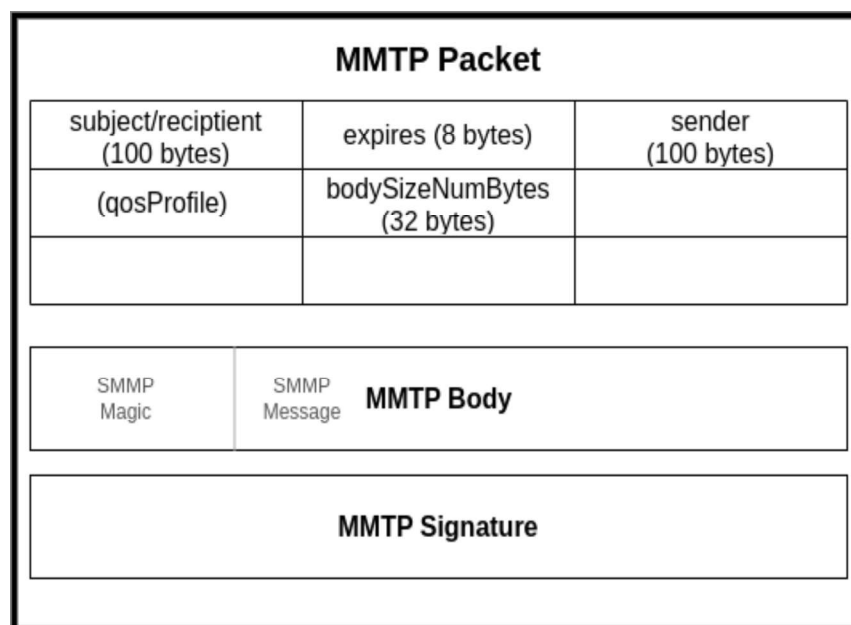
### 8.2.2 SMMP message identifier (magic word)

A magic word shall be prepended to the encoded data resulting from Protobuf serialization of an *SmpMessage*. This informs to the receiving agent that the MMTP payload should be treated as an SMMP message.

The following algorithm shall be used to prepend the magic word:

1. Allocate an empty buffer of bytes, B
2. Append the ASCII-encoded bytes for *SMMP* to B
3. Append the encoded data resulting from Protobuf serialization to B

The resulting value B should be treated as a regular MMTP payload.



The SMMP message is treated as an MMTP payload, where the magic word is prepended to the serialized SMMP message

Upon reception of an MMTP message, the recipient should inspect if the MMTP payload should be treated as an SMMP message. This check is conducted by inspecting whether the first four bytes of the MMTP payload matches the magic word.

### 8.2.3 SMMP Handshake

The *SMMP Handshake* shall be used to establish a SMMP session between two SMMP clients over an MMTP channel. When confidentiality is required, Elliptic Curve Diffie-Hellman Key Exchange (ECDH), defined in [14] shall be performed. Curve P-384 shall be used for ECDH as described in [15]. The shared secret shall be used to calculate a 256-bit AES session key using CTR mode of operation.

#### 8.2.3.1 Handshake procedure

A SMMP Handshake between two clients shall conform to the following procedure:

1. The initiating SMMP Client sends a SMMP message to the receiving SMMP Client with the **Handshake** bit set. Furthermore, the initiating SMMP Client shall set the following bits dictating which guarantees should be provided in the session:
  - **Confidentiality** bit if communication should be confidential.

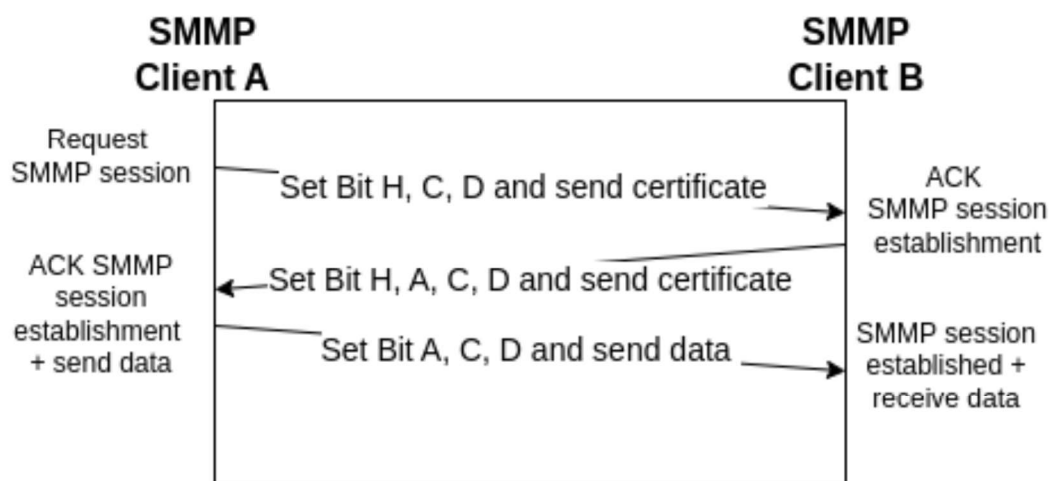
- **Delivery Guarantee** bit if a delivery guarantee should be provided.
- **Non-repudiation** bit if a non-repudiation guarantee should be provided.

If confidentiality is requested, the data payload shall contain the DER-encoded certificate of the initiating SMMP Client. Otherwise, the data payload shall be empty.

1. The receiving SMMP Client responds with a SMMP message, setting the same bits as the initiating SMMP Client, if able to accommodate the guarantees. In addition, the receiving SMMP Client should set the **Acknowledgement** bit, indicating that the request to establish a SMMP session has been accepted. If confidentiality is requested, the data payload shall contain the DER-encoded certificate of the receiving SMMP Client. Otherwise, the data payload shall be empty.
2. The initiating SMMP Client should respond with a SMMP setting the same bits as the receiving SMMP client, thereby acknowledging which security guarantees will be provided by the SMMP session. In addition, the **Handshake** bit should be unset. This SMMP message may include a data payload.

### 8.2.3.2 SMMP Handshake diagram

The following diagram shows the SMMP messages exchanged to establish a confidential SMMP session with delivery guarantee.



The SMMP header control bits are set to establish an SMMP session and negotiate the guarantees that should be provided in the session

Note: The Confidentiality, Delivery Guarantee and Non-repudiation bits shall only be set during the SMMP handshake, where session guarantees are negotiated.

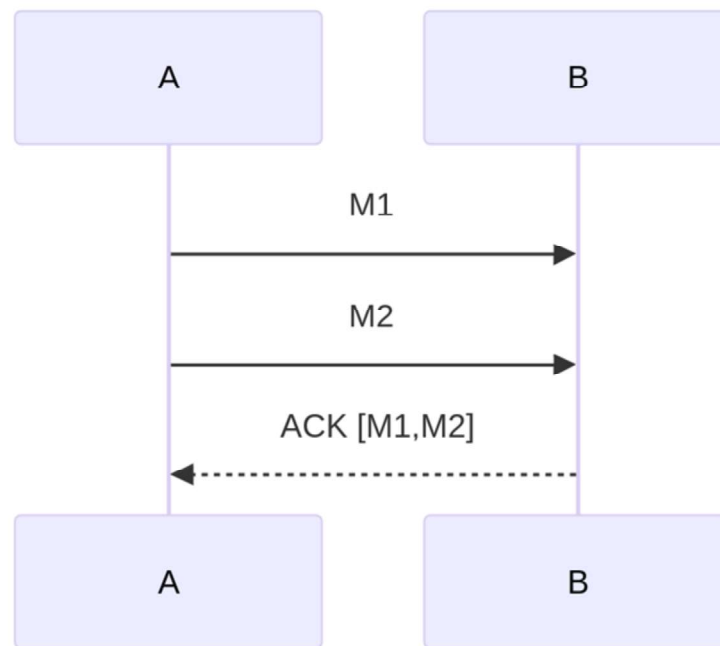
### 8.2.4 SMMP Message reception

#### 8.2.4.1 Reception of messages with delivery guarantee

In a SMMP session where delivery guarantee is desired, the receiving SMMP Client shall respond with an acknowledgement to a received message. Such an acknowledgement shall be an SMMP Message where:

- The Acknowledgement bit is set
- The repeated **SmpHeader** field **responseToUuid** contains the UUID of one or more received SMMP messages.

Note: Sending an acknowledgement containing the UUIDs of multiple received messages, serves as an optimization such that individual acknowledgements can be bundled. This is shown in [17](#)



**Figure 17 – UML Sequence Diagram Delivery Guarantee: The receiving SMMP client may bundle acknowledgements.**

#### 8.2.4.2 Reception of messages with non-repudiation guarantee

In a SMMP session where non-repudiation guarantee is desired, the receiving SMMP Client shall give proof of successful message reception to the sender. Such proof shall be an SMMP Message where:

- The Acknowledgement bit is set
- The repeated *SmpHeader* field *responseToUuid* contains the UUID of the message which the receiver intends to prove reception of.
- The payload (*data* field) is a signature containing the bytes of a signed hash of the received *SmpMessage data*, signed with the MCP private key associated with the sender MRN in the context of the MCP MIR. Signing follows the following algorithm, where the byte encoding of a string is assumed to be UTF-8:
  - a. allocate an empty list of bytes *B*,
  - b. append the value of *data* to *B*,
  - c. append the current time, expressed as a value in seconds after the 1st of January 1970, to *B*,
  - d. give *B* and private key as inputs to the signing algorithm defined by [12] Section 6.4.1 and store the output values *r* and *s*, and
  - e. DER encode *r* and *s* using the ASN.1 structure defined by [13] Section 2.2.3 and return the result.

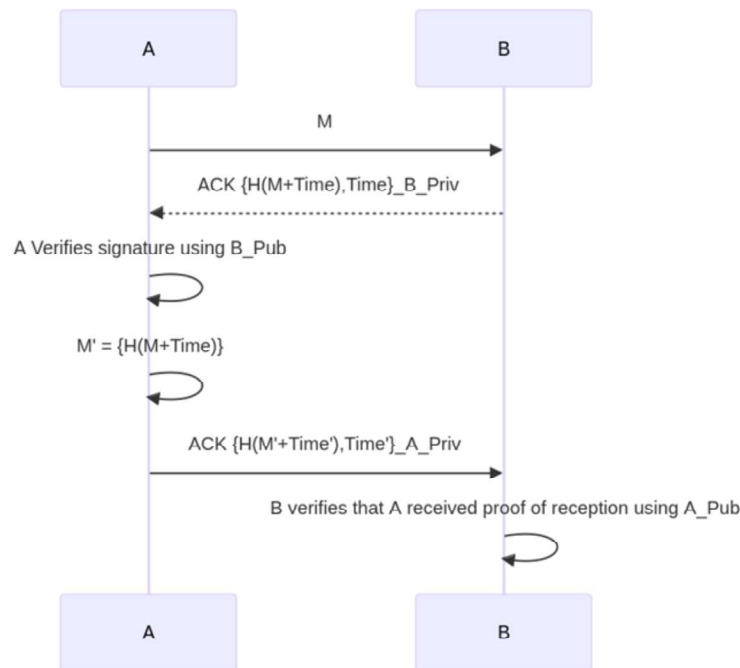
The signature shall be verified by the sending agent, following the signature verification algorithm defined [12] Section 6.4.2.

The sending SMMP Client shall give proof to the receiving client, that the proof of message receptions has been successfully received. Such proof shall be an SMMP Message where:

- The Acknowledgement bit is set
- The repeated *SmpHeader* field *responseToUuid* contains the UUID of the message in which the receiver proves reception.
- The payload (*data* field) is a signature containing the bytes of a signed hash of the received *SmpMessage data*, signed with the MCP private key associated with the sender MRN in the context of the MCP MIR. Signing follows the following algorithm, where the byte encoding of a string is assumed to be UTF-8:
  - a. allocate an empty list of bytes *B*,
  - b. append the value of *data* to *B*,
  - c. append the current time, expressed as a value in seconds after the 1st of January 1970, to *B*,
  - d. give *B* and private key as inputs to the signing algorithm defined by [12] Section 6.4.1 and store the output values *r* and *s*, and
  - e. DER encode *r* and *s* using the ASN.1 structure defined by [13] Section 2.2.3 and return the result.

The above procedure is illustrated in 18

Note, to achieve full non-repudiation it is up to the application layer to store messages and proofs of reception in a non-volatile manner.



**Figure 18 – UML Sequence Diagram Non-repudiation: The receiving SMMP client must provide proof of reception using his digital signature.**

#### 8.2.4.3 Reception of messages in a lost session

Upon reception of a SMMP message, for which there exists no valid SMMP session, the recipient must reply with a SMMP Message in which the Error bit has been set.

#### 8.2.5 SMMP session termination

A SMMP client can terminate an active SMMP session by sending a SMMP message with the Finish bit set indicating SMMP session termination. The receiving SMMP Client must acknowledge session termination by responding with an SMMP Message with the Acknowledgement and Finish bit set.

##### 8.2.5.1 Secure session termination

To ensure secure SMMP session termination, the SMMP Client initiating session termination shall wait for the receiving SMMP Clients acknowledgement of the session termination. The SMMP Client initiating session termination shall delete the session key immediately after receiving such acknowledgement from the receiving SMMP Client. The receiving SMMP client shall delete the session key immediately after acknowledging the request to terminate the SMMP session.

Note: Secure session termination is necessary to avoid session hijacking caused by a compromise of the session key prior to deletion.

## 9 The MMS Router Network Protocol

### 9.1 Overview (informational)

The MMS Router Network Protocol is the protocol that handles the connections and communication between MMS Routers. It is heavily based on the libp2p [16] framework and several of the protocols that are defined within it. The protocol handles

- connections between MMS Routers,
- routing of MMTP messages between MMS Routers, and



- handling of subscriptions on behalf of connected MMS Edge Routers.

## 9.2 Requirements

The MMS Router Network Protocol shall provide a transport for routing MMTP messages between MMS Routers.

This chapter specifies the particular use of that protocol, i.e. a binding.

The MMS Router Network Protocol shall:

- enable MMS Routers to establish connections between each other,
- allow for publishing and subscription of MMS subjects and MRN-addressed messages, and
- ensure that any message published in the Router Network are routed to all subscribers.

## 9.3 Definitions

### 9.3.1 Connection Between MMS Routers

For the connection between MMS Routers the protocol for connection establishment in libp2p [17] shall be used.

While the above mentioned protocol does support a variety of underlying transport mechanisms, an MMS Router shall at least support TCP [34] and QUIC [35,36,37,38] as the underlying transport mechanisms.

Connections between MMS Routers shall be secured with TLS 1.3 [8] using the libp2p specification that is defined by [18].

MMS Routers shall use the p2p multiaddr format [19] from libp2p to address other MMS Routers.

### 9.3.2 Establishment of MMS Router Network

In order for MMS Routers to discover each other and form a network, the libp2p Kademlia DHT [20] shall be used.

#### 9.3.2.1 Bootstrapping the DHT

Before an MMS Router can use the libp2p Kademlia for discovery of other MMS Routers it needs to be bootstrapped. To do this the Router shall connect to another Router that it already knows in advance using the protocols described in 9.3.1.

After successfully establishing a connection, the Router shall initialize a local DHT in *server mode* and perform the *bootstrap process* as described in [20].

#### 9.3.2.2 Discovery of Additional Router Nodes

After having successfully bootstrapped the DHT, the Router shall advertise a route in the Kademlia routing table with the key *K* that is defined for the MMS Router Network.

To then discover other Routers nodes that are advertising the same route, the Router shall use the *FIND\_NODE* operation with the key *K* as input and then try to connect to as many of the candidate nodes as possible that are returned by the operation.

### 9.3.3 Handling of Subscriptions

For handling of subscriptions in the MMS Router Network, the libp2p PubSub interface [21] shall be used. This interface defines operations for both subscribing and publishing to *topics*.

### 9.3.3.1 Subscribing to Subjects and MRN-Addressed Messages

When an MMS Router receives an MMTP Message with a *Subscribe* message inside from a connected Edge Router, the Router shall first determine whether it is already subscribed to the Subject contained in the *Subscribe* message.

If it is, the Router shall register internally that the requesting Edge Router is now subscribed to the Subject and return.

If it is not, the Router shall construct a *SubOpts* [21] message where the *subscribe* field is set to **true** and the *topicid* field is set to the value of the *subject* field from the *Subscribe* message.

The constructed *SubOpts* message shall then be used to populate the *subscriptions* field in an *RPC* message, which shall then be advertised to the MMS Router Network according to the libp2p gossipsub protocol [22].

Finally, the MMS Router shall register internally that the requesting Edge Router is now subscribed to the Subject and return.

### 9.3.3.2 Unsubscribing from Subjects and MRN-Addressed Messages

When an MMS Router receives an MMTP Message with a *Unsubscribe* message inside from a connected Edge Router, the Router shall register internally that the requesting Edge Router is no longer subscribed to the Subject contained in the *Unsubscribe* message.

After having done that, the Router shall check whether it has other connected Edge Routers that are subscribed to the Subject.

If it has, the Router does not need to do anything further and can return.

If it has not, the Router shall construct a *SubOpts* [21] message where the *subscribe* field is set to **false** and the *topicid* field is set to the value of the *subject* field from the *Unsubscribe* message.

The constructed *SubOpts* message shall then be used to populate the *subscriptions* field in an *RPC* message, which shall then be advertised to the MMS Router Network according to the libp2p gossipsub protocol [22].

## 9.3.4 Routing of Messages

### 9.3.4.1 Sending Messages

When an MMS Router receives an MMTP Message with a *Send* message inside, the Router shall first check whether the message is a subject-cast message or an MRN-addressed message. If the message is a subject-cast message, the Router shall construct a libp2p PubSub *Message* [21] where the *data* field is populated with the received MMTP message and the *topic* field is populated with the subject from the *Send* message.

If the message is MRN-addressed message, the Router shall for each recipient in the *Send* message construct a libp2p PubSub *Message* [21] where the *data* field is populated with the received MMTP message and the *topic* field is populated with the recipient.

After having constructed the message, the Router shall send the message to the MMS Router Network according to the libp2p gossipsub protocol [22].

### 9.3.4.2 Receiving Messages

In order to receive messages from the MMS Router Network, an MMS Router shall for each libp2p topic that it is subscribed to listen for messages coming in from the MMS Router Network. Whenever a message is received, the Router shall add the message to the message queue of all connected Edge Routers that are subscribing to the subject of the MMTP message contained in the received message.

## 10 Binding

Binding describes how to use the underlying protocol layers to transport the MMTP protocol over LAN or WAN IP networks.

For binding to other means of transport, see the Appendixes.

### 10.1 WebSocket binding

#### 10.1.1 WebSocket Endpoints

An MMS Edge Router or Router has an HTTPS endpoint where it can accept WebSocket [23] connections.

#### 10.1.2 Connection Management

Agents shall use secure WebSocket transport [23] binding toward the MMS Edge Router, i.e. the Agent can verify the authenticity of the MMS Edge Router.

Agents that require authenticated connection to the MMS Edge Router, shall use mutual authenticated TLS WebSocket binding, as defined in TLS [8].

MMS Edge Routers that connect to MMS Routers shall use mutual authenticated TLS WebSocket binding, as defined in TLS [8].

WebSocket connections are kept alive by the WebSocket integrated ping/pong mechanism [23].

#### 10.1.3 Discovery of Endpoints

Discovery of the MMS Edge Routers endpoints is described in 6.

MMS Routers are discoverable in a Service Registry as defined in [24] Section 9, e.g. the MCP Service Registry.

#### 10.1.4 Status

MMTP shall implement a status, facilitated by a HTTP GET call. Either the Agent calls the Edge router, or the Edger call the router.

The path for the status shall be “/status”.

Status shall return a JSON object [25] containing the status as described in 6.1.6.

#### 10.1.5 Timeouts

Timeouts for WebSocket shall be implemented as defined by the WebSocket standard [23].

## 11 Example Implementation of a use case (informative)

This informative chapter details how a selected use case can be realized using the protocols described in this standard.

### 11.1 MUC 2.5 realization

Ships at sea need to receive the latest navigation information from the shore in a timely manner. However, communication at sea is not always capable of providing sufficient coverage and high speeds, unlike that on land. In some cases, IP-based broadband communication can be used, and in some cases, only non-IP-based narrowband communication, such as VDES, can be used. MMS was developed in consideration of this to enable the use of maritime information services using various means of communication. With MMS, you can efficiently update the information you need to receive at the right time, such as NW, by subscribing to a specific subject. This section describes how MMS transport maritime services to ships on VDES, especially subscription to a subject.

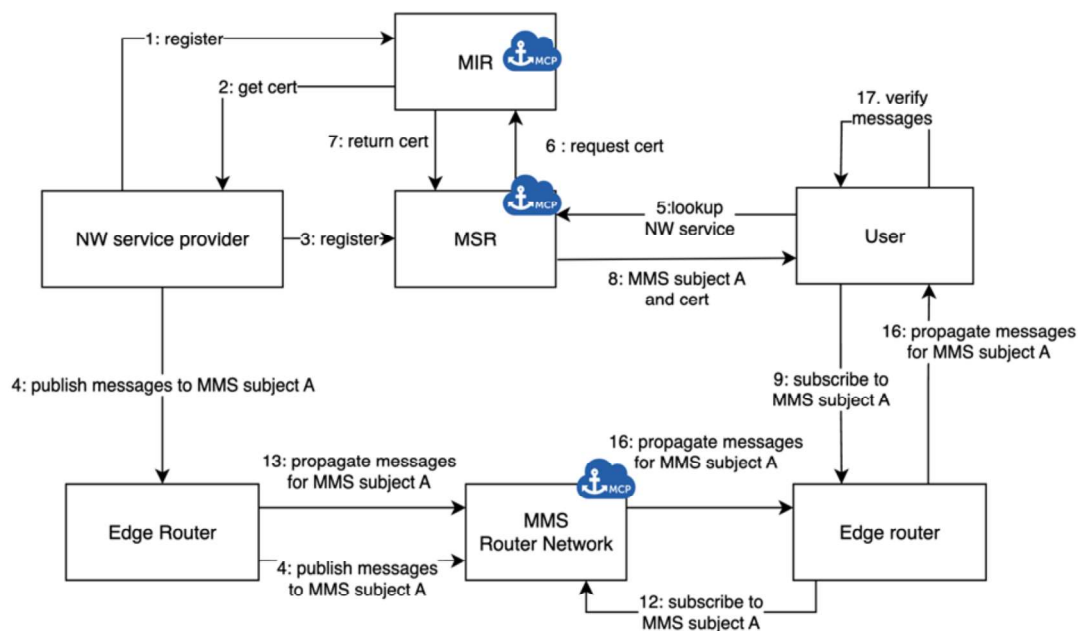


Figure 19 – Use Case Implementation and signalling steps.

#### 11.1.1 Service Registration

MCP, as is well known, has MIR and MSR as its core components along with MMS. In order to provide a reliable maritime service for service users, it is helpful for a service provider (SP) to obtain its certificate from MIR that includes the service provider's MRN and related information. After the certificate is issued, the service specifications, including the SP's MRN and the content and coverage of the service, need to be registered in the MSR, see Figure 19, signalling step numbers 1 to 3. In doing so, SPs, i.e. NW SP, make their MRNs searchable by service consumers (SCs) along with the content of the services they provide.

A NW SP will then be able to provide the latest NW information to ships by publishing the NW they generate to MMS.

#### 11.1.2 Service provision and consumption

In order for SPs to provide services, they only need to continuously publish information about the specific subject they provide to the MMS Router through the MMS Agent and the Edge Router, see Figure 19, signalling step 4 and 13.

In order for SC to subscribe to the information published by SP, the SC must first obtain information about the service it would like to subscribe. This can be obtained by searching for SPs at MSR, see Figure 19, signalling steps 5 to 8. MSR can be operated in conjunction with MIR, which allows users to provide a SP's certificate when requesting information about the service. SC will use the information about the services obtained from MSR to select the services they will use. MSR retrieves a relatively large amount of information such as service lists, specifications, and certificates compared to general maritime services, so it can be convenient to use it in a broadband IP communication environment, i.e. when still in the harbour.

After acquiring information about a service, the SC can obtain navigational information from a SP by submitting requested information when the SP uses MMS, or use the maritime information service by subscribing to the subject of his or her interest, see Figure 19, signalling steps 9 and 12. The service data is propagated from the MMS Router Network to the User after subscription and new propagations/publishing happens according to Figure 19, signalling steps 4, 13, and 16. It seems

appropriate to have e.g. a Traffic Clearance Service in the former way (MRN-addressed messaging) and the NW service in the latter way, by subject subscription.

### 11.1.3 Subscription to a subject using MMTP over VDES

To receive information from a specific subject using MMTP over VDES, the MMS agent linked to the onboard application, such as ECDIS or ECS, must be connected to an onboard VDES Edge Router (VDES ER). In this case, either the connectAnonymous() or connectAuthenticated() function is used. Once the MMS Agent is connected to the VDES ER, the VDES ER will connect to the Routers Network via VDES and fetch any subscribed messages. Through this procedure, the message fetched to the VDES ER is subscribed by the MMS agent using the subscribe(subject) function and finally delivered from the MMS agent to the onboard application, and then to users through display, etc. See Figure 20 for an illustration of this process.

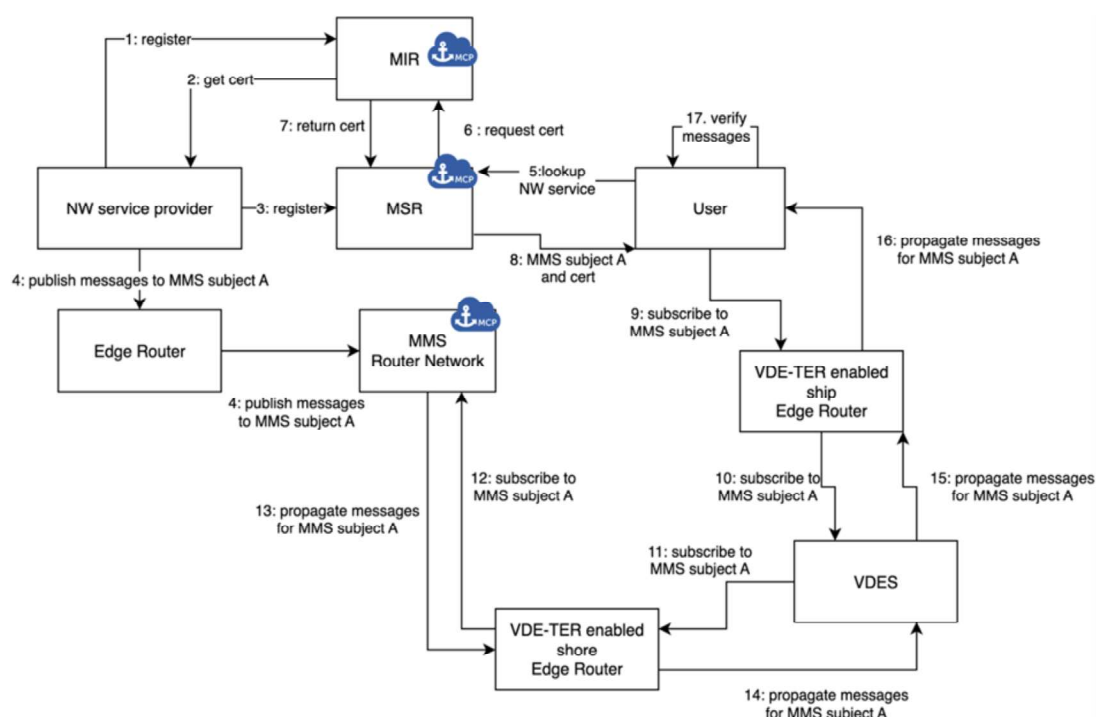


Figure 20 – Service Subscription and Delivery.

## Annex A (informative)

### MMS Motivational Use Cases

The following motivational use cases (MUC) are the basis for the requirements of MMS.

#### A.1 MUC1: User group - Navigator

##### A.1.1 MUC1.1: Navigational Supplementary Information

Story: As a navigator, I want to reliably and automatically get the navigational supplementary information for an area of interest displayable as an ECDIS overlay, authenticated and integrity checked, so that I can minimize the navigation risk for the remainder of my voyage in a user friendly and efficient manner.

Note: SECOM or otherwise provided S-100 data may be made available to the MMS through adaptation with an MMS Agent that implements the SECOM interface, as described in Annex G; users find the service through the MSR by searching for e.g. data type, region, authority; then, users subscribe to the subject-cast MRN for the services via MMS and receive all updates that are available for that service, as long as they are subscribed.

##### A.1.2 MUC1.2: Route validation service

Story: As a navigator, I want to submit my actual route to a trusted service provider in order for it to be analyzed for associated navigational risks. I expect to receive advice including e.g. annotations or alternative route elements, such that I can minimize the navigation risk for the remainder of my voyage. The data should be exchanged confidentially, authenticated and with integrity.

Note: this use cases includes S-421 based route exchange, attached to encrypted messages using the SMMP protocol, see 5.3.2, that are sent from the ship to the service provider (e.g. VTS) and back.

##### A.1.3 MUC1.3: Chat service

Story: As a navigator, I want to communicate with the crew of a nearby ship, so that I can inform about my intentions and coordinate navigational strategies with the other ship with authenticity and integrity protected, possibly confidentiality, in order to minimize risk for the remainder of my vessels voyage.

Note: this use case may be implemented by mandating a MMS text message Agent for all MMS ship edge routers, to exchange text messages signed via MMTP and optionally also encrypted via SMMP between Agents. As every MMS Edge Router announces its publicly available local services via e.g. VDES, nearby ships know that MMS text message client is available. The text message service could allow the attachment of files, such as S-421 based route data in case of route coordination between ships.

##### A.1.4 MUC1.4: Emergency Signalling

Story: As a navigator, I want (as a supplement to GMDSS) to signal my state of emergency to nearby ships and authorities by modern communication means, including mobile networks, satellite communication and VDES, in order to start actions to save the lives of my crew.

Note: this use case may be implemented by mandating a MMS safety message Agent for all MMS ship edge routers, to be able to transmit selected data in line with other distress messaging, however allowing signing of the data would ensure the authenticity and integrity of the data, and many different communication ways would be supported over MMS.

##### A.1.5 MUC1.5: Intention broadcast

Story: As a navigator, I want to share my intent with the crews of nearby ships, so that they can take informed navigational decisions in order to minimize the navigation risk for the remainder of my voyage.

Note: Possible implementation includes the broadcast of the next few waypoints of the intended route in S-421 format, e.g. using terrestrial VDES as a broadcast message.

#### **A.1.6 MUC1.6: Multiple services**

Story: As a navigator, I want to reliably and automatically get data for multiple services at the same time, so that I user friendly and efficiently can minimize the risk for the remainder of my voyage under different navigational aspects such as weather, navigational warnings, route validation, etc.

Note: MMS supports the transport of messages over same or different physical channels at virtually the same time, such that it appears for the operator as simultaneously.

### **A.2 MUC2: User group - Maritime Service Provider**

Maritime Service Providers include Maritime Authorities, VTS, Port Authorities and private enterprises.

#### **A.2.1 MUC2.1: Search and Rescue Coordination**

Story: As a maritime search and rescue coordinator, after receiving a Distress message, I want to coordinate search and rescue missions by the use of messages, in order to minimize the time before helpers reach a vessel in need.

Note: this use case may be implemented by the use of S-421 route exchange data transported over the currently available means of transport to different ships; each ship might have different available means of transport, e.g. satcom internet, VDE-SAT, VDE-TER, or even NAVDAT are possible with the use of MMS.

#### **A.2.2 MUC2.2: Priorities on Safety**

Story: As a maritime actor, I want to be able to prioritize safety related communication over all other traffic, in order to safe life at sea.

Note: While Agents only handle one application at a time, and protocol does not allow to set priority in the MMS, it is the Edge Routers on ship and shore, that offer policing of priorities based on the service MRN. This leads to data for one service being e.g. transported over all available means regardless of price, while other services (of lower priority) can be restricted only to use certain means of transport, e.g. to reduce the amount of transported data over an expensive satcom internet connection, waiting for land mobile network connectivity to appear.

#### **A.2.3 MUC2.3: AToN monitoring**

Story: As a maritime authority, I want to monitor my aids to navigation remotely, i.e. position, power supply, temperatures, pressures, in order to be able to take responsible preventive maintenance actions or to issue notices to mariners in case of malfunction or displacement.

Note: this uses case could be implemented by the use of SMMP to allow encrypted communications with the AtoN over multiple redundant connections, e.g. 3G mobile or satellite networking and terrestrial or even satellite VDES. If one connection method fails, the other would be used. Priorities are stored in local configuration of the MMS edge routers to allow "least cost routing", choosing always the cheapest connection based on local rules on the mobile MMS Edge Router.

#### **A.2.4 MUC2.4: Virtual Aids-to-Navigation**

Story: As an AtoN Authority, I wish to provide Virtual AtoNs to all ships in, and only in, a given area, in a standard format displayable on ECDIS, with authenticity and integrity guaranteed.

Note: this use case may be implemented by use of the signed S-125 or S-201 data exchanged over internet and terrestrial or satellite VDES, or NAVDAT, dependent on how large the intended coverage area and expected means of reception by the users. Such transmitted data will be received trustworthy independent of the channel used.



### **A.2.5 MUC2.5: Subject based service provisioning**

Story: As a maritime service provider, I wish to provision my services in a way, in order they can be found by the users searching for subjects.

Note: as described in MUC1.1, services are registered in the MSR with several parameters, one of them being their unique subject type, and therefore, this is searchable through the MSR.

### **A.2.6 MUC2.6: Network aware response to service request**

Story: As a maritime service provider, I wish to provide my service scaling the amount of data responded to a request, in order that it adapts to the stability and bandwidth of the network used for transport of the service, to give the user always a successful response and vary the amount of content based on the network stability and bandwidth.

Note: MMS supports this by offering policies that make certain MRN available only through certain channels; e.g. a small bandwidth ice chart based on S-411 can be provided to ships through VDE-SAT, while users who subscribe through satcom internet may be allowed through ship's own policies to subscribe to the high-bandwidth service. On the service side, the Agent creates the pre-decided different bandwidth (file size) options based on its configuration, decided by the service provider, without the need to recreate all data from scratch, based on algorithms decided by the service provider.

### **A.2.7 MUC2.7: Automatic Information Exchange**

Story: as a Coastal State Government Authority or Port Community Service Provider, I want to automatically collect/subscribe to up-to-date administrative and operational port call information from a ship's ICT ship reporting application to reduce the administrative burden on my staff and the Bridge Team and to avoid human error. The information exchange named here can be used for digital twins or data mining.

### **A.2.8 MUC2.8: AIS Authentication**

Story: as a Coastal State Government Authority or Port Community Service Provider, I want to get authentication of AIS messages in order to be sure that the transmissions for a ship are really from that ship and not from an imposter.

Note: MMS requires all VDES installations that are MMS compatible to generate AIS Authentication messages in order to get trusted positions and identities used for routing of messages. That AIS authentication information, transmitted in IALA G1117 format, may be used by authorities and other ships directly to validate authenticity and integrity of AIS transmissions of MMS enabled VDES ship stations every 300 seconds.

## **A.3 MUC3: User group - Pilot**

### **A.3.1 MUC3.1: Pilotage**

Story: As a Pilot, boarding a ship, I want to use my PPU to consume maritime services through various types of ship network, so that I can help the ship to navigate safely.

Note: MMS enabled PPU's connect to each new ship's MMS Edge Router and by that use all available connectivity that this ship has. E.g. if the ship has an MMS Edge Router and connected VDES transceiver on board, local VDE-TER services can be consumed in a unique way on board of the ship. It would be recommended to standardize a unique MRN pattern for pilot services, such that standardized policing can be tested in type approval for ship equipment to be equal on each ship.

## **A.4 MUC4: User group - Ship Owner**

### **A.4.1 MUC4.1: Mirroring of Messages**

Story: As a ship owner, I want to receive a copy of all messages that go to one of my ships, so that I can keep a log of all messages.



Note: that is supported by the ship owner subscribing to the same MRN's the ship is subscribed to.

## **Annex B** (informative)

### **Annex MMS Ship Equipment**

The following introduces classes of ship equipment that may be defined for different complexity grades of MMS ship equipment.

Ship Equipment supporting VDES, internet and NAVDAT shall implement all the following chapters requirements.

Variants may be made, with ship equipment only supporting existing ways of transport, and where testing is performed only for the transports that are to be supported.

#### **B.1 Ship Equipment for utilizing internet connectivity**

Ship Agents and Edge Routers that shall be able to utilize MMS over any of the ship's internet connections shall implement functionality as described in this Standard, as of sections 5, 6, 7, 10.

This is the minimum MMS configuration that all installations should support.

#### **B.2 Ship Equipment for utilizing optional SMMP**

Agents supporting SMMP, shall implement at minimum the Agent functionality as defined in the requirements given for B.1, and additionally 8.

#### **B.3 Ship Equipment for utilizing VDES connectivity**

Ship Edge Routers supporting VDE-TER and VDE-SAT shall implement the minimum functionality as defined in B.1, and additionally Annex C and Annex D.

#### **B.4 Ship Equipment for utilizing optional NAVDAT**

Ship Equipment supporting NAVDAT, shall implement at minimum B.4, and additionally Annex F, optionally also VDES.

## Annex C (informative)

### MMS Binding for VDE-TER networks

VDES contains a terrestrial component for ship to ship, ship to shore and shore to ship transfers of messages called VDE-TER, see [2], General section and Annex 4 for details.

This Appendix describes the bindings and functionality that shall be implemented by equipment providing transport of MMS messages over a VDE-TER network.

#### C.1 Entities overview

This chapter introduces the entities that shall provide functionality to support MMS messages over VDE-TER. An overview over the system is shown in Figure 21.

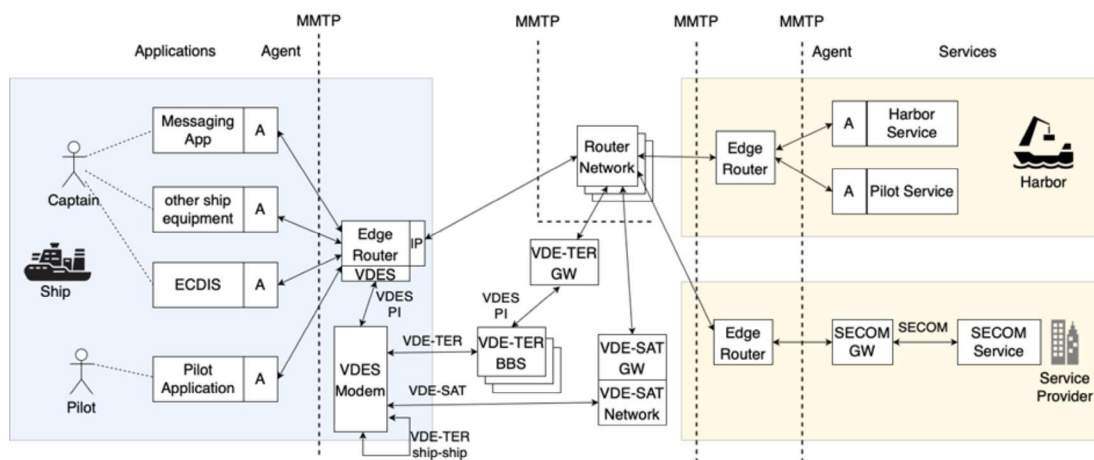


Figure 21 – Overview of MMS system architecture with VDE-TER network.

##### C.1.1 VDE-TER Shore Base Station

VDE-TER Shore Base Stations provide VDE-TER radio access to VDE-TER mobile equipment from typically a fixed location at shore.

VDE-TER Shore Base Stations coordinate the VDE-TER resources for all connectivity between mobile VDE-TER equipment and themselves in the radio coverage area of the base station according to [2].

In Figure 21, the VDE-TER Shore Base Station is abbreviated as “VDE-TER BBS”.

MMS compliant VDE-TER Shore Base Stations shall route received VDE-TER traffic that is sent to their own VDES MMSI with a VDE-TER payload data identified as MMS according to [26], Annex B.3.1 to an MMS VDE-TER Gateway for MMS routing.

MMS compliant VDE-TER Shore Base Stations shall allow an MMS VDE-TER Gateway to send:

1. MRN-addressed MMS messages as directed VDE-TER messages to the specified MMSI using VDE-TER, and
2. subject cast MMS messages as VDE-TER broadcast to MMSI=0, i.e. to all receivers in its coverage area.

A VDE-TER Shore Base Station shall provide a Presentation Interface to the MMS Shore Edge Router as defined in [27].

In Figure 21, the VDE-TER Base Station Presentation Interface is abbreviated as “VDES PI”.

### C.1.2 MMS VDE-TER Gateway

An MMS VDE-TER Gateway provides a link between the MMS Router Network and one or multiple VDE-TER Shore Base Stations.

In Figure 21, the VDE-TER Gateway is abbreviated as “VDE-TER GW”.

An MMS VDE-TER Gateway is an Edge Router and shall conform to 6.2. Additionally, an MMS VDE-TER Gateway shall perform at least following functions:

1. broadcast information about MMS capabilities for VDE-TER enabled MMS Mobile Edge Routers on all connected VDE-TER Shore Base Stations with necessary information for mobile equipment to perform MMS,
2. maintain routing to reach subscribed own MRN's via VDE-TER as long as these are in the VDE-TER network coverage area,
3. subscribe to MRNs with the MMS Router Network on behalf of the VDE-TER connected mobile MMS Edge Routers in the VDE-TER network,
4. send messages from the MMS Router Network to MRNs in coverage of the VDE-TER Network, utilizing its VDE-TER Shore Network,
5. using the VDE protocol format header layer to identify MMS traffic according to [26], Annex B.3.1,
6. priority based queuing of messages with mobile destinations where the target MRN is not reachable until a timeout happens,
7. forward MMS messages received through the VDE-TER Shore Network to the destination if it can be reached locally in the VDE-TER Shore Network,
8. forward MMS messages received through the VDE-TER Shore Network to the MMS Router Network for routing, where local routing is not possible,
9. apply cleaning of its buffers, own routing and mapping tables when ships have left the coverage area.

Note: applicable standard MMS services that an MMS VDE-TER Gateway may provide and announce to be available through VDE-TER broadcasts are:

- MIR query service to retrieve public certificates to support end-to-end encryption of MMS messages between MMS Agents, e.g. ship-ship,
- MIR revocation service,
- MSR query interface, to retrieve service certificates for services transported over that VDE-TER Shore Network

### C.1.3 VDE-TER Link

The link between the VDE-TER Shore Base Station and the VDE-TER Mobile Equipment utilizes the maritime VHF frequency band according to ITU-R M.2092-1 [2].

In Figure 21, the VDE-TER Link is labelled “VDE-TER”.

#### C.1.4 VDE-TER Mobile Equipment

VDE-TER Mobile Equipment, e.g. a VDES ship transceiver, facilitates communication to other mobile equipment and shore base stations through VDE-TER as defined in [2].

Note: typically, VDE-TER Mobile Equipment is a VDES Ship Transceiver on board of a ship.

In Figure 21, the VDE-TER Mobile Equipment is labelled “VDE-TER Modem”.

Note: MMS message exchange over VDE-TER is enabled to use following VDE-TER directed message types:

- ship to ship,
- ship to shore, and
- shore to ship,

and the VDE-TER broadcast (identified by destination MMSI = 0).

VDE-TER Mobile Equipment shall conform with [2] General section and Annex 4, and shall be type approved by [1].

VDE-TER Mobile Equipment shall provide a Presentation Interface to the MMS Mobile Edge Router as defined in [1].

Note: the VDE-TER presentation interface is based on VDE-TER specific sentences as defined in [1], transported over lightweight ethernet [28] standard providing NMEA/UDP/IP. This interface is labelled “VDES PI” in Figure 21.

#### C.1.5 VDE-TER enabled mobile MMS Edge Router

A VDE-TER enabled mobile MMS Edge Router is an MMS Edge Router providing the MMTP interface to MMS Agents as described in 6.2, that is capable to use VDE-TER for transport of MMS messages to other VDE-TER equipment that is connected to a VDE-TER enabled Shore or Mobile Edge Router.

To use VDE-TER transport in the MMS, a mobile MMS Edge Router shall support VDE-TER mobile equipments’ PI interface as defined in [1] and implement additional functionality:

1. manage a local root certificate storage for the authentication of VDE-TER bulletin boards,
2. update the local certificate storage based on revocations sent through an MMS MIR revocation service,
3. update the local certificate storage based on certificates received from trusted MMS VDE-TER Gateways, for services the Edge Router itself subscribes to,
4. provide access to the local certificate storage for local MMS Agents and VDE-TER mobile equipment, using the MMS certificate query service interface,
5. decide to use or not use a VDE-TER Shore Base Station based on local trust configuration, using the VDE-TER bulletin board signature received from a VDE-TER Shore Base Station,
6. receive and apply MMS capability broadcasts from MMS VDE-TER Gateways,
7. use VDE-TER connectivity to another MMS mobile Edge Router for exchange of messages to that destination, and
8. use VDE-TER connectivity to use an MMS VDE-TER Gateway if in connectivity range.

#### C.1.6 VDE-TER Shore Network

A VDE-TER Shore Network consists of:

- one or multiple VDE-TER base stations, and
- one or multiple MMS VDE-TER Gateways to connect the VDE-TER Shore Network to the MMS Router Network.

## C.2 VDE-TER transport specific function details

The following sections define additional details that VDE-TER enabled MMS nodes shall comply to.

### C.2.1 MMS VDE-TER Gateway

This section defines the functionality an MMS VDE-TER Gateway shall implement for managing a VDE-TER Network.

#### C.2.1.1 MMS Discovery Shore Base Station Broadcast

The MMS VDE-TER Gateway shall command all connected VDE-TER Shore Base Stations to transmit an MMTP Discovery message within 60 seconds after each terrestrial bulletin board transmission.

Note: These MMTP Discovery message transmissions are received by VDE-TER Mobile Equipment in reach of VDE-TER Base Stations and giving relevant information to VDE-TER enabled mobile MMS Edge Routers.

The MMS Discovery Shore Base Station Broadcast shall be built using an MMTP Discovery message and shall contain:

1. the MRN of the Shore Base Station,
2. the MMSI to which all MMS traffic shall be sent in that corresponding VDE-TER network, and
3. the list of MMS services provided by that VDE-TER network (listing the MRN and the service certificate of that service), and
4. the signature of the VDE-TER Gateway.

#### C.2.1.2 Routing

The MMS VDE-TER Gateway shall route received messages in the associated VDE-TER network locally, and through the connected MMS Router Network globally, according to the gained position information of mobile equipment through authenticated AIS receptions and the MMS Discovery Mobile Messages received by the VDE-TER network's VDE-TER Shore Base Stations.

#### C.2.1.3 VDE-TER Broadcast

The MMS VDE-TER Gateway shall support the transfer of a subject cast message type to all receivers in the same radio range by only transmitting the message once over the air interface. This concept is called for broadcast in [2].

1. The MMS VDE-TER Gateway shall in its local configuration allow to specify a list of subject cast MRNs to subscribe to.
2. The MMS VDE-TER Gateway shall in its local configuration allow to specify a specific repetition interval for each of the base stations that shall transmit the subscribed subject-cast MRNs.
3. The MMS VDE-TER Gateway shall in its local configuration allow to specify a list of VDE-TER basestations per subscribed subject-cast MRN, and for each of them a Link ID to be used to broadcast the service.
4. The MMS Gateway shall transmit all subject-cast messages to the VDE-TER base stations with the MRN specific repetition interval to MMSI=0.

5. The MMS Gateway shall apply the VDES Protocol Format Indicator for MMS, as described in [26], Annex B.3.1.

#### **C.2.1.4 VDE-TER MRN-addressed Message**

The MMS VDE-TER Gateway shall support the transfer of MRN-addressed Messages utilizing VDE-TER according to [2] specifically implementing:

1. application of the VDES Protocol Format Indicator for MMS to all VDE-TER message content, as described in [26], Annex B.3.1.
2. for VDE-TER Shore Base Station to mobile equipment direction:
  - a. setting the VDE-TER message header to the correct MMSI for each separate destination MRN, based on received MMS Discovery Mobile Messages from mobile equipment,
  - b. selecting the best suited Shore Base Station for the transmission to the mobile equipment, based on the size, the expected duration of the transfer, and the position of the mobile equipment;
3. for VDE-TER mobile to Base Station direction:
  - a. validation of the identity of the mobile equipment,
  - b. validation of message integrity,
  - c. queuing of validated messages for further routing.

#### **C.2.1.5 VDE-TER Mobility Management**

Note: The link between a VDE-TER shore base station and a VDE-TER mobile station is subject to permanent changes due to:

- noise floor,
- atmospheric phenomena,
- interference,
- weather,
- tides and waves, impacting the height and the angle of the mobile antenna,
- and other phenomena.

Therefore, the MMS VDE-TER Gateway shall maintain a status about the VDE-TER mobile station reachability through the VDE-TER shore network based on the received mobile discovery messages (see C.2.2.2) containing at least:

1. the position of the VDE-TER mobile station based on the latest authenticated AIS received position,
2. the best VDE-TER basestation to use to send messages to the VDE-TER mobile station, according to the configuration of the MMS VDE-TER Gateway, and
3. the last time, an authenticated AIS position was received.

#### **C.2.1.6 Subscription management**

The MMS VDE-TER Gateway shall handle subscriptions on behalf of the mobile equipment towards the MMS Router Network as described in 6.2, with timeout of subscriptions according to section C.2.1.7.

**C.2.1.7 Automatic Clean-up**

The MMS VDE-TER Gateway shall:

1. clean-up unused memory and message queues after expiration, and
2. clean-up saved subscriptions and mobility management states if a mobile station has not been seen for 15 minutes.

**C.2.1.8 Monitoring**

The MMS VDE-TER Gateway shall, as a minimum, provide following monitoring performance indicators for monitoring of the system through SNMP:

1. number of mobile equipment subscribed through this gateway,
2. number of successfully transferred messages ship-shore,
3. number of successfully transferred messages shore-ship,
4. number of transmitted broadcast messages,
5. number of message transport failures ship-shore,
6. number of message transport failures shore-ship,
7. number of failures in broadcast,
8. number of successfully accepted messages from MMS Router Network,
9. number of successfully routed messages to the MMS Router Network,
10. number of successfully relayed messages ship-shore-ship without access to Router Network,
11. number of errors in MMS headers,
12. number of connected VDE-TER base stations,
13. number of total VDE-TER base station transmissions per base station,
14. number of total VDE-TER base station received messages per base station,
15. number of messages in queue for each priority.

**C.2.2 VDE-TER enabled ship MMS Edge Router****C.2.2.1 AIS Authenticated Message**

The MMS VDE-TER enabled mobile MMS Edge Router shall transmit a VDES message to authenticate one AIS position report at least every 300 seconds, according to [26], Annex B.2.8.

In case the mobile equipment is in a base station controlled area, the VDES message is addressed to the MMSI indicated for MMS in the MMS Discovery Shore Base Station Broadcast.

Outside of base station controlled areas, the VDES message is transmitted as broadcast to MMSI=0.

Note: this transmission provides the MMS VDE-TER Gateway and other MMS VDE-TER enabled mobile Edge Routers with the capability to validate authenticity and integrity of the AIS information of the VDES station for routing and optimal transmission resource selection purposes.

**C.2.2.2 MMS Discovery Mobile Message**

The MMS VDE-TER enabled mobile MMS Edge Router shall transmit an MMS discovery mobile Message to the subject "vdes-mms-discovery", which shall:



1. be attempted to be sent using the TDB PI interface sentence (see [1], A.3.1) every 300 seconds,
2. contain an MMTP Discovery message containing:
  - a. the MRN of the Mobile Edge Router,
  - b. the MMSI to which all MMS traffic shall be sent,
  - c. the list of MMS services provided by the Agents that are connected to that VDE-TER enabled ship MMS Edge Router (listing the MRN and the service certificate of that service). Examples may include:
    - i. reception of S-100 documents, e.g. S-421 for route exchange or search and rescue search patterns;
    - ii. reception of authenticated text messages in UTF-8 format, and
  - d. and the signature of the mobile Edge Router.

Note: the purpose of the discovery mobile message is to inform MMS Edge Routers on shore and other ships about a ships MMS capabilities and identity.

The message shall be sent to VDES MMSI = 0 as a broadcast.

In base station control areas, a directed VDES message, shall be used to transfer the above content, addressed to the VDES MMSI indicated by the latest received MMS Discovery Shore Base Station Broadcast.

#### **C.2.2.3 VDE-TER Mobility Management**

Note: The link between a VDE-TER stations are subject to permanent changes due to:

- noise floor,
- atmospheric phenomena,
- interference,
- weather,
- obstacles (like other ships),
- tides and waves, impacting the height and the angle of the mobile antenna,
- and other phenomena.

Therefore, the VDE-TER enabled ship MMS Edge Router shall maintain a status about other VDE-TER station's reachability through the VDE-TER shore network based on the received mobile discovery messages (see [14.2.2.2](#)) containing at least:

1. the position and time of other received VDE-TER stations based on the latest AIS received position,
2. the states and services indicated in received MMS Discovery Mobile Messages,
3. the best VDE-TER shore base station to use, considering the bulletin board of all base stations as to their coverage areas, local configuration of the MMS VDE-TER Gateway, and signal strength.

#### C.2.2.4 Send Direct Message via Base Station

When in the transmission range of a VDE-TER Gateway, as defined by the VDE-TER Base Station bulletin board, a VDE-TER enabled ship MMS Edge Router shall:

1. attempt to transmit all queued messages that are allowed for transmission through that VDE-TER Shore Network,
2. in order of their indicated priority.

#### C.2.2.5 Send Direct Message via Ship to Ship

When not in the transmission range of a VDE-TER Base Station, as defined by the bulletin board, a VDE-TER enabled ship MMS Edge Router shall:

1. attempt to transmit all queued messages that are allowed for transmission through direct messaging via VDE-TER,
2. to the destinations that are in reception range, as identified through its own VDE-TER Mobility Management function,
3. in order of their indicated priority.

#### C.2.2.6 Receive Messages

When the VDE-TER enabled ship MMS Edge Router receives messages from the VDE-TER network through VDES Mobile Equipment, it shall:

1. reassemble the MMS message from the VDES fragments delivered over the Presentation Interface,
2. ensure that the MMS message is complete and following the MMTP protocol,
3. continue to process the MMS message according to 6.2.

### C.3 VDE-TER Discover Protocol Message

The *discover* protocol message shall be sent by either

4. A VDE-TER enabled ship MMS Edge Router, or
5. A VDE-TER Gateway

to allow discoverability of an MMS capable ship or shore VDES station by other ships or shore VDES stations.

The *discover* protocol message shall contain:

- a *MRN* for identification of the sender of this message, shall be an MRN no longer than 100 characters,
- a *MMSI* for identification of the VDES equipment used,
- the current position, identified by *latitude* and *longitude*,
- a list of services in the *service* field,
- an indication if service forwarding is possible in the *forwardingEnabled* field,
- a *timestamp*, value is seconds after the 1st of January 1970; shall be the timestamp when the message content was created in seconds since the 1st of January 1970, 00:00:00 UTC,
- a *signature*, containing the bytes of a signed hash of the message header and body, signed with the MCP private key associated with the sender MRN in the context of the MCP MIR.

Signing follows the following algorithm, where the byte encoding of a string is assumed to be UTF-8:

- a. Allocate an empty list of bytes *B*,
- b. Encode the value of *MRN* as bytes and append the result to *B*,
- c. Encode the decimal string representation of the value of *MMSI* as bytes and append the result to *B*,
- d. Encode the decimal string representation of the value *latitude* as bytes and append the result to *B*,
- e. Encode the decimal string representation of the value *longitude* as bytes and append the result to *B*,
- f. For each service encode the *serviceMRN* as bytes and append results to *B*, append afterwards the *servicecertificate* to *B*,
- g. Encode the decimal string representation of the value *forwardingEnabled* as bytes and appended the result to *B*,
- h. Encode the decimal string representation of the value *timestamp* as bytes and append the result to *B*,
- i. Give *B* and private key as inputs to the signing algorithm defined by [12] Section 6.4.1 and store the output values *r* and *s*,
- j. DER encode *r* and *s* using the ASN.1 structure defined by [13] Section 2.2.3 and return the result.

The signature shall be verified by the receiving entity, following the signature verification algorithm defined [12] Section 6.4.2.

The following protobuf code does implement the required normative structure:

```
syntax = "proto3";
```

```
message VdeTerDiscover{
  string MRN = 1;
  uint64 MMSI = 2;
  float latitude = 3;
  float longitude = 4;
  repeated Service service = 5;
  bool forwardingEnabled = 6;
  uint64 timestamp = 7;
  bytes signature = 8;
}
```

```
message Service{
  string ServiceMRN = 1;
  bytes ServiceCertificate = 2;
}
```

## Annex D (informative)

### MMS Binding for VDE-SAT Networks

VDES contains a satellite component for ship to ship, ship to shore, shore to ship transfers of messages called VDE-SAT, see [2], General section and Annex 5 for details.

This Annex describes the bindings and functionality that shall be implemented by MMS equipment providing transport of MMS messages over a VDE-SAT network.

#### D.1 Entities overview

This chapter introduces the entities that shall provide additional functionality to support MMS messages over VDE-SAT. An overview over the system is shown in Figure 22.

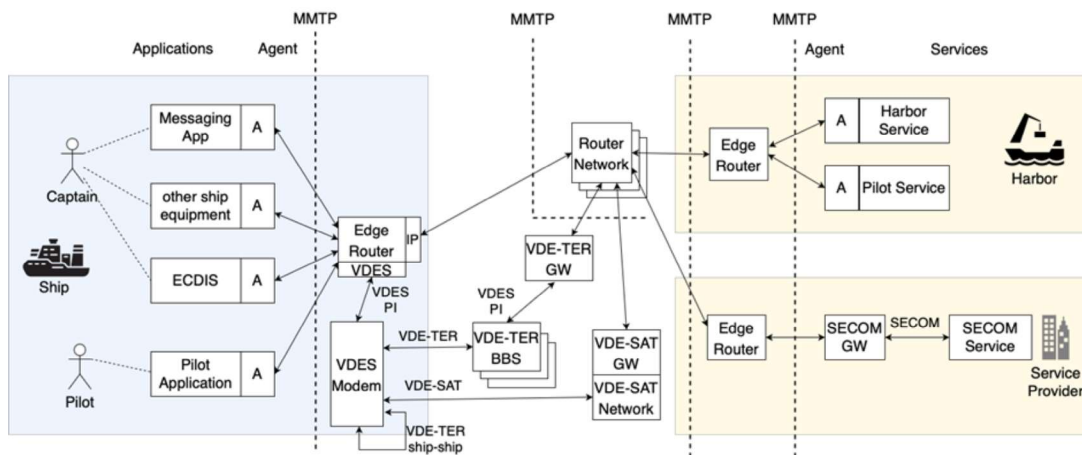


Figure 22 – Overview of MMS system architecture with VDE-SAT network.

##### D.1.1 VDE-SAT Satellite Station

VDE-SAT Satellite Stations provide the VDE-SAT radio access for VDE-SAT mobile equipment.

Note: VDE-SAT Satellite Stations are usually in Low Earth Orbit (LEO), i.e. circling around the earth. As the satellites are not geostationary, they are visible only for several minutes at a time from one given point on earth, giving short windows of communication opportunity. VDE-SAT Satellite Stations also may not have permanent ground connectivity to the shore segment. The MMS store-and-forward concept is compatible with these limitations, but also can leverage cases, where more permanent connectivity is available.

VDE-SAT Satellite Stations coordinate the VDE-SAT resources for all connectivity between mobile VDE-SAT equipment and themselves according to [2].

MMS enabled VDE-SAT Satellite Stations shall contain an MMS VDE-SAT Edge Router Function that can operate without a real-time connection to the MMS VDE-SAT Gateway.

##### D.1.2 VDE-SAT Satellite Network

A VDE-SAT Satellite Network consists of:

- one or multiple VDE-SAT Satellite Stations,
- optional direct connections between these VDE-SAT Satellite Stations, and

- one or multiple MMS VDE-SAT Gateways to connect the VDE-SAT Satellite Network with the MMS Router Network.

### D.1.3 MMS VDE-SAT Gateway

An MMS VDE-SAT Gateway provides a link between the MMS Router Network and one or multiple VDE-SAT Satellite Stations.

An MMS VDE-SAT Gateway shall conform to 6.2 and additionally perform at least following functions:

1. broadcast information about MMS capabilities for VDE-SAT enabled mobile MMS Edge Routers over all VDE-SAT Satellite Stations with necessary information about available services and MMSI mappings applicable,
2. maintain routing and MMSI mapping to reach subscribed own MRN's via VDE-SAT as long as these are reachable via the VDE-SAT network,
3. subscribe to MRNs with the MMS Router Network on behalf of the VDE-SAT connected mobile MMS Edge Routers in the VDE-SAT network,
4. send messages from the MMS Router Network to MRNs in coverage of the VDE-SAT Network, utilizing its VDE-SAT Satellite Stations,
5. using the VDE protocol format header layer to identify MMS traffic according to [26], Annex B.3.1,
6. priority based queuing of messages with mobile destinations where the target MRN is not reachable until a timeout happens,
7. forward MMS messages received through the VDE-SAT Satellites to the destination if it can be reached locally in the VDE-SAT Network,
8. forward MMS messages received through the VDE-SAT Network to the MMS Router Network for routing, where local routing immediately via VDE-SAT in the same coverage area is not possible,
9. apply cleaning of its buffers, own routing and mapping tables when ships have left the coverage area.

Note: applicable standard MMS services that an MMS VDE-SAT Gateway may provide and announce to be available through VDE-SAT broadcasts are:

- MIR query service to retrieve public certificates to support end-to-end encryption of MMS messages between MMS Agents, e.g. ship-ship,
- MIR revocation service,
- MSR query interface, to retrieve service certificates for services transported over that VDE-SAT Shore Network

### D.1.4 VDE-SAT Link

The link between the VDE-SAT Satellite Station and the VDE-SAT Mobile Equipment utilizes the maritime VHF frequency band according to ITU-R M.2092-1 [2].

In Figure 22, the VDE-SAT Link is labelled “VDE-SAT”.

### D.1.5 VDE-SAT Mobile Equipment

VDE-SAT mobile equipment facilitates communication to other mobile equipment and satellites through VDE-SAT as defined in [2].

Note: typically, VDE-SAT mobile equipment is a VDES Ship Transceiver on board of a ship.

Through such a VDE-SAT communication, the MMS Edge Router is able to transport MMS messages to and from other MMS Edge Routers that are connected to a VDE-SAT mobile or satellite equipment.

Note: MMS message exchange over VDE-SAT is enabled to use:

- ship to ship, and
- ship to shore and shore to ship.

VDE-SAT mobile equipment shall conform with [2] General section and Annex 4, and shall be type approved by [1].

VDE-SAT mobile equipment shall provide a Presentation Interface to the mobile MMS Edge Router as defined in [1].

Note: the VDE-SAT presentation interface is based on VDE-SAT specific sentences as defined in [1], transported over lightweight ethernet [28] standard providing NMEA/UDP/IP. This interface is labelled “VDES PI” in Figure 22.

#### **D.1.6 VDE-SAT enabled mobile MMS Edge Router**

A VDE-SAT enabled mobile MMS Edge Router is an MMS Edge Router providing the MMTP interface to MMS Agents as described in 6.2, that is capable to use VDE-SAT for transport of MMS messages to other VDE-SAT equipment that is connected to VDE-SAT enabled Shore and Mobile Edge Routers.

To use VDE-SAT transport in the MMS, a mobile MMS Edge Router shall support VDE-SAT mobile equipment's NMEA interface as defined in [1] and shall implement additional functionality:

1. manage a local root certificate storage for the authentication of VDE-SAT bulletin boards,
2. update the local certificate storage based on revocations send through an MMS MIR revocation service,
3. update the local certificate storage based on certificates received from trusted MMS VDE-SAT Gateways, for services the Edge Router itself subscribes to,
4. provide access to the local certificate storage for local MMS Agents and VDE-SAT mobile equipment, using the MMS certificate query service interface,
5. decide to use or not use a VDE-SAT Satellite Stations based on local trust settings as to which VDE-SAT networks to trust, based on the VDE-SAT bulletin board signature received from each VDE-SAT Satellite Station,
6. receive and act upon MMS discovery broadcasts from MMS VDE-SAT Satellite Stations,
7. use VDE-SAT connectivity to an MMS VDE-SAT Gateway.

#### **D.1.7 VDE-SAT Satellite Network**

A VDE-SAT Satellite Network consists of:

- one or multiple VDE-SAT Satellite Stations, and
- one or multiple MMS VDE-SAT Gateways to connect the VDE-SAT Satellite Network to the MMS Router Network.

### **D.2 VDE-SAT transport specific function details**

The following sections define additional details VDE-SAT enabled MMS nodes shall comply to.

#### **D.2.1 VDE-SAT Satellite Edge Router**

An MMS enabled VDE-SAT Satellite shall contain an MMS VDE-SAT Edge Router Function.

The VDE-SAT Satellite Edge Router Function shall support following general functionality:

1. operate autonomously without a real-time connection to the MMS VDE-SAT Gateway,
2. synchronize relevant policies and data from the MMS VDE-SAT Gateway to the Satellite when connectivity is available:
  - a. last known positions of all ships that are known to be equipped with MMS and VDE-SAT, for autonomous routing in the satellite,
  - b. downlink directed and subject-cast messages, with time window when to transmit them, and at which priority,
  - c. antenna pointing information,
  - d. bulletin board updates,
3. synchronize relevant data and metrics from the MMS VDE-SAT Satellite Station back to the VDE-SAT Gateway:
  - a. satellite received uplink addressed MMS messages that could not be delivered directly to the destination before the next contact to a VDE-SAT Gateway,
  - b. Satellite received authenticated position reports from ships back to the VDE-SAT Gateway,
  - c. metrics to assist performance evaluation of the VDE-SAT link and improvement of the standards:
    - received signal strength on both mobile and satellite modem for each VDE-SAT subframe for each addressed up- and downlink message transfer with MMSI,
    - grand total number of failed addressed uplink transfers, per MMSI
    - grand total number of ignored uplink requests by reason, per MMSI
    - grand total number of successfully acknowledged UL fragments by LinkID, per MMSI
    - grand total number of successfully acknowledged addressed DL fragments by LinkID, per MMSI

The VDE-SAT Satellite Edge Router Function shall support following uplink support functionality:

1. act upon VDE-SAT uplink data requests from VDE-SAT mobile equipment, deciding how many and which resources to assign to each requested transfer,
2. based on local policies synchronized from the VDE-SAT Gateway,
3. selecting a well-suited VDE-SAT LinkID for all uplink message exchange with VDE-SAT mobile equipment,
4. stopping the assignment of resources on VDE-SAT uplink message requests where no routing to the MMS destination is supported by the VDE-SAT Network, controlled through policies synchronized with the VDE-SAT Gateway,
5. queue received VDE-SAT uplink MMS messages (identified as MMS according to [26], Annex B.3.1) for transmission to the MMS VDE-SAT Gateway at next opportunity and according to the message priority,
6. directly route messages between mobile equipment, applying local policies (Note: ship-satellite-ship without VDE-SAT Gateway involvement, e.g. for arctic use cases),

The VDE-SAT Satellite Edge Router Function shall support following downlink functionality:

1. queue MRN-addressed MMS messages as addressed VDE-SAT messages to the specified MMSI using VDE-SAT link,
2. queue subject cast MMS messages as VDE-SAT broadcast to MMSI=0, i.e. to all receivers in its coverage area, repetitively and in areas, designated by the information included in the VDE-SAT Gateway,
3. schedule transmission of the queued MMS messages to mobile equipment,
4. based on their last known location and directly received AIS signals on the satellite,
5. selecting a well-suited VDE-SAT LinkID for all downlink message exchange with VDE-SAT mobile equipment,
6. be able to exchange firmware in order to adapt to changes of this standard,

### **D.2.2 MMS VDE-SAT Gateway**

This section defines the functionality an MMS VDE-SAT Gateway shall implement for managing a VDE-SAT Network.

#### **D.2.2.1 Protected areas**

The MMS VDE-SAT Gateway shall allow in its local configuration to specify areas where

1. no transmissions are allowed to respect ITU defined radioastronomy sites, or
2. a defined maximum transmission level is not exceeded,

in order to keep operator-specific agreements over these areas, e.g. to apply ITU-R Radio regulations footnote 5-288.AC.

#### **D.2.2.2 MMS Discovery Satellite Station Broadcast**

The MMS VDE-SAT Gateway shall command all connected VDE-SAT Satellite Stations to transmit an MMTP Discovery message within 60 seconds after each satellite bulletin board transmission.

Note: These MMTP Discovery message transmissions are received by VDE-SAT Mobile Equipment in reach of VDE-SAT Satellite Stations giving relevant information to VDE-SAT enabled mobile MMS Edge Routers.

The MMS Discovery Satellite Station Broadcast shall be built using an MMTP Discovery message and shall contain:

1. the MRN of the VDE-SAT Gateway,
2. the MMSI to which all MMS traffic shall be sent in that corresponding VDE-SAT network, and
3. the list of MMS services provided by that VDE-SAT network (listing the MRN and the service certificate of that service), and
4. the signature of the VDE-SAT Gateway.

#### **D.2.2.3 Routing**

The MMS VDE-SAT Gateway shall route received messages in the associated VDE-SAT network locally, and through the connected MMS Router Network globally, according to the gained position information of mobile equipment through authenticated AIS receptions and the MMS Discovery Mobile Messages received by the VDE-SAT network's VDE-SAT Satellite Stations.



#### **D.2.2.4 VDE-SAT Broadcast**

The MMS VDE-SAT Gateway shall support the transfer of a subject cast message type to a large number of receivers in the VDE-SAT coverage path on earth by transmitting the message repeatedly over the air interface. This concept is called for broadcast in [2].

1. The MMS VDE-SAT Gateway shall in its local configuration allow to specify a list of subject cast MRNs to subscribe to.
2. The MMS VDE-SAT Gateway shall in its local configuration allow to specify a specific repetition interval for each of the base stations that shall transmit the subscribed subject-cast MRNs.
3. The MMS VDE-SAT Gateway shall in its local configuration allow to specify a broadcast areas per subscribed subject-cast MRN, and for each of them a Link ID to be used to broadcast the service.
4. The MMS VDE-SAT Gateway shall from its local configuration, calculate a transmit schedule, including pointing for the VDE-SAT antenna, for each VDE-SAT Satellite Station.
5. The MMS Gateway shall transmit all subject-cast messages to the VDE-SAT Satellite Stations, containing:
  - a. the MRN specific repetition interval,
  - b. the VDE-SAT destination MMSI=0, and
  - c. the time when the transmissions shall be repeatedly sent.
6. The MMS Gateway shall apply the VDES Protocol Format Indicator (VPFI) for MMS, as described in [26], Annex B.3.
7. The MMS Gateway shall, between the VPFI and the MMTP payload apply the MMS VDE-SAT specific Header as defined in [\[sec:VdeSatHdr\]](#).

#### **D.2.2.5 VDE-SAT MRN-addressed Messages**

The MMS VDE-SAT Gateway shall support the transfer of MRN-addressed Messages utilizing VDE-SAT according to [2] specifically implementing:

1. application of the VDES Protocol Format Indicator for MMS to all VDE-SAT message content, as described in [26], Annex B.3.1.
2. for VDE-SAT Satellite Station to mobile equipment direction:
  - a. setting the VDE-SAT message header to the correct MMSI for each separate destination MRN, based on received MMS Discovery Mobile Messages from mobile equipment,
  - b. selecting the best suited Satellite for the transmission to the mobile equipment, based on the size, the expected duration of the transfer, and the position of the mobile equipment;
3. for VDE-SAT mobile equipment to Satellite Station direction:
  - a. validation of the identity of the mobile equipment,
  - b. validation of message integrity,
  - c. queuing of validated messages for further routing.

#### **D.2.2.6 VDE-SAT Mobility Management**

Note: The link between a VDE-SAT shore base station and a VDE-SAT mobile equipment is subject to permanent changes due to:

- satellite orbital movement,
- satellite antenna pointing performance,
- noise floor,
- atmospheric phenomena,
- interference,
- weather,
- tides and waves, impacting the height and the angle of the mobile antenna,
- and other phenomena.

Therefore, the MMS VDE-SAT Gateway shall maintain a status about the VDE-SAT mobile station reachability through the VDE-SAT network based on the received mobile discovery messages (see [15.2.3.2](#)).

#### **D.2.2.7 Subscription management**

The MMS VDE-SAT Gateway shall handle subscriptions on behalf of the mobile equipment towards the MMS Router Network as described in [6.2](#), with timeout of subscriptions according to section [15.2.2.8](#).

#### **D.2.2.8 Automatic Clean-up**

The MMS VDE-SAT Gateway shall:

1. clean-up unused memory and message queues after expiration, and
2. clean-up saved subscriptions and mobility management states if a mobile station has not been seen for 48 hours.

#### **D.2.2.9 Monitor Connection States**

The MMS VDE-SAT Gateway shall, as a minimum, provide following monitoring performance indicators for monitoring of the system through SNMP:

1. number of mobile equipment subscribed through this gateway,
2. number of successfully transferred messages ship-satellite,
3. number of successfully transferred messages satellite-ship,
4. number of transmitted broadcast messages,
5. number of message transport failures ship-satellite,
6. number of message transport failures satellite-ship,
7. number of failures in broadcast,
8. number of successfully accepted messages from MMS Router Network,
9. number of successfully routed messages to the MMS Router Network,
10. number of successfully relayed messages ship-satellite-ship without access to Router Network,

11. number of errors in MMS headers,
12. number of currently connected VDE-SAT satellite stations,
13. number of total VDE-SAT satellite station transmissions per satellite station,
14. number of total VDE-SAT satellite station received messages per satellite station,
15. number of messages in queue for each priority.

### **D.2.3 VDE-SAT enabled ship MMS Edge Router**

#### **D.2.3.1 AIS Authenticated Message**

The MMS VDE-SAT enabled mobile MMS Edge Router shall attempt to transmit a VDE-SAT message to authenticate one AIS position report at least every 2 hours, according to [26], Annex B.2.8 and when connected to a VDE-SAT satellite using the MMSI given in the MMS Discovery Satellite Station Broadcast.

Note: this transmission provides the MMS VDE-SAT Satellite Edge Router and the VDE-SAT Gateway with the capability to validate authenticity and integrity of the AIS information of the VDES station for routing and optimal transmission resource selection purposes.

#### **D.2.3.2 MMS Discovery Mobile Message**

The MMS VDE-SAT enabled mobile MMS Edge Router shall attempt to transmit an MMS Discovery Mobile Message to the subject “vdes-mms-discovery” every 48 hours, which shall:

1. be attempted to be sent using the SUM PI interface sentence (see [1], A.4.4) once per day during VDE-SAT Satellite Station visibility.
2. contain an MMTP Discovery message containing:
  - a. the MRN of the Mobile Edge Router,
  - b. the MMSI to which all MMS traffic shall be sent,
  - c. the list of MMS services provided by the Agents that are connected to that VDE-SAT enabled ship MMS Edge Router (listing the MRN and the service certificate of that service). Examples may include:
    - i. reception of S-100 documents, e.g. S-421 for route exchange or search and rescue search patterns, and
    - ii. reception of authenticated text messages in UTF-8 format;
  - d. and the signature of the mobile Edge Router.

#### **D.2.3.3 VDE-SAT Mobility Management**

Note: The link between a VDE-SAT stations is subject to permanent changes due to:

- satellite orbital movement,
- satellite antenna pointing performance,
- noise floor,
- atmospheric phenomena,
- interference,
- weather,

- tides and waves, impacting the height and the angle of the mobile antenna,
- and other phenomena.

Therefore, the VDE-SAT enabled ship MMS Edge Router shall maintain a status about VDE-SAT satellite networks based on the received mobile discovery messages (see D.2.3.2) containing at least:

1. the MMS enabled VDE-SAT networks seen during the last 48 hours,
2. the states and services indicated in received MMS Discovery Mobile Messages per VDE-SAT network,
3. the orbital data from the VDE-SAT networks, decoding orbital data as described in [26], Annex B.1.1 to predict next availability of the usable MMS enabled VDE-SAT networks.

#### **D.2.3.4 Send Direct Message to Satellite**

When in the transmission range of a VDE-SAT Satellite Station, a VDE-SAT enabled ship MMS Edge Router shall:

1. attempt to transmit all queued messages that are allowed for transmission through that VDE-SAT Network according to local policies,
2. in order of their indicated priority,
3. applying the VDES Protocol Format Indicator for MMS to all VDE-SAT message content, as described in [26], Annex B.3.1.

#### **D.2.3.5 Receive Messages**

When the VDE-SAT enabled ship MMS Edge Router receives messages from the VDE-SAT network through VDES Mobile Equipment, it shall:

1. reassemble the MMS message from the VDES fragments delivered over the Presentation Interface,
2. ensure that the MMS message is complete and following the MMTP protocol,
3. continue to process the MMS message according to 4.2,
4. applying the VDES Protocol Format Indicator for MMS to all VDE-SAT message content, as described in [26], Annex B.3.1, and
5. for VDE-SAT broadcast messages, use the MMS VDE-SAT specific Header as defined in D.3, to attempt reassembly of a complete MMTP message from retransmitted fragments.

### **D.3 VDE-SAT Fragment Header**

For each VDES fragment sent to contain MMTP over VDE-SAT, a specific header shall be applied inside the header as defined in [26], Annex B.3.1.

The header shall contain 32 bits in total:

1. Bit 0-7: MMTP VDE-SAT message Session ID,
2. Bit 8-19: Number of Fragments in this Session,
3. Bit 19-31: Number of this Fragment in the Session.

This header shall be used for fragmentation and reassembly of one MMTP message into multiple VDES fragments, making it possible to reconstruct MMTP messages from multiple receptions of the same MMTP message in different VDE-SAT sessions.

#### D.4 VDE-SAT Discover Protocol Message

The *discover* protocol message shall be sent by either

1. A VDE-SAT enabled ship MMS Edge Router, or
2. A VDE-SAT Satellites

to allow discoverability of an MMS capable ship or satellite VDES station.

The *discover* protocol message shall contain:

- a *MRN* for identification of the sender of this message, shall be an MRN no longer than 100 characters,
- a *MMSI* for identification of the VDES equipment used,
- the current position, identified by *latitude* and *longitude*,
- two satellite orbit descriptions *TLE1* and *TLE2*,
- a list of services in the *service* field,
- a *timestamp*, value is seconds after the 1st of January 1970; shall be the timestamp when the message content was created in seconds since the 1st of January 1970, 00:00:00 UTC,
- a *signature*, containing the bytes of a signed hash of the message header and body, signed with the MCP private key associated with the sender MRN in the context of the MCP MIR. Signing follows the following algorithm, where the byte encoding of a string is assumed to be UTF-8:
  - a. Allocate an empty list of bytes *B*,
  - b. Encode the value of *MRN* as bytes and append the result to *B*,
  - c. Encode the decimal string representation of the value of *MMSI* as bytes and append the result to *B*,
  - d. Encode the value *TLE1* as bytes and append the result to *B*,
  - e. Encode the value *TLE2* as bytes and append the result to *B*,
  - f. For each service encode the *serviceMRN* as bytes and append results to *B*, append afterwards the *servicecertificate* to *B*,
  - g. Encode the decimal string representation of the value *timestamp* as bytes and append the result to *B*,
  - h. Give *B* and private key as inputs to the signing algorithm defined by [12] Section 6.4.1 and store the output values *r* and *s*,
  - i. DER encode *r* and *s* using the ASN.1 structure defined by [13] Section 2.2.3 and return the result.

The signature shall be verified by the receiving entity, following the signature verification algorithm defined [12] Section 6.4.2.

The following protobuf code does implement the required normative structure:

```
syntax = "proto3";
```

```
message VdeSatDiscover{
  string MRN = 1;
```

RTCM 13900.0

– 94 –

```
uint64 MMSI = 2;  
string TLE1 = 3;  
string TLE2 = 4;  
repeated Service service = 5;  
int64 timestamp = 6;  
bytes signature = 7;  
}  
  
message Service{  
  string ServiceMRN = 1;  
  bytes ServiceCertificate = 2;  
}
```

**Annex E**  
(informative)

**Annex MMS Binding for ITU-R M.2116 [29]**

Recommendation ITU-R M.2116-0, to be revised, provides a technical description of the technology that is used to support aeronautical and maritime applications. The International Radio Regulations designate a band for the aeronautical and maritime services on a primary basis, but it may be limited by the future World Radio Communications Conference in 2027 (WRC-27) to this band, and terrestrial services may be permitted to share it on a secondary basis with limitations on the power flux density mask to be decided. Nevertheless, the band is expected to continue to be available to the maritime services on a primary basis. Ships with an appropriate server should be able to support access to this band by for extended high bandwidth applications.

## **Annex F** (informative)

### **Annex MMS Binding for NAVDAT**

#### **F.1 Introduction**

The ITU NAVDAT recommendations [30] and [31] define a broadcast message service operating in the MF and HF bands, with a very large transmission range from a single transmitter. NAVDAT is an evolution of NAVTEX. NAVDAT can transmit these messages from shore to ship stations but cannot receive any messages from ships back to shore.

MF NAVDAT transfer rates, including forward error correction with coding rates of 0.5 to 0.75, vary between 5 and 27 kbit/s. See [30] section 2.

HF NAVDAT transfer rates, including forward error correction with coding rates of 0.5 to 0.75, vary between 6 and 29 kbit/s. See [30] section 2.

The NAVDAT system can use 4 bandwidths: 1, 3, 5, or 10 kHz.

This Annex describes the bindings and functionality that shall be implemented by MMS equipment providing subject-cast message transport of MMS messages over NAVDAT.

#### **F.2 Background and Notes**

A performance standard for NAVDAT is currently under development by IMO to become a transport medium for Safety of Navigation communications. The IMO NCSR correspondence group also works on consequential amendments to their work back to the ITU recommendations.

NAVDAT can be made compatible with MMS by designating a specific “Subject of message” code for MMS, as shown in Table 29 in [30] and Table 29 in [31]. The addition of MMS could happen by replacing the text “Reserved” with “MMS” for Subject Message code “50” in these tables (TBC).

#### **F.3 Entities Overview**

This chapter introduces the MMS entities that shall provide additional functionality to support the transport of MMS subject-cast messages over MMS.

An overview of the system is shown in Figure 23 of this Annex.



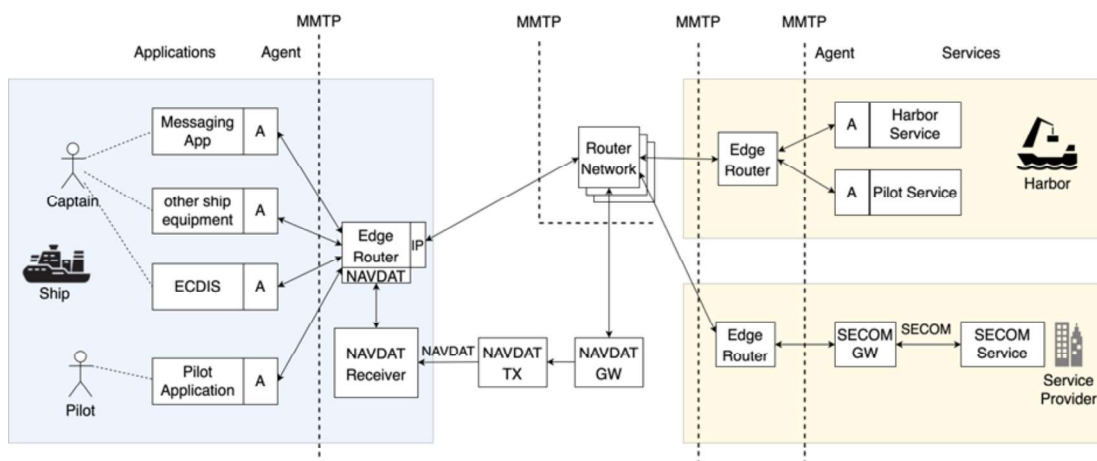


Figure 23 – Overview of MMS system architecture with NAVDAT.

### F.3.1 NAVDAT Transmitter Station

The NAVDAT Transmitter Station transports digital subject-cast data as NAVDAT broadcast according to the ITU NAVDAT Recommendations [30] and [31] between shore and ship in MF and HF bands, respectively.

### F.3.2 NAVDAT Ship Receiver

The NAVDAT ship receiver receives the NAVDAT transmissions from the NAVDAT Transmitter Station according to relevant equipment standards to implement IMO performance requirements (under development).

According to A3-4.1.7 of [31] and 4.1 of [30], the NAVDAT ship receiver outputs received NAVDAT messages through an IEC 61162 series interface.

### F.3.3 MMS NAVDAT Gateway

An MMS NAVDAT Gateway provides a link between the MMS Router Network and one or multiple NAVDAT Transmitter Stations.

Note: The main task for the MMS NAVDAT Gateway is to set the NAVDAT message head field values according to Table 26 of [31] and Table 27 of [30], see details below.

An MMS NAVDAT Gateway is an Edge Router and shall conform to 4.2. Additionally, an MMS NAVDAT Gateway shall perform at least the following functions:

1. Allow specifying in a local configuration which subject-cast MRNs to broadcast and when.
2. Allow specifying for each of the MRNs the corresponding settings for the NAVDAT message head settings, including at least the following settings:
  - a. Broadcast mode, default = 00 General broadcast.
  - b. Detail of Broadcast modes, default = 0x0000 0000 0.
  - c. Detail of Broadcast mode 11, default = 00, shall be possible to be set to a 4-position polygon according to Note of Table 20 of [31] and Table 22 of [30].
  - d. Priority.
  - e. Alternatively, offer a logic that can set some or all of these values independently of local config based on information from the MSR.

3. Calculation of how many times the exact same subject-cast MMTP message was repeated to set the value Broadcast count of the NAVDAT message head properly.
4. Setting the NAVDAT message head Numbering of message number using the full range available between consecutive messages.
5. Subscribe to MRNs with the MMS Router Network based on its local configuration.
6. Send subject-type messages from the MMS Router Network to NAVDAT receivers in coverage of the NAVDAT Transmitter Station.
7. Setting the NAVDAT message head Subject of message code 50 to identify the NAVDAT data as MMS traffic.
8. Automatically calculating the NAVDAT message head settings:
  - a. Length of data.
  - b. Total packets.
  - c. Length of file.
  - d. CRC.
9. Segment the MMS MMTP message, if necessary, such that a NAVDAT receiver can assemble it correctly again after receipt.
10. Attach the MMS message segments in MMTP format as NAVDAT binary content to the NAVDAT message.

#### **F.3.4 NAVDAT enabled mobile MMS Edge Router**

A NAVDAT enabled MMS Edge Router is an MMS Edge Router providing the MMTP interface to MMS Agents as described in 4.2, that is capable of receiving MMS messages via NAVDAT from NAVDAT Transmitter Stations.

To use NAVDAT transport in the MMS, a mobile MMS Edge Router shall support the NAVDAT receiver interface as defined in A3-4.1.7 of [31] and 4.1 of [30] and implement additional functionality:

1. Distinguish all NAVDAT messages with Subject of message code 50 to be interpreted as MMS messages following the MMTP protocol.
2. Reconstruct the MMTP messages from the received NAVDAT messages.
3. Transport the MMTP messages to the connected MMS Agents that are subscribed to the subject-type of the via NAVDAT received MMTP messages.

The NAVDAT enabled mobile MMS Edge Router may include an optional application that is subscribing to a maritime subject-cast service providing S-123 based Marine Radio Services information.

After validation of integrity and authenticity, the data may be used to add additional NAVDAT receiver station information automatically to the NAVDAT receiver.

## **Annex G** (informative)

### **Annex MMS Binding for SECOM**

The SECOM IEC standard [24] defines an interface for shore services.

This Appendix describes how MMS bridges the “last mile”, i.e. connecting the ship’s applications to SECOM services, allowing the transfer of SECOM services over all MMS supported transport media as e.g. internet access (Inmarsat BGAN/VSAT, Iridium NEXT, Starlink) and maritime dedicated digital communications such as terrestrial or satellite VDES and NAVDAT.

#### **G.1 Entities Overview**

This chapter introduces the MMS entities that shall provide functionality to support the transport of SECOM services over MMS.

##### **G.1.1 SECOM Service**

The SECOM Service is implementing a service that shall be transported over MMS using the interface defined by the IEC SECOM Standard [24].

This service shall be supporting:

1. the mandatory interfaces Capability and Ping according to [24], Section 5.7.1,
2. subscription to the container type S100\_ExchangeSet according to [24], Table 51,
3. delivering the envelopeUploadObject, as defined in [24], Table 16, with the upload object
  - a. containing always the mandatory envelopeSignature, and
  - b. containing the envelope, consisting of the zipped S100\_ExchangeSet and all other mandatory data.
4. entries in the MIR and MSR for authentication of the service through the envelopeSignature.

##### **G.1.2 MMS SECOM Gateway**

The MMS SECOM Gateway is an MMS Agent that shall

1. advertise in its SECOM Capability interface that it supports the Upload interface,
2. act towards the SECOM Service as a SECOM consumer according to [24], consuming the SECOM Service, and
3. towards the MMS act as an MMS Agent, providing the SECOM Service to the MMS, according to 4.1.

The implementation may differ according to the SECOM Service.

The MMS SECOM Gateway is identified by a unique MRN in the MIR.

For clients to subscribe to the MMS SECOM Gateway, a service identifying MRN is listed separately from the SECOM Service MRN in the MSR. Registrations may use “.mms” as an MRN suffix for SECOM services that are converted to MMS in the MMS SECOM Gateway.

### G.1.3 SECOM Ship Agent

The ship MMS Edge Router shall provide an interface which allows SECOM compatible ship equipment to consume MMS services through the SECOM interface. [how do we do that?]

## G.2 SECOM specific function details

### G.2.1 SECOM Gateway

The SECOM Gateway is an MMS Agent, all requirements of 6.1 apply.

The SECOM Gateway shall authenticate to an MMS Edge Router.

The SECOM Gateway further shall:

1. subscribe to a SECOM service using the Subscription interface of the service with the following attributes for the *SubscriptionRequestObject*:
  - *containerType* shall be set to *S100\_ExchangeSet*,
  - all other attributes for the *SubscriptionRequestObject* can optionally be set according to the configuration of the SECOM Gateway.
2. providing the SECOM data to MMS by connecting to an MMS Edge Router and publishing data received from the SECOM service that it is subscribed to, to a configured subject MRN using the following procedure:
  - a. verify the envelope signature of the received *UploadObject* using the procedure described by [24], Section 7.3.6,
  - b. Base64 decode the value of the *data* attribute from the *envelope* of the *UploadObject* and store it in a temporary variable *temp*,
  - c. following the definition of MMTP given in 7 construct an *MmtpMessage* containing a *Send* where the *body* is set to the value of *temp*, the *subject* set as configured for the Gateway and fill out any other required fields of the *MmtpMessage*,
  - d. send the newly constructed *MmtpMessage* to the connected MMS Edge Router.
3. be registered in an MCP Service Registry [32] with the configured subject MRN as the endpoint URI for the MMS side of the Gateway,
4. be registered in an MCP Service Registry [32] with the root URL of the SECOM API as the endpoint URI for the SECOM side of the Gateway.

The SECOM Gateway may use local policies and configuration to store and/or filter the received SECOM data to facilitate transport into the MMS, e.g.:

- to implement an S-124 service subject cast, fetch the complete list of all active navigational warnings of a Navarea in an agreed interval and redistribute into MMS, setting the MMS Message expiration time to the time when the next update is expected to be available to all clients on all ships;
- according to local policies that are governed by the agreement with the competent authority with regards to how often a service is to be updated and how it is transmitted, e.g. it can be using SMMP or MMTP and if it is transmitted to specific receivers only or as a subject cast.

## Annex H (informative)

### Annex Protobuf Definition of MMTP

```
syntax = "proto3";

message ApplicationMessage {
  ApplicationMessageHeader header = 1;
  bytes body = 2;
  bytes signature = 3;
}

message ApplicationMessageHeader {
  oneof SubjectOrRecipient {
    string subject = 1;
    Recipients recipients = 2;
  }
  int64 expires = 3;
  string sender = 4;
  optional string qosProfile = 5;
  uint32 bodySizeNumBytes = 6;
}

message Recipients {
  repeated string recipients = 1;
}

message MmtpMessage {
  MsgType msgType = 1;
  string uuid = 2;
  oneof body {
    ProtocolMessage protocolMessage = 3;
    ResponseMessage responseMessage = 4;
  }
}

enum MsgType {
  UNSPECIFIED_MESSAGE = 0;
  PROTOCOL_MESSAGE = 1;
  RESPONSE_MESSAGE = 2;
}

message ProtocolMessage {
  ProtocolMessageType protocolMsgType = 1;
  oneof body {
    Subscribe subscribeMessage = 2;
    Unsubscribe unsubscribeMessage = 3;
    Send sendMessage = 4;
    Receive receiveMessage = 5;
    Fetch fetchMessage = 6;
    Disconnect disconnectMessage = 7;
    Connect connectMessage = 8;
    Notify notifyMessage = 9;
  }
}

message Subscribe {
  oneof subjectOrDirectMessages {
    string subject = 1;
```

```

    bool directMessages = 2;
  }
}

message Unsubscribe {
  oneof subjectOrDirectMessages {
    string subject = 1;
    bool directMessages = 2;
  }
}

message Send {
  ApplicationMessage applicationMessage = 1;
}

message Receive {
  optional Filter filter = 1;
}

message Filter {
  repeated string messageUuids = 1;
}

message Fetch {
}

message Disconnect {
}

message Connect {
  optional string ownMrn = 1;
  optional string reconnectToken = 2;
}

message Notify {
  repeated MessageMetadata messageMetadata = 1;
}

enum ProtocolMessageType {
  UNSPECIFIED = 0;
  SUBSCRIBE_MESSAGE = 1;
  UNSUBSCRIBE_MESSAGE = 2;
  SEND_MESSAGE = 3;
  RECEIVE_MESSAGE = 4;
  FETCH_MESSAGE = 5;
  DISCONNECT_MESSAGE = 6;
  CONNECT_MESSAGE = 7;
  NOTIFY_MESSAGE = 8;
}

message ResponseMessage {
  string responseToUuid = 1;
  ResponseEnum response = 2;
  optional string reasonText = 3;
  repeated MessageMetadata messageMetadata = 4;
  repeated MessageContent messageContent = 5;
  optional string reconnectToken = 6;
}

enum ResponseEnum {

```

```
UNSPECIFIED_RESPONSE = 0;
GOOD = 1;
ERROR = 2;
}

message MessageMetadata {
  string uuid = 1;
  ApplicationMessageHeader header = 2;
}

message MessageContent {
  string uuid = 1;
  ApplicationMessage msg = 2;
}
```

## **Annex I** (informative)

### **Annex Protobuf Definition of SMMP**

```
syntax = "proto3";
```

```
message SmpMessage {  
  SmpHeader header = 1;  
  bytes data = 2;  
}
```

```
message SmpHeader {  
  bytes control = 1;  
  uint32 payloadLen = 2;  
  optional uint32 blockNum = 3;  
  optional uint32 totalBlocks = 4;  
  string uuid = 5;  
  repeated string responseToUuid = 6;  
}
```



## Bibliography

- [1] IEC, “IEC 63514 DRAFT: Maritime navigation and radiocommunication equipment and systems – VHF Data Exchange System – Requirements and Methods of testing for shipborne mobile station.”
- [2] ITU, “Technical characteristics for a VHF data exchange system in the VHF maritime mobile band.” <https://www.itu.int/rec/R-REC-M.2092-1-202202-l/en>
- [3] IMO, “IMO e-Navigation strategy implementation plan MSC.1/circ.1595.” [https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/enavigation/MSC.1-Circ.1595%20-%20E-Navigation%20Strategy%20Implementation%20Plan%20-%20Update%201%20\(Secretariat\)%20\(2\).pdf](https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/enavigation/MSC.1-Circ.1595%20-%20E-Navigation%20Strategy%20Implementation%20Plan%20-%20Update%201%20(Secretariat)%20(2).pdf)
- [4] International Organization for Marine Aids to Navigation, “IALA guideline G1183: The provision of Maritime Connectivity Platform (MCP) identities, edition 1.0.” <https://www.iala-aism.org/product/g1183-provison-of-mcp-identities/>
- [5] International Organization for Marine Aids to Navigation, “IALA guideline G1183: The provision of Maritime Connectivity Platform (MCP) identities, edition 1.0.” <https://www.iala-aism.org/product/g1183-provison-of-mcp-identities/>
- [6] S. Cheshire and M. Krochmal, “Multicast DNS.” in RFC 6762. <https://datatracker.ietf.org/doc/html/rfc6762>
- [7] S. Cheshire and M. Krochmal, “DNS-based service discovery.” in RFC 6763. <https://datatracker.ietf.org/doc/html/rfc6763>
- [8] E. Rescorla, “The transport layer security (TLS) protocol version 1.3.” in RFC 8446. 2018. <https://www.rfc-editor.org/rfc/rfc8446>
- [9] G. LLC, “Protocol Buffers Documentation.” <https://protobuf.dev/>
- [10] K. Davis, B. Peabody, and P. Leach, “Universally Unique Identifiers (UUIDs).” in RFC 9562. <https://datatracker.ietf.org/doc/html/rfc9562>
- [11] Management of Maritime Resource Name Organization Identifiers, “IALA guideline G1164, ed 1.1.” <https://www.iala-aism.org/content/uploads/2022/09/G1164-Ed1.1-Management-of-Maritime-Resource-Name-Organisation-Identifiers-December-2021.pdf>
- [12] National Institute of Standards and Technology, “FIPS 186-5 - digital signature standard (DSS).” <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf>
- [13] R. H. W. Polk and L. Bassham, “Algorithms and identifiers for the internet x.509 public key infrastructure certificate and certificate revocation list (CRL) profile.” in RFC 3279. <https://www.rfc-editor.org/rfc/rfc3279.html>
- [14] National Institute of Standards and Technology, “Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography.” <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf>
- [15] National Institute of Standards and Technology, “NIST SP 800-186 - recommendations for discrete logarithm-based cryptography: Elliptic curve domain parameters.” <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-186.pdf>
- [16] Protocol Labs, “libp2p.” <https://libp2p.io/>
- [17] Protocol Labs, “Connection establishment in libp2p.” <https://github.com/libp2p/specs/blob/master/connections/README.md>
- [18] Protocol Labs, “libp2p TLS handshake.” <https://github.com/libp2p/specs/blob/master/tls/tls.md>

- [19] Protocol Labs, “Addressing in libp2p.”  
<https://github.com/libp2p/specs/blob/master/addressing/README.md>
- [20] Protocol Labs, “libp2p kademlia DHT specification.”  
<https://github.com/libp2p/specs/blob/master/kad-dht/README.md>
- [21] Protocol Labs, “PubSub interface for libp2p.”  
<https://github.com/libp2p/specs/blob/master/pubsub/README.md>
- [22] Protocol Labs, “Gossipsub v1.1: Security extensions to improve on attack resilience and bootstrapping.” <https://github.com/libp2p/specs/blob/master/pubsub/gossipsub/gossipsub-v1.1.md>
- [23] I. Fette and A. Melnikov, “The WebSocket Protocol.” in RFC 6455. <https://www.rfc-editor.org/rfc/rfc6455>
- [24] IEC, “IEC 63173-2:2022 maritime navigation and radiocommunication equipment and systems - Data interfaces - Part 2: Secure communication between ship and shore (SECOM).”  
<https://webstore.iec.ch/publication/64543>
- [25] T. Bray, “The JavaScript object notation (JSON) data interchange format.” in RFC 8259.  
<https://www.rfc-editor.org/rfc/rfc8259>
- [26] IALA, “Guideline G1117: G1117 VHF Data Exchange System (VDES) Overview.”  
<https://www.iala-aism.org/product/g1117/>
- [27] IEC, “IEC DRAFT [TBD]: Maritime navigation and radiocommunication equipment and systems – VHF Data Exchange System – Requirements and Methods of testing for shore base station.”
- [28] IEC, “IEC 61162-450:2018 Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 450: Multiple talkers and multiple listeners – Ethernet interconnection.” <https://webstore.iec.ch/publication/28704>
- [29] ITU, “Technical characteristics and protection criteria for the aeronautical mobile service systems operating within the 4 400-4 990 MHz frequency range.” <https://www.itu.int/rec/R-REC-M.2116>
- [30] ITU, “Characteristics of a digital system, referred to as navigational data for broadcasting maritime safety and security related information from shore-to-ship in the 500 kHz band.”  
<https://www.itu.int/rec/recommendation.asp?lang=en&parent=R-REC-M.2010-2-202302-I>
- [31] ITU, “Characteristics of a digital system, referred to as navigational data for broadcasting maritime safety and security related information from shore-to-ship in the maritime HF frequency band.” <https://www.itu.int/rec/recommendation.asp?lang=en&parent=R-REC-M.2058-1-202302-I>
- [32] Maritime Connectivity Platform Consortium, “Maritime service registry of the maritime connectivity platform.”
- [33] International Organization for Marine Aids to Navigation, “IALA guideline G1128: The Specification of e-Navigation technical services, edition 1.2.” 2018. <https://www.iala-aism.org/product/g1128-specification-e-navigation-technical-services/>
- [34] E. Wesley, “Transmission Control Protocol (TCP).” in RFC 9293.  
<https://datatracker.ietf.org/doc/html/rfc9293>
- [35] M. Thomson, “Version-Independent Properties of QUIC.” in RFC 8999.  
<https://datatracker.ietf.org/doc/html/rfc8999>
- [36] J. Iyengar and M. Thomson, “QUIC: A UDP-Based Multiplexed and Secure Transport.” in RFC 9000. <https://datatracker.ietf.org/doc/html/rfc9000>
- [37] M. Thomson and S. Turner, “Using TLS to Secure QUIC.” in RFC 9001.  
<https://datatracker.ietf.org/doc/html/rfc9001>

- [38] J. Iyengar and I. Swett, “QUIC Loss Detection and Congestion Control.” in RFC 9002.  
<https://datatracker.ietf.org/doc/html/rfc9002>