CONTENTS

The Radio Technical Commission for Maritime Services

_____-

MARITIME MESSAGING SERVICE ARCHITECTURE AND PROTOCOL

Committee DRAFT for comment

1 Normative References

2 Terms, Definitions and abbreviated terms

2.1 Terms and Definitions

AtoN Aids to Navigation

EUT Equipment under Test

DHT Distributed Hash Table

GMDSS Global Maritime Distress and Safety System

MCC MCP Consortium

MCP Maritime Connectivity Platform

MIR Maritime Identity Registry

MMS Maritime Messaging Service

MMSI Maritime Mobile Service Identity

MMTP Maritime Message Transfer Protocol

MRN Maritime Resource Name

MSR Maritime Service Registry

QUIC A transport layer network protocol as described by [2], [3], [4] and [5]

SMMP Secure Maritime Message Protocol

TCP Transmission Control Protocol as described by [6]

TTL Time to Live

TE Test Equipment

VDES VHF Data Exchange Service

VDE-TER The terrestrial VHF Data Exchange access as described by [7], Annex 4

VDE-SAT The satellite VHF Data Exchange access as described by [7], Annex 5

2.2 Definitions

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

2.2.1 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.

2.2.2 Binding

A protocol binding defines how the MMS protocol messages are transported using a specific network protocol e.g. “MMS Protocol over VDE-SAT”. The binding defines a set of rules how MMS protocol messages are mapped to network protocol messages and back.

2.2.3 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, however different receiver parameters can make the actual range larger or smaller than expected, dependent on interference, the signal path and the receiver performance and antenna height.
Multiple transmitters can be used to broadcast the same message to achieve larger coverage. Broadcast may include repetition of the same message until the given TTL to reach receivers that were outside range, shadowed or switched off during earlier transmissions.

2.2.4 MRN addressed Message

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

2.2.5 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.

2.2.6 Anonymity

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

2.2.7 Maritime Identity Registry

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`.

2.2.8 Maritime Service Registry

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`.

2.2.9 MCP MRN

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

2.2.10 Navigation

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

2.2.11 Navigator

The person on board a ship responsible for its Navigation.

2.2.12 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.

2.2.13 Service Consumer

A software application, service, or some other type of software module that requires a (Technical) Service.

2.2.14 Service Provider

An entity providing a Service.

2.2.15 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.

2.2.16 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, it will be deleted from all queues, independend if it was delivered or not.

2.2.17 VDE-TER Network

A network consisting of one or multiple VDE shore base stations that are interconnected with a shore side MMS Edge Router to facilitate access to mobile VDES equipment through the VHF Data Exchange terrestrial access method described in [7].

2.2.18 VDE-SAT Network

A network consisting of one or multiple VDE satellites that are interconnected with a shore side MMS Edge Router to facilitate access to mobile VDES equipment through the VHF Data Exchange satellite access method described in [7].

3 General (Informative)

3.1 Motivation

There is a need for maritime digitalisation to happen. Digital solutions will enable increased operational efficiency and better productivity. A number of key digital services have been identified in the IMO e-Navigation Strategy Implementation Plan [8], incl. 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 digitalisation and automation.
Why is that so? The two main reasons are:

- Connectivity at sea is generally difficult and costly. In near-shore waters, vessels may of course 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. Generally, connectivity in the maritime environment is less stable than on land, therefore it is costly to establish.
- Safety at sea is a vital requirement. When a vessel leaves harbour, it will be in a state of potential emergency if anything goes wrong, this means that maritime digital services need to be deployed on strictly certified hardware and need to be trustable. It shall be easy to establish a good cyber security on board even though using modern e-Navigation services. Even though there are solutions to solve this, there are no established standards that enable smaller vessels to easily deploy the required safety level when connecting through existing solutions.

As a result, the maritime industry is much more conservative than land-based industries when it comes to the use of IT and communications, and highly manual procedures are used for services that could be digitalised.
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 used in 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 visualised 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.

3.2 The Maritime Connectivity Platform

The MCP is a decentralised platform that facilitates secure and reliable information exchange within the maritime domain and beyond. Beyond – because the maritime world isn't isolated, but need to exchange information with other domain – 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 decentralised platform, there is no single entity operating this. Several organisations 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 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 such, 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

3.3 The Maritime Messaging Service

The MMS is a 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.
The Appendix F lists the motivational use cases that lead to the following architecture and requirements for the MMS.

4 System Architecture (Informative)

The architecture of the Maritime Messaging Service (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.

4.1 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 the 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 a MMS Edge Router using MCP certificate from MSS Agents MCP MRN. All messages from MMS Agents must be authenticated (signed) with certificate from sending MCP MRN. 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 harbour or service provider.
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

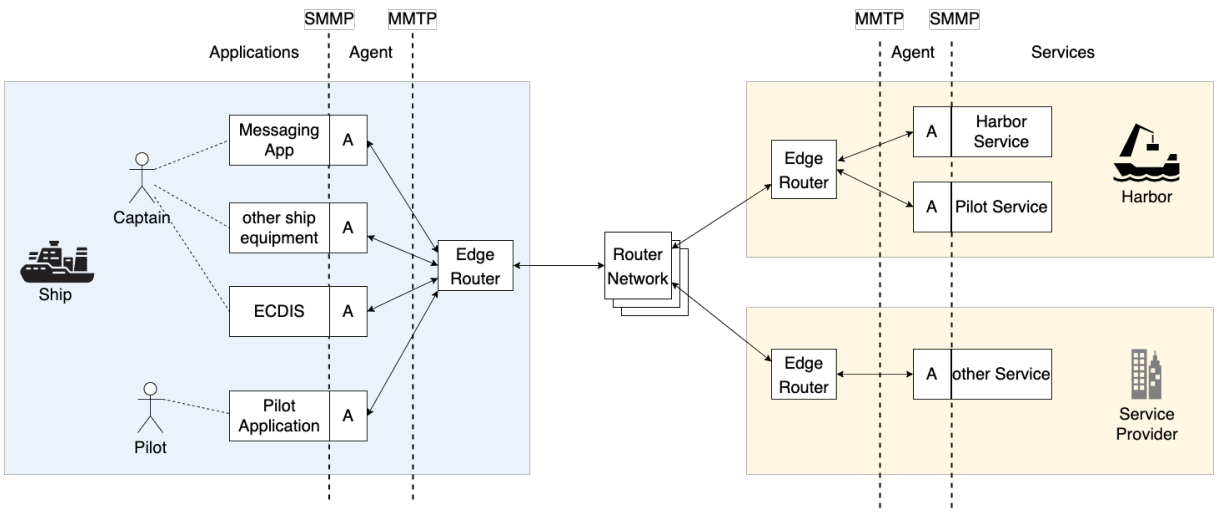

Figure 1 – Overview of MMS system architecture.

- MMS Router Network.

An MMS Router Network consists of zero 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.

4.2 MMS Message types

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

4.2.1 MRN Addressed Messages

MRN addressed messages are messages send from a specific MCP MRN to a specific MCP MRN. The receiver can be zero of more agents.

4.2.2 Subject-cast Messages

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

4.3 Protocols

The MMS defines the following two protocols.

4.3.1 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. Multicast messages are identified with a subject-string.
Note, that the MCP MRN used by an MMS Agent is provided by the associated Actor. This comes from the need for authentication using an MIR (being MIR-authenticated), which will require a MIR certificate associated with the MRN. For the example a ship crew sending a message to the Danish Maritime Authority (DMA), DMA might have several MRNs which it uses, depending on the specific message. Similarly, when a person today 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. 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:

- *..:Navelink:DMA:NW* for navigational warnings, or
- *..:Navelink:DMA:GreenposReporting* for GREENPOS reporting, and so on.

4.3.2 Secure Maritime Message Protocol (SMMP)

SMMP is an end-to-end protocol that provides security guarantees between System Actors.
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 for a given receiver; message cannot be altered and 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 to give proof of reception.
- Segmentation of larger messages.
- Streaming of data.

To use the SMMP, Actors must authorise into the MMS with an MCP-MIR certificate.
NB! Authenticity is also included in the MMTP protocol. It may be that there two authentications are overlapping. However, there is not requirement that the MMS Agent uses the sake MCP MIR certificate (and MCP MRN) as used for the SMMP.

4.4 Nodes

The MMS defines the following nodes.

4.4.1 MMS Agent

An MMS Agent is client software that interfaces with System Actors and provides connectivity to the MMS. MMS Agents connect to MMS Edge Routers via the Agent-Router Network interface using MMTP.
An MMS Agent is either MIR-authenticated, meaning that it

- has been assigned a MCP-MRN [9], in a MIR, and
- has been assigned a MIR 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 multicast 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.

4.4.2 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 either is MIR-authenticated, meaning that it

- has been assigned a MCP-MRN [9], in a MIR, and
- has been assigned a MIR certificate

An MMS Edge Router may connect to one or multiple MMS Routers. An MMS Edge Router may have a preferred MMS Router defined, it also is able to find an MMS Router through a connection dependent lookup. If an MMS Edge Router chooses to operate as MIR authenticated MMS Edge Router, it 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 MIR authenticated MMS Edge Router may expect the full functionality of the MMS Router Network.
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,
- subscription to Router Network provided subjects on behalf of the local Agents, and

- distribution of subject messages received from the Router Network to the local Agents.

Message broking thereby allows the distribution of a single received message to multiple subscribed MMS Agents, and by that avoiding that multiple MMS Actors' subscriptions to the same MRN or subject result in increased traffic over the link between MMS Actor and MMS Router. 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.

4.4.3 Router Network

The MMS Router Network consists of zero 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. [**NOTE**: MKT: We must be careful with the implementation of this.]
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.

4.5 Interfaces

For the MMS the following interfaces are defined.

4.5.1 Interface Agent - Edge Router

The Agent - Router Network Interface uses the Maritime Messaging Transfer Protocol (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 6.
The MMTP may give up on delivery attempts after a timeout, and therefore no delivery guarantee is given by the MMTP itself.

4.5.2 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,
- 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.

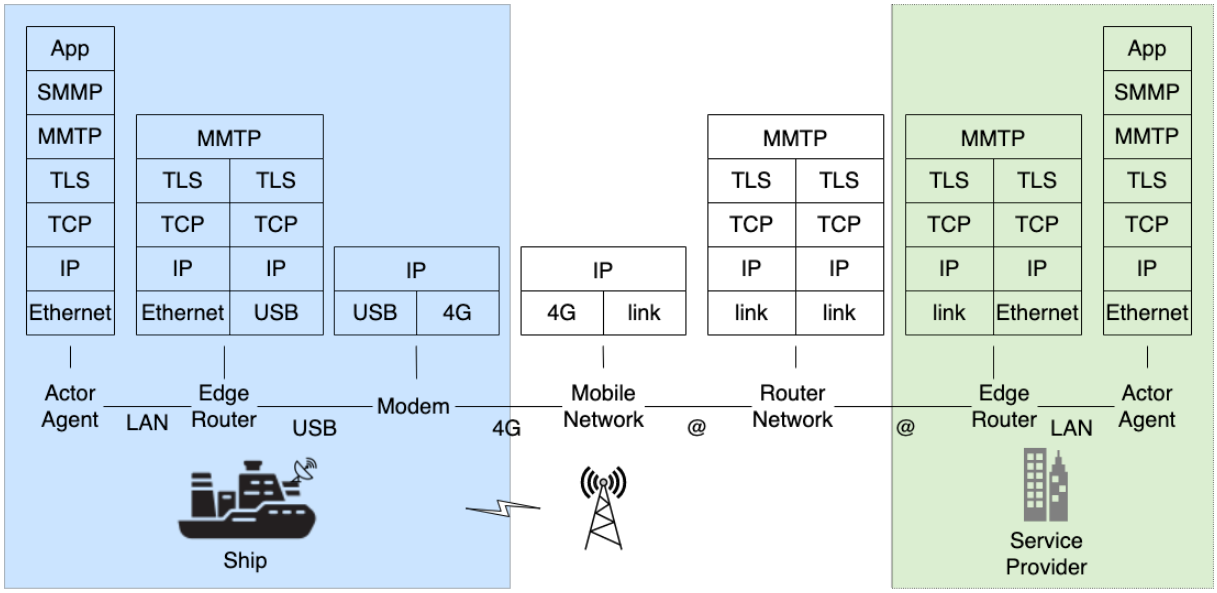

Figure 2 – Example of MMS protocol layering for messages over IP.

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

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

4.6 VHF Data Exchange System (VDES)

The VDES may be used as means to transport MMS traffic by connecting the ship side Edge Router with the Router Network over a VDES Network.
VDES provides AIS, ASM, VDE Terrestrial (VDE-TER) and VDE Satellite (VDE-SAT) services.
VDE-TER and VDE-SAT provide capabilities to route MMS traffic, as described in this specification.
Note: AIS and ASM data channels are reserved for small messages and thereby not of value for the MMS.
In order to allow MMS transport (see Figure 3) over VDES,

- the ship shall be equipped with a VDES enabled Edge Router,
- the ship shall be equipped with a VDES Modem according to ITU-R M.2092-1,
- the ship shall be in a MMS enabled VDES Network coverage area,
- the current available VDES Network shall provide MMS routing services into the MMS Router Network.

Also, Figure 3 shows how VDE bridges the VDES Network side Edge Router to the ship Edge Router, seen from the Router Network. For the MMS Router Network, the VDES Network Edge Router provides the same functionality, as the ship Edge Router with 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,

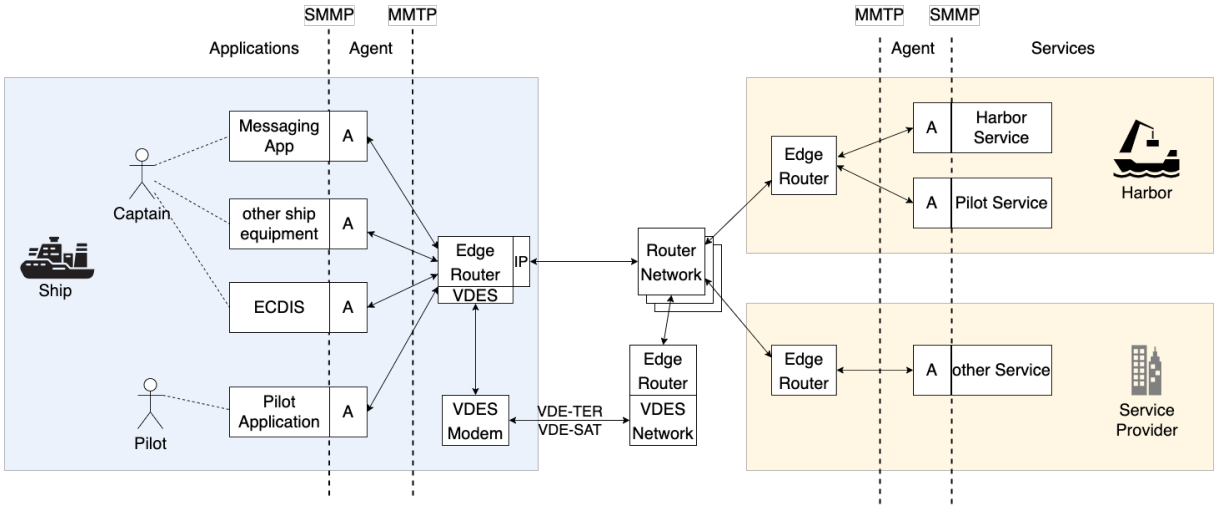

Figure 3 – Overview of MMS system architecture with VDES connection.

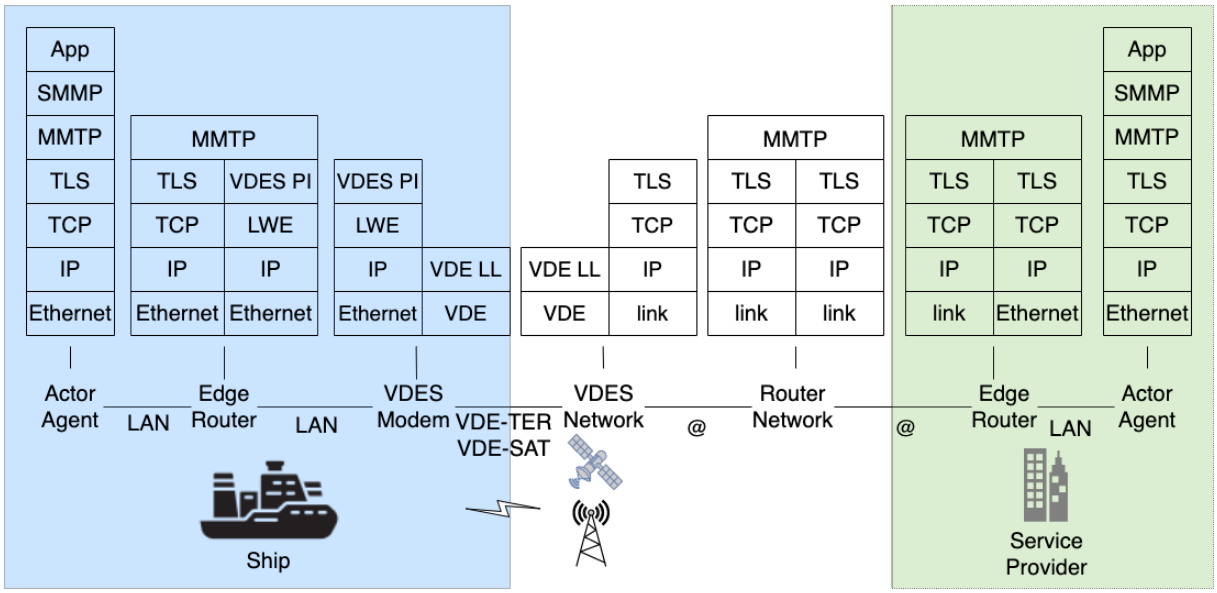

Figure 4 – Example of MMS protocol layering for messages over VDES.

- that terrestrial VDE (VDE-TER) provides coverage along coastlines where the distance between ship and coast station reduces the connection quality and speed,
- 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 Figure 4.

5 Functionality of System Components

This section describes the functionalities of the different system components that comprise the MMS. In Figure 5 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.

5.1 Functionality of MMS Agent

An MMS Agent enables an Actor to be connected to MMS by establishing a single connection with one MMS Edge Router on a LAN using the MMTP. Sending and receiving of messages and subscribing to subjects are the basic functionalities of an MMS Agent. [**NOTE**:stefan: might be removed and does not harm: An MMS Agent handles connection selection according to the situation by finding the best connection (question: is that not the MMS Edge Router's job? No, it's agent's job. MMS Edge Router has bindings with network. See fig:sys_arch-vdes.), and can authenticate itself.]
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 authenticated connected and has been 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 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 MRN addressed messages with the MMS Edge Router. This require 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.

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 6.
[**NOTE: We might need to describe: Connections and Timeouts**]
In the following, each function of the MMS Agent is describe in more detail.

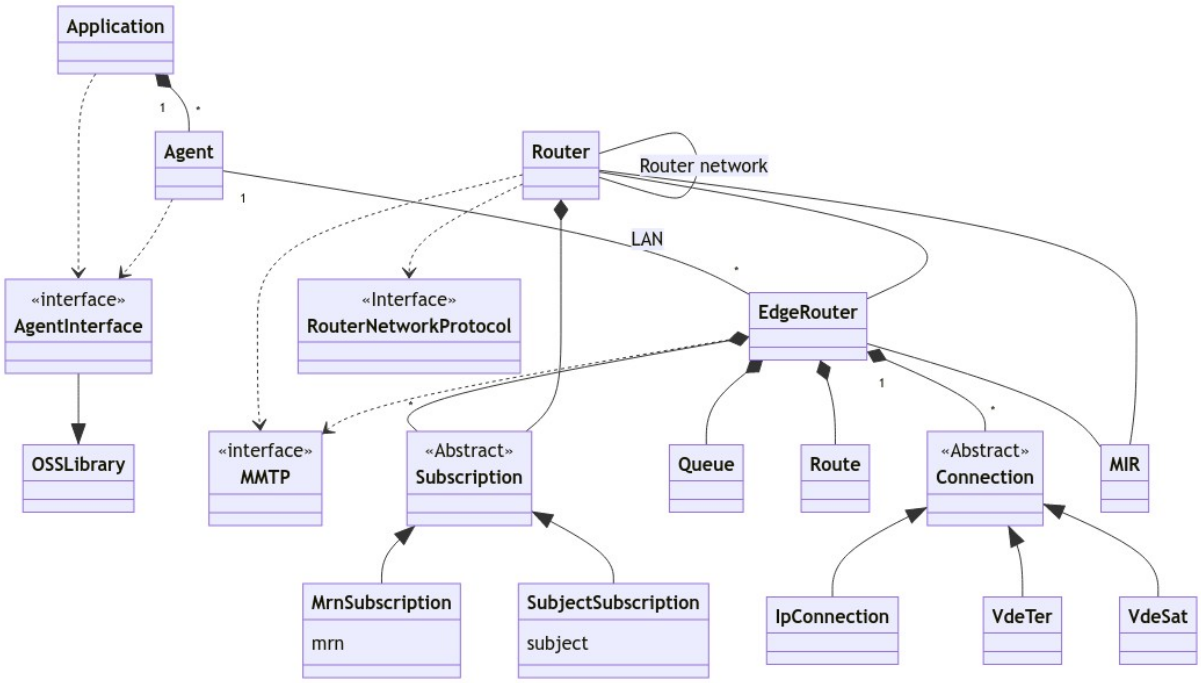

Figure 5 – UML diagram showing the components of the MMS.

5.1.1 Discover Edge Routers

The Discover function shall find MMS Edge Routers on the configured LAN using the mDNS [10] and DNS-SD [11] protocols.
The function shall not accept any arguments.
The function shall return a list with the MRNs of all MMS Edge Routers that are found on the configured LAN.
Note: This will be based on how devices like Chromecast and similar announce their presence on a network using mDNS and DNS-SD.
Note: we need to standardise names for the MMS Edge routers for discovery. The procedure for how to do this is described in [?] and the actual registration is done through the form here.

5.1.2 ConnectAnonymously `Edge Router`

This function shall establish an anonymous connection to a specific MMS Edge Router using secure transport [**NOTE**:TLS V1.3][12] 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 priory (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.

5.1.3 ReconnectAnonymously `Edge Router Token`

This function shall re-establish an anonymous connection to a specific MMS Edge Router using secure transport [**NOTE**:TLS V1.3][12] and shall keep it alive until disconnected or lost.

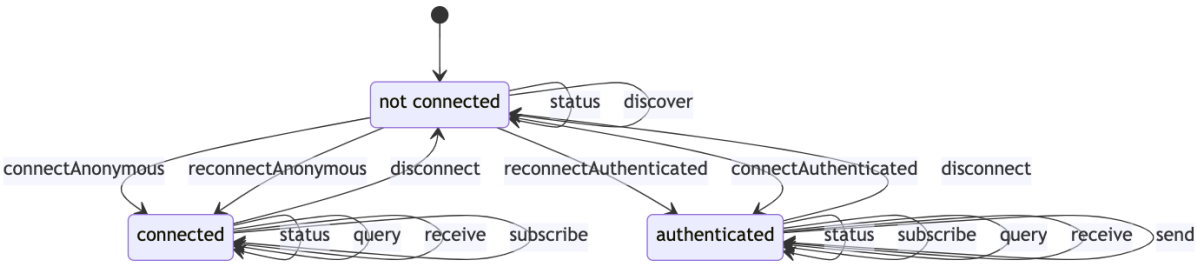

Figure 6 – UML diagram showing the functionality of the MMS Agent.

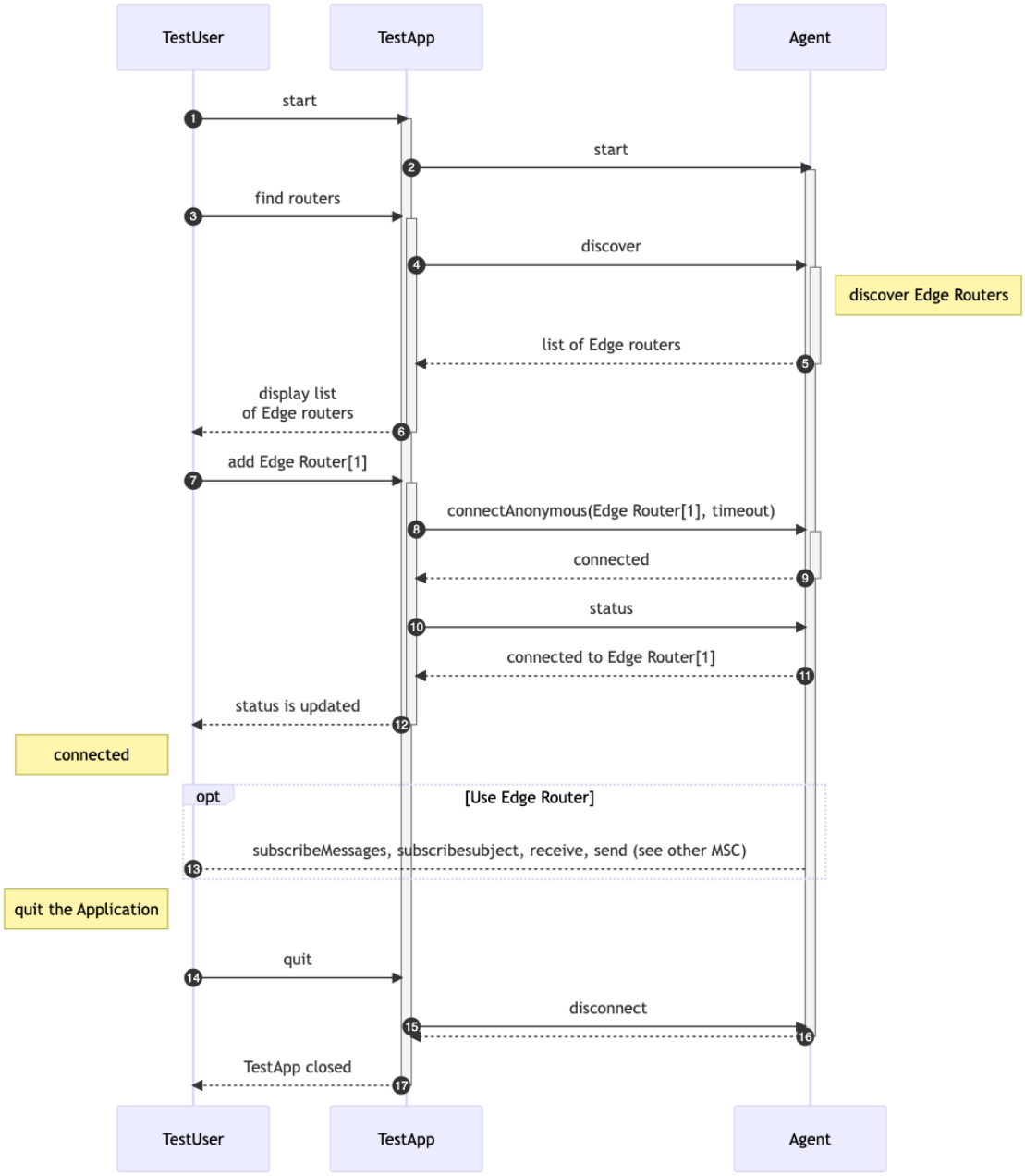

Figure 7 – UML MSC Diagram: MMS Agent connects anonymousely to an MMS Edge Router from User/App point of view.

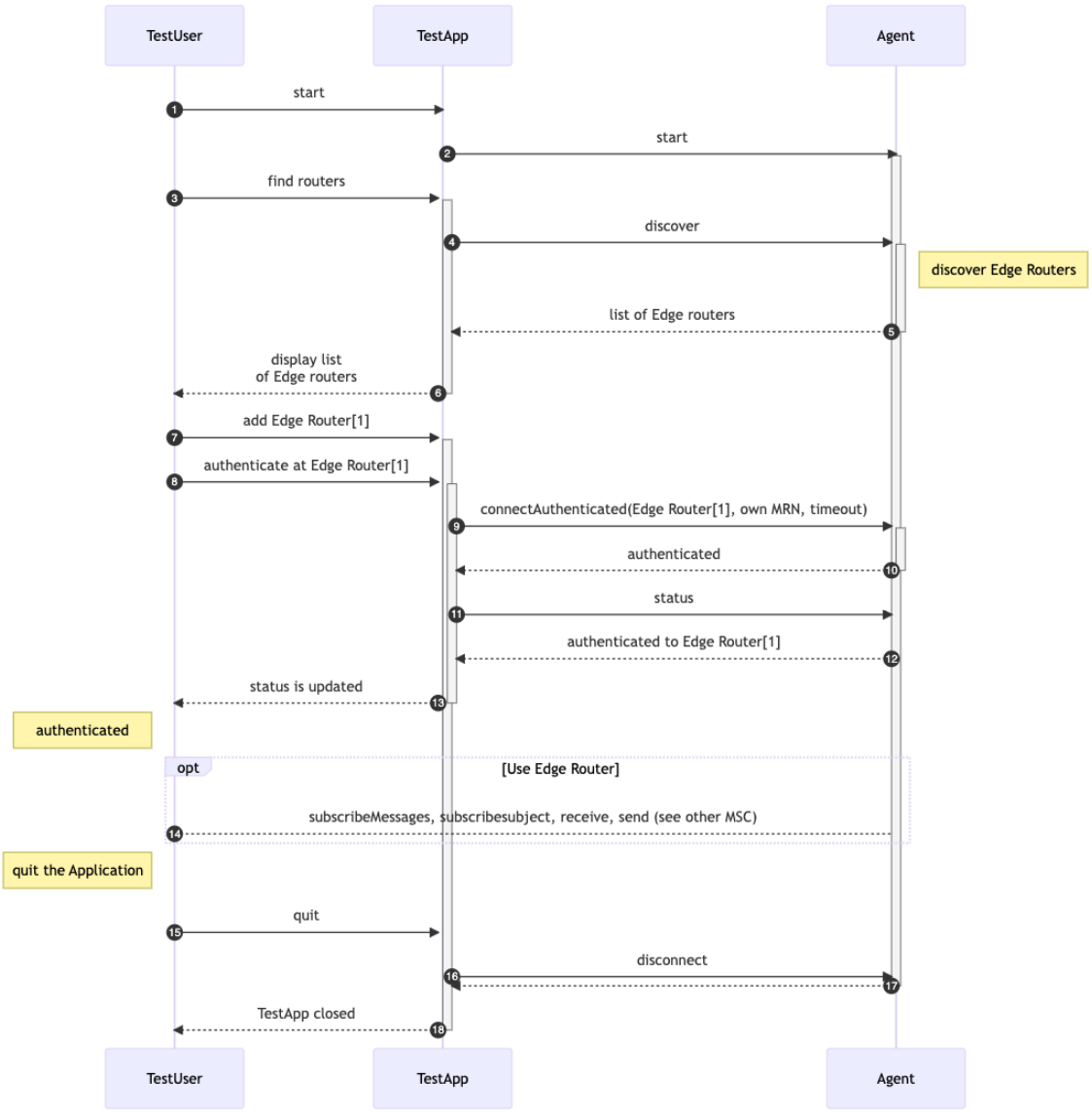

Figure 8 – UML MSC Diagram: MMS Agent connects and authenticates to an MMS Edge Router from User/App point of view.

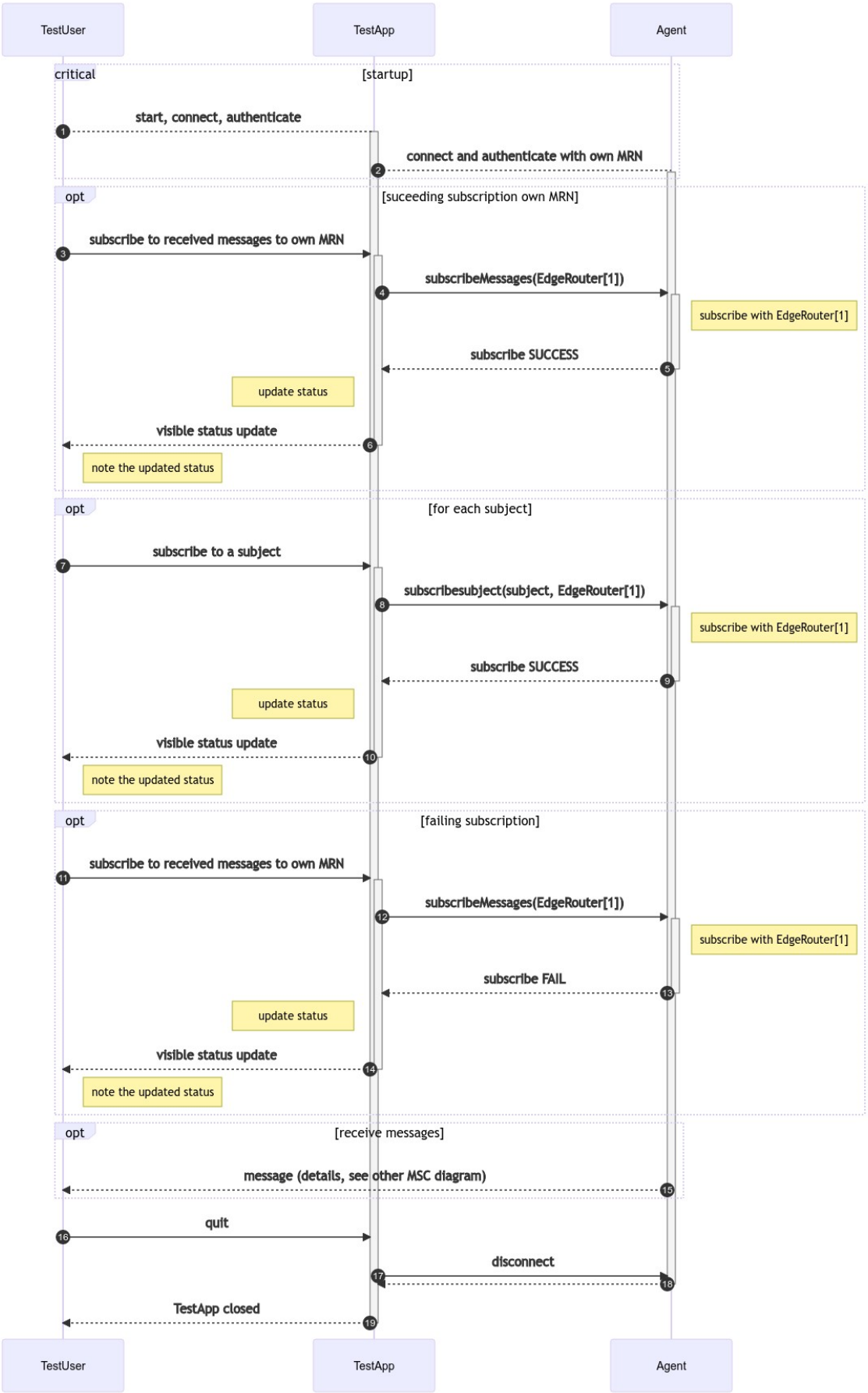

Figure 9 – UML MSC Diagram: authenticated MMS Agent subscribes to messages from User/App point of view.

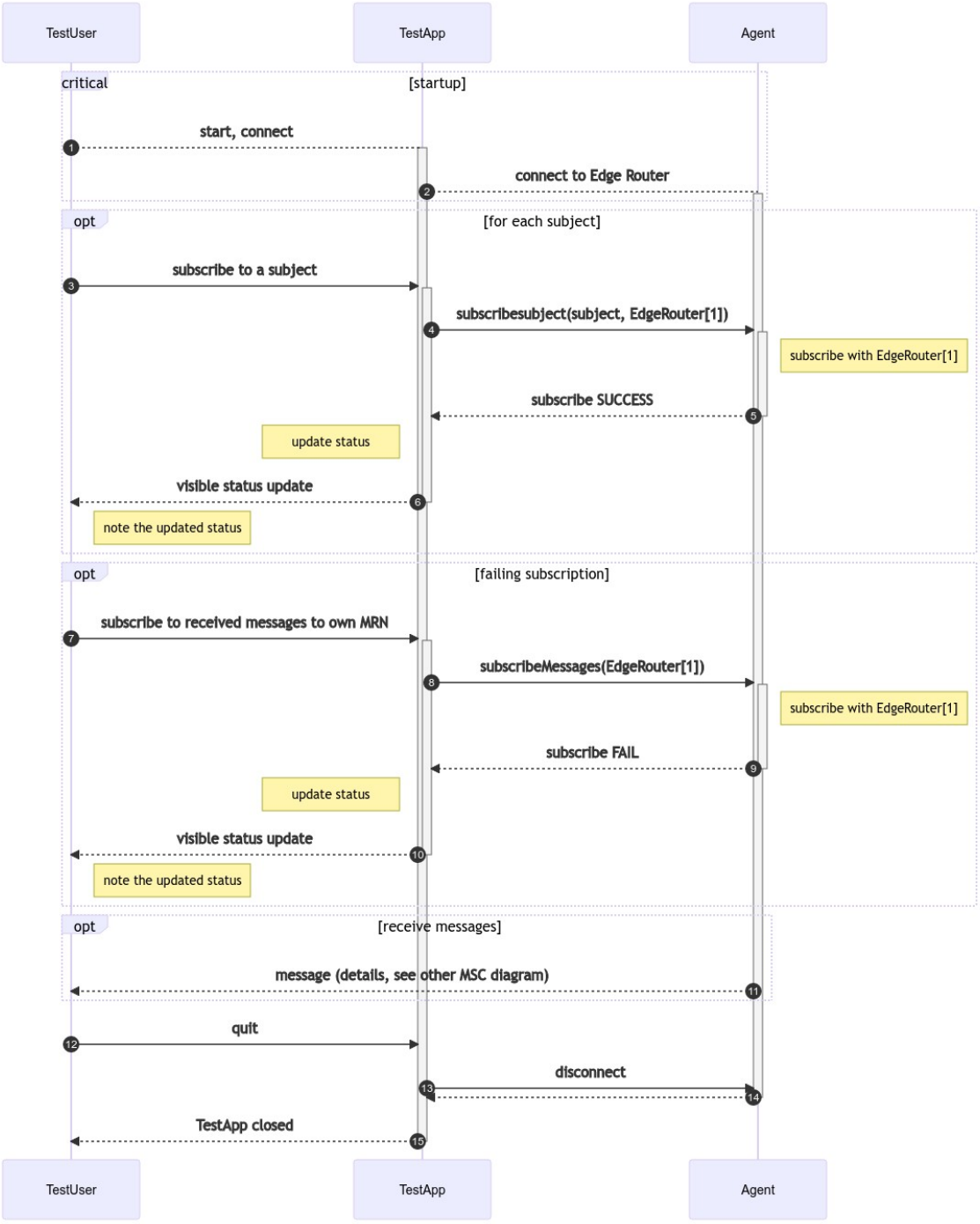

Figure 10 – UML MSC Diagram: non-authenticated MMS Agent subscribes to messages from User/App point of view.

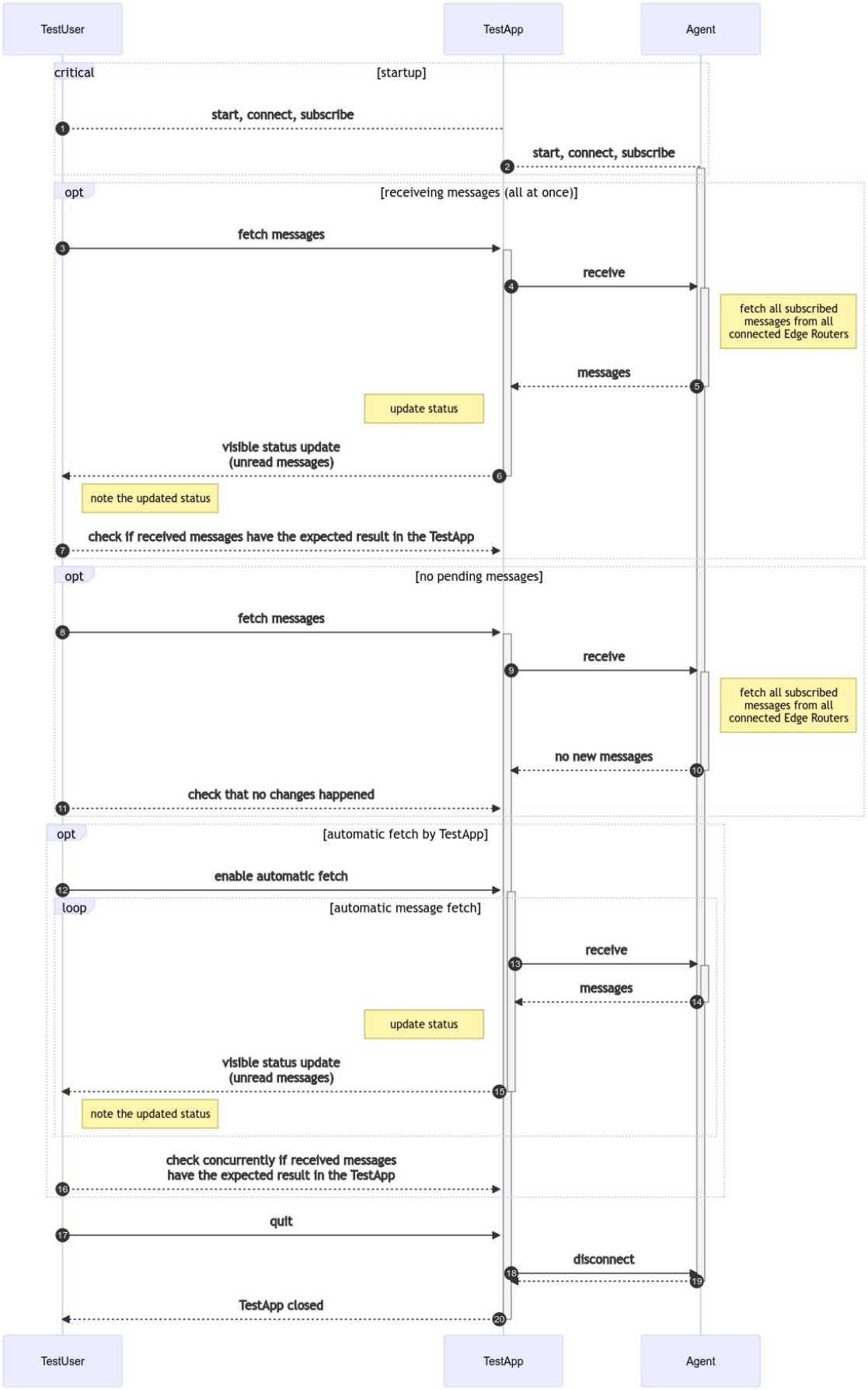

Figure 11 – UML MSC Diagram: MMS Agent receives messages.

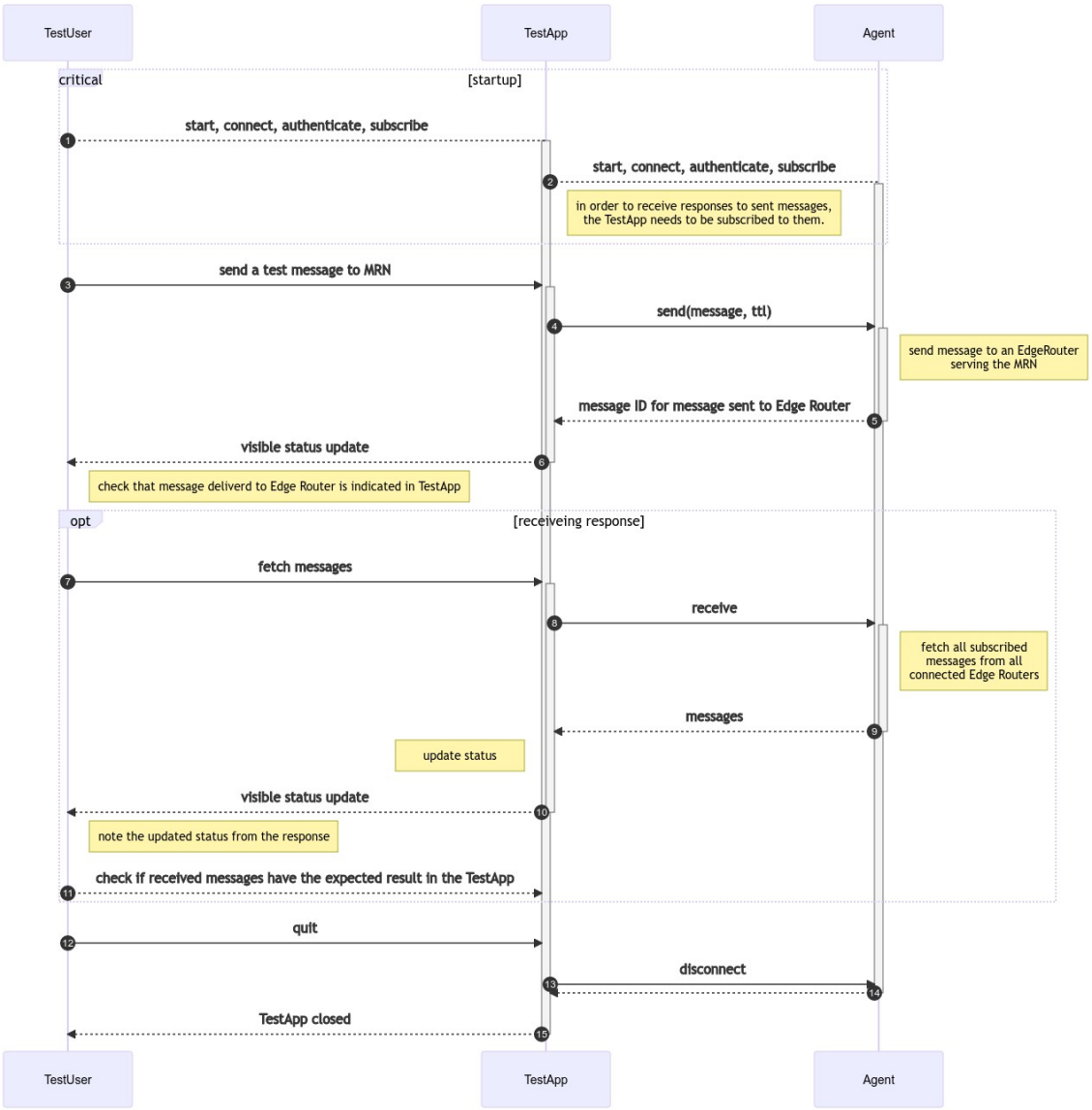

Figure 12 – UML MSC Diagram: authenticated Application is sends messages and receives response.

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 priory 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.

5.1.4 **ConnectAuthenticated** `Edge Router`

This function shall establish an authenticated connection to a specific MMS Edge Router using secure transport [**NOTE**:TLS V1.3] [12] 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 priory 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. If successful, the MMS Agent shall store the MRN based MCC Certificated of the Application to be used for later calls to the SubscribeMessages function. The MMS Agent shall store the reconnection token and its associated authentication status (anonymous or authenticated) for later reconnect.

5.1.5 **ReconnectAuthenticated** `Token`

The function shall re-establish an authenticated connection to a specific MMS Edge Router [**NOTE**:using TLS] 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 or 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 priory 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.

5.1.6 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 states of the MMS Agent.

5.1.7 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 (**Note: Format to be decided**)

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.
[**NOTE: This format shall be defined another place!!**]

5.1.8 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 expect 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`.

Note: if we think that we want to support authenticated reception of broadcasts (like pay-TV that requires a subscription, but uses broadcast resources to distribute), we might consider that subscription to some subjects requires authentication
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.

5.1.9 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.

5.1.10 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.

5.1.11 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.

5.1.12 Send

This function shall deliver a 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,
- 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.

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.

5.1.13 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.

5.1.14 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.

5.1.15 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 to 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.

5.1.16 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.

5.2 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. [**NOTE**: by use of the mTLS protocol.] 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.

A 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.
A 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 sate 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 Agent in one of the above states is described below. All functions shall be non-blocking.

Startup Perform tests and checks, and initialize all interfaces.

Connect `ROUTER`**.** Connects to another MMS Router in the Router Network.

Send `MRN`**.** Send messages.

Fetch. Get list of available messages at a MMS Router

Receive `filter`**.** Receive messages.

Subscribe `MRN`**.** Subscribe to receive messages for a certain MRN.

Subscribe `subject`**.** Asks a MMS Router to deliver messages to the MMS Edge Router with a specific subject.

Shutdown. Shuts down the MMS Edge Router.

5.2.1 General Functionality Concepts

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:
    1. administrative users, and
    2. 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 spacial differentiable positioned LEDs with clearly readable labels or a default installation display terminal,
8. provide interfaces through witch 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 behaviour, 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.

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.

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.

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:
    1. duplicated messages identified by UUID of the message,
    2. subject of subscription, and
    3. messages with a limited time until TTL.

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.

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

5.2.2 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.

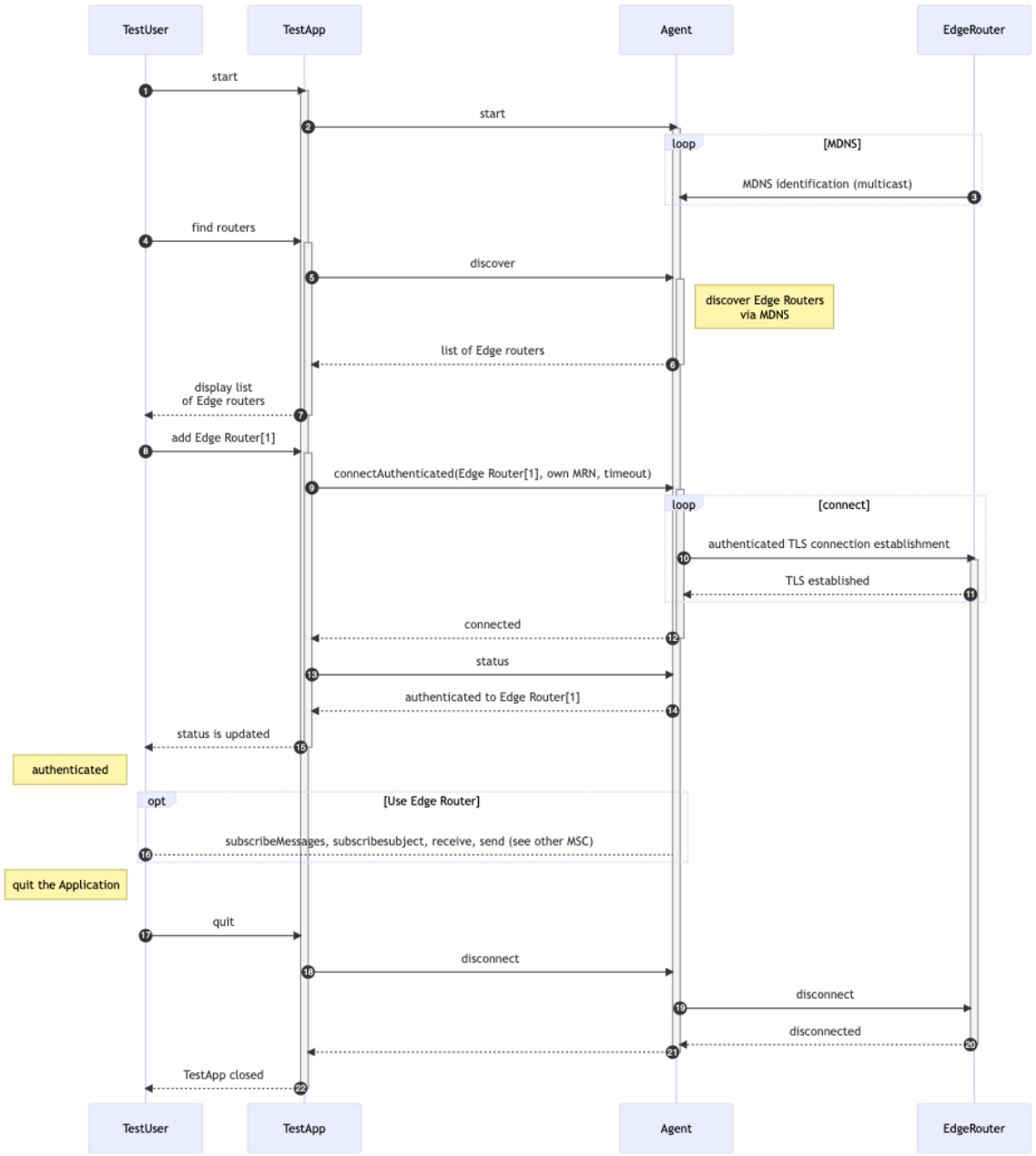

Figure 13 – UML MSC Diagram: MMS Agent connects and authenticates to MMS Edge Router from User/App point of view.

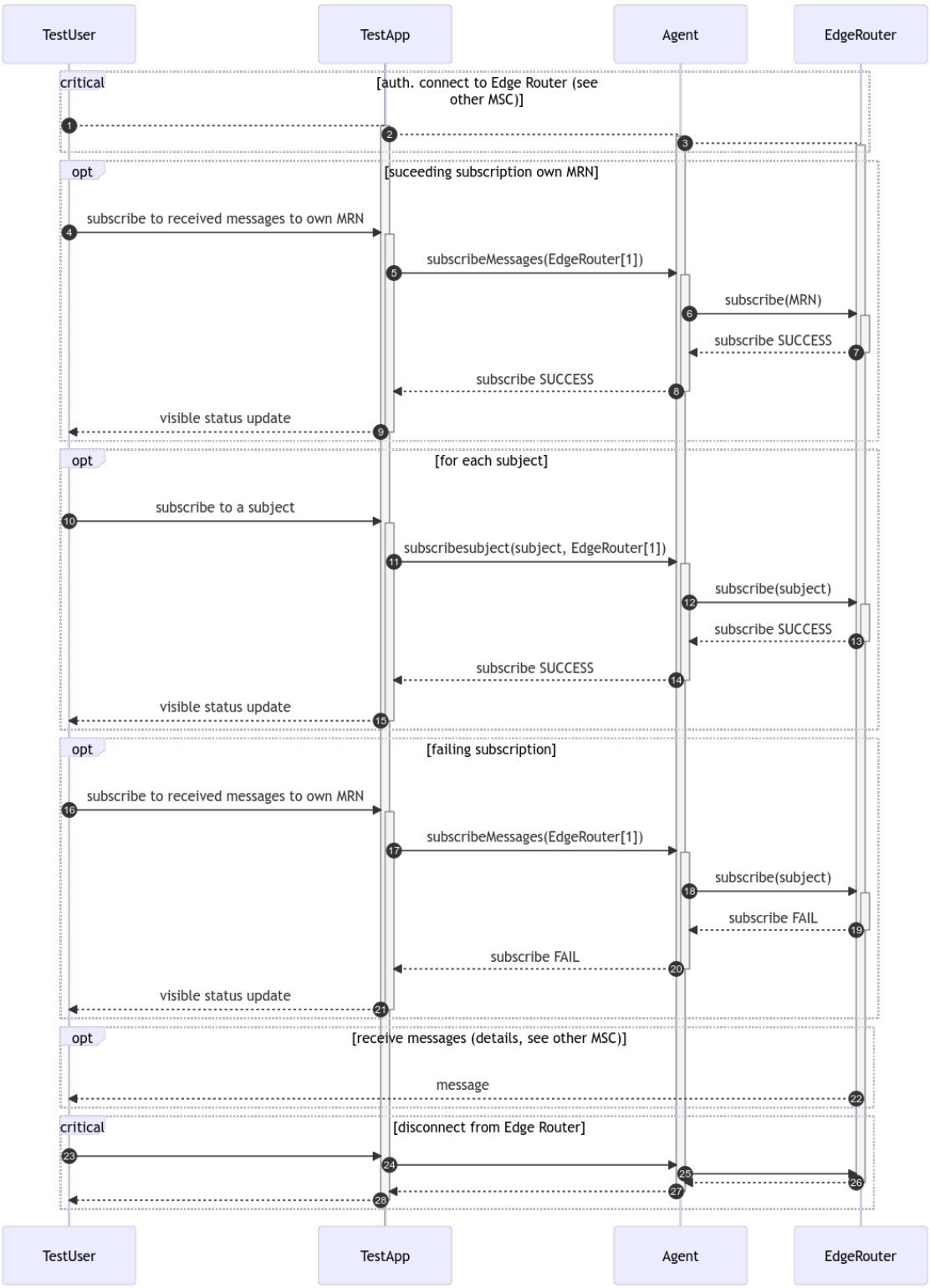

Figure 14 – UML MSC Diagram: authenticated MMS Agent subscribes to messages at an MMS Edge Router.

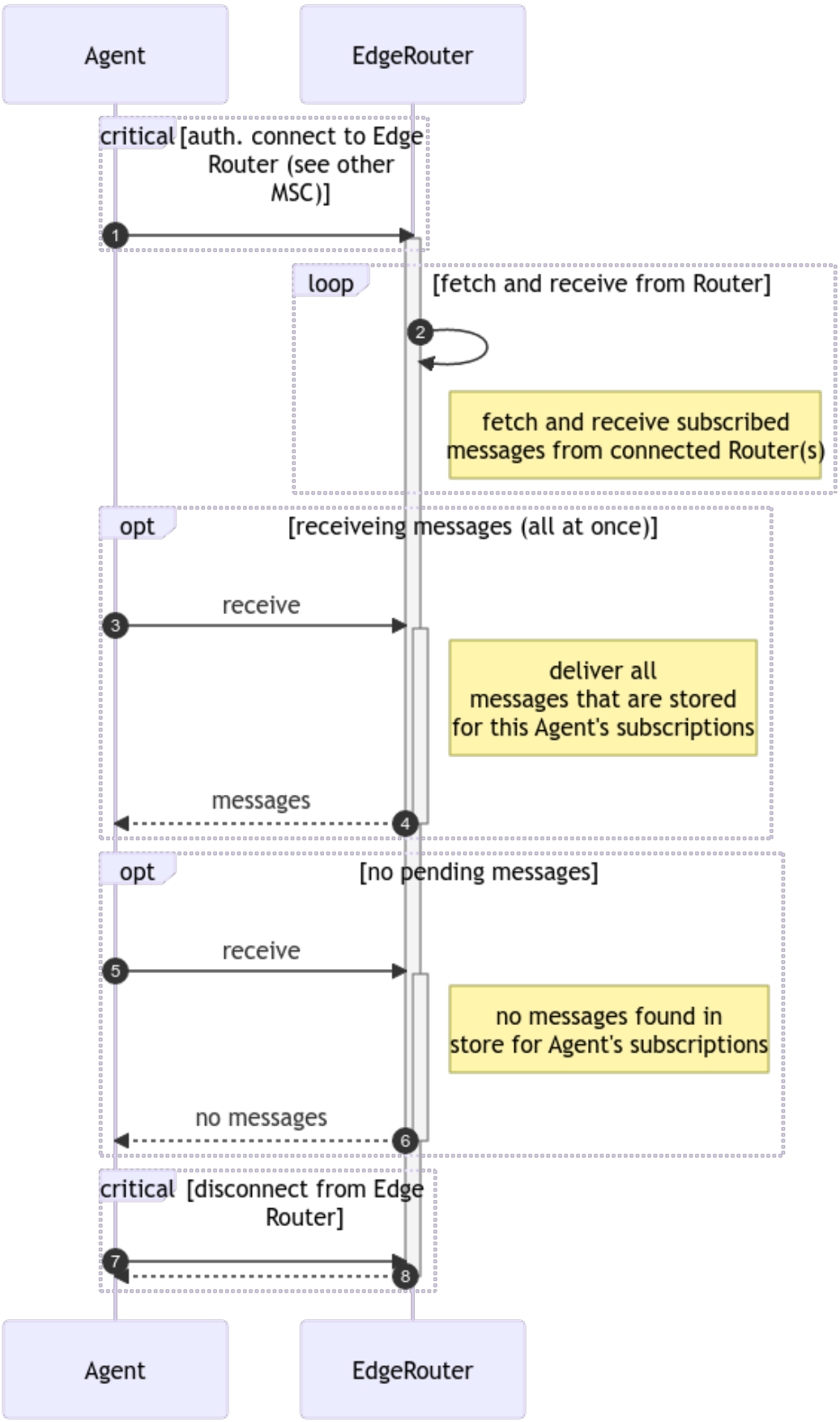

Figure 15 – UML MSC Diagram: MMS Agent receives messages from an MMS Edge Router.

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:
    1. normal operation as configured,
    2. reduced operation limiting some configured functionality, or
    3. 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
    1. identify inconsistent states and behaviour of functions, and
    2. log and indicate such inconsistencies for momentary and later analysis by users and operators, and
    3. 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.

Built In Self Test This internal function is part of the Startup procedure and shall perform a self test.
I 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.
[**NOTE:** check IEC61993 AIS about the requirements there, and apply what makes sense]

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.
[**NOTE:** check IEC61993 AIS about the requirements there, and apply what makes sense]

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 side MMS Edge Router MMSI.

[**NOTE** consider to move the details to binding] #### Connect `ROUTER`
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.

Disconnect `ROUTER` This internal MMS Edge Router function shall disconnect from a MMS Router. The MMS Edge Router shall:

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

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. maintenance of a connection to the connected MMS Agent until the MMS Agent disconnects.

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.

Send [`MRN` | `subject`**]** 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 MRN, and
    - connected local MMS Agents that have subscribed to that message subject or MRN.

5.2.3 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.

5.2.4 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.

Fetch (from MMS Agent) This function is requested by an MMS Agent fetching the list of unreceived messages 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.

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.

Fetch (to MMS Router) This internal MMS Edge Router function is invoked by the MMS Edge Router to fetch the list of stored messages for the requesting MMS Edge 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.

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.

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.

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.

Subscribe `subject` 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 connected MMS Routers, and
4. store the subscription status for that subject and requesting MMS Agent according to the above decision.

Unsubscribe `subject` 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.

Query 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.

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:
    1. stored messages,
    2. stored subscription states, and
    3. stored connection states,
5. close the connection to the requesting MMS Agent.

Shutdown 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.

5.3 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, a MMS Router maintains connections between MMS Routers and with MMS Edge Routers.
A 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 Figure 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, a 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.

5.3.1 Interface to MMS Edge Routers

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

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.

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:
    1. transfer all subscriptions to the new transfer MMS Router,
    2. transfer all messages that were stored for the requesting MMS Edge Router to the new transfer MMS Router,
    3. taking into account local configuration,

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.

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.

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.

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.

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.

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.

5.3.2 Routing Network Interface

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.

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.

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.

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.

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.

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.

Housekeeping A MMS Router shall regularly:

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

5.4 Functionality of MMS Router Network

A 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 The MMS Transfer Protocol

6.1 Overview (informational)

The Maritime Messaging Transfer Protocol (MMTP) is the transfer protocol between MMS Agents via 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.

6.2 Requirements

The MMTP shall provide a transport for sending and receiving protocol messages between MMS Agents and MMS Edge 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 Section 8.

6.3 Definitions

All messages listed here are defined in protobuf format [13] prefixed with

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

The complete protobuf definition of MMTP can be found in Appendix J.

6.3.1 MMTP messages

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

6.3.2 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;
}
```

6.3.3 MMTP Request Messages 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;
}
```

6.3.4 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,
5. zero or multiple application messages, and
6. zero or one reconnect token, containing an UUID according to [14].

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 ApplicationMessage applicationMessages = 5;
  optional string reconnectToken = 6;
}
```

using

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

and

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

6.3.5 MRN

All MRN references in this protocol definition shall comply with MCP MRN [9], which is a subdomain of MRN [15].

6.3.6 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
    1. a *subject* or *recipients* being
        1. the value of the *subject* property, if present, shall be a string no longer than 100 characters.
        2. the value of the *recipients* property, if present shall be a list with one or more MRNs.
    2. an *expires* property, value is milliseconds after the 1st of January, 1970; shall be the timestamp when the message content is expected to be no longer relevant in milliseconds 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.
    3. a *sender* property, value shall be the MRN of the Agent that constructed the message.
    4. a quality-of-service profile as defined in Appendix.
2. a *body* containing the binary data of the message in the protobuf bytes format.
3. a *signature* containing a string 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:
    1. allocate an empty list of bytes *B*,
    2. 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*,
    3. encode the decimal string representation of the value of *expires* as bytes and append the result to *B*,
    4. encode the value of *sender* as bytes and append the result to *B*,
    5. if *qosProfile* is set, encode the value of *qosProfile* as bytes and append the result to *B*,
    6. encode the decimal string representation of the value of *bodySizeNumBytes* as bytes and append the result to *B*,
    7. append the value of *body* to *B*,
    8. give *B* and private key as inputs to the signing algorithm defined by [16] Section 6.4.1 and store the output values *r* and *s*,
    9. DER encode *r* and *s* using the ASN.1 structure defined by [17] Section 2.2.3,
    10. Base64 encode the result from Step 9 and return the result.

The following protobuf code does implement the required normative structure:

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

6.3.7 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.

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* boolean, value shall identify a subscription to own MRN.

[note: it is assumed that the MRN is also referring to the format of the body, e.g. a subject could be "DK_NAV_WARNINGS_S124_XML"].
The following protobuf code does implement the required normative structure:

```
message Subscribe {
  oneof subjectOrDirectMessages {
    string subject = 1;
    bool directMessages = 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* boolean, 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;
  }
}
```

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:

- a Application message.

[note: it is assumed that the MRN is also referring to the format of the body, e.g. a subject could be "DK_NAV_WARNINGS_S124_XML"].
The following protobuf code does implement the required normative structure:

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

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 an application message.
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 messageUuids = 1;
}
```

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 {
}
```

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 {
}
```

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 [14], 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.

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;
}
```

7 The MMS Router Network Protocol

7.1 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 [18] 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.

7.2 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 direct messages,
- ensure that any message published in the Router Network are routed to all subscribers.

7.3 Definitions

7.3.1 Connection Between MMS Routers

For the connection between MMS Routers the protocol for connection establishment in libp2p [19] shall be used.
While the above mentioned protocol does support a variety of underlying transport mechanisms, an MMS Router shall at least support TCP and QUIC as the underlying transport mechanisms.
Connections between MMS Routers shall be secured with TLS 1.3 [12] using the libp2p specification that is defined by [20].

7.3.2 Establishment of MMS Router Network

In order for MMS Routers to discover each other and form a network, the libp2p Kademlia DHT [21] shall be used.

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 Section 7.3.1.
After successfully establishing a connection, the Router shall initialize a local DHT in *server mode* and perform the *bootstrap process* as described in [21].

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.

7.3.3 Handling of Subscriptions

For handling of subscriptions in the MMS Router Network, the libp2p PubSub interface [22] shall be used. This interface defines operations for both subscribing and publishing to *topics*.

Subscribing to Subjects and MRN Addressed Messages When an MMS Router receives an MMTP Message with a *Subscribe* message inside, the Router shall construct a *SubOpts* 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 [23]. This protocol is an implementation of the libp2p PubSub interface [22] providing gossip based advertisement of subscriptions and routing of messages in a network of libp2p nodes.

7.3.4 Routing of Messages

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 a MRN addressed message. If the message is a subject-cast message, the Router shall construct a libp2p PubSub *Message* [22] 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* [22] 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 [23].

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.

8 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.

8.1 WebSocket binding

8.1.1 WebSocket Endpoints

An MMS Edge Router or Router has an HTTPS endpoint where it can accept WebSocket [24] connections.

8.1.2 Connection Management

Agents shall use secure WebSocket transport [24] 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 [12].
MMS Edge Routers that connect to MMS Routers shall use mutual authenticated TLS WebSocket binding, as defined in TLS [12].
WebSocket connections are kept alive by the WebSocket integrated ping/pong mechanism [24].

8.1.3 Discovery of Endpoints

Discovery of the MMS Edge Routers endpoints is described in Section 5.
MMS Routers are discoverable in a Service Registry as defined in [25] Section 9, e.g. the MCP Service Registry.

8.1.4 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 [26] containing the status as described in Section 5.1.6.

8.1.5 Timeouts

Timeouts for WebSocket shall be implemented as defined by the WebSocket standard [24].

9 System Tests (informative)

A MMS System shall support following test scenarios to be compliant with this specification.

9.1 General

All system tests require a minimum test system setup consisting of:

- 1 SP test instance, namely referred to as SP1
  - with 1 dedicated Agent,
  - registered in an MSR
- 2 SC test instances, namely SC1 and SC2
  - with 1 dedicated Agent each,
  - each registered in a MIR
- 2 Edge Routers:
  - ER1 for the SC side
  - ER2 for the SP side
- 1 Router instance between the SP and the SC
- access to a test MIR instance, namely MIR1, as defined in [27]
- access to a test MSR instance, namely MSR1, as defined in [28]

Figure 16 shows an overview of the test setup.
In order to avoid the test to be impacted by load of other traffic, the system under test shall only consist of the above listed test components for conformance testing.
As these system tests also apply to live systems, they may be run in live systems to create performance KPI's as a proof of function. All timing measurements in real systems, however, need to appropriately take the current system load into account by other SCs and SPs that use the system.

9.1.1 Values and Parameters Common to System Tests

t_p = 120 seconds: maximum MMS total processing delay in the longest routing chain. Consisting of following specific maximum delays for the single compoents:

1. maximum Agent processing delay t_p_A = 40 seconds;
2. maximum Edge router processing delay t_p_ER = 40 seconds;
3. maximum Router processing delay t_p_R = 40 seconds;

t_f = forwarding delay calculated for each case: The forwarding delay is given by the physics of the underlying transport below MMS, taking into account:

1. the speed of electromagnetic waves in the given media over the total signal travel distance, and
2. the protocol relayed access and operation delays imposed by the means of transport.

The test contains the test MRNs that are referenced in the test descriptions by the following names:

- MRN(A1) = the MRN of the first Test Agent,
- MRN(A2) = the MRN of the second Test Agent,
- MRN(A3) = the MRN of the third Test Agent,
- MRN(ER1) = the MRN of the first MMS Edge Router,
- MRN(ER2) = the MRN of the second MMS Edge Router, and
- MRN(R) = the MRN of the MMS Router.

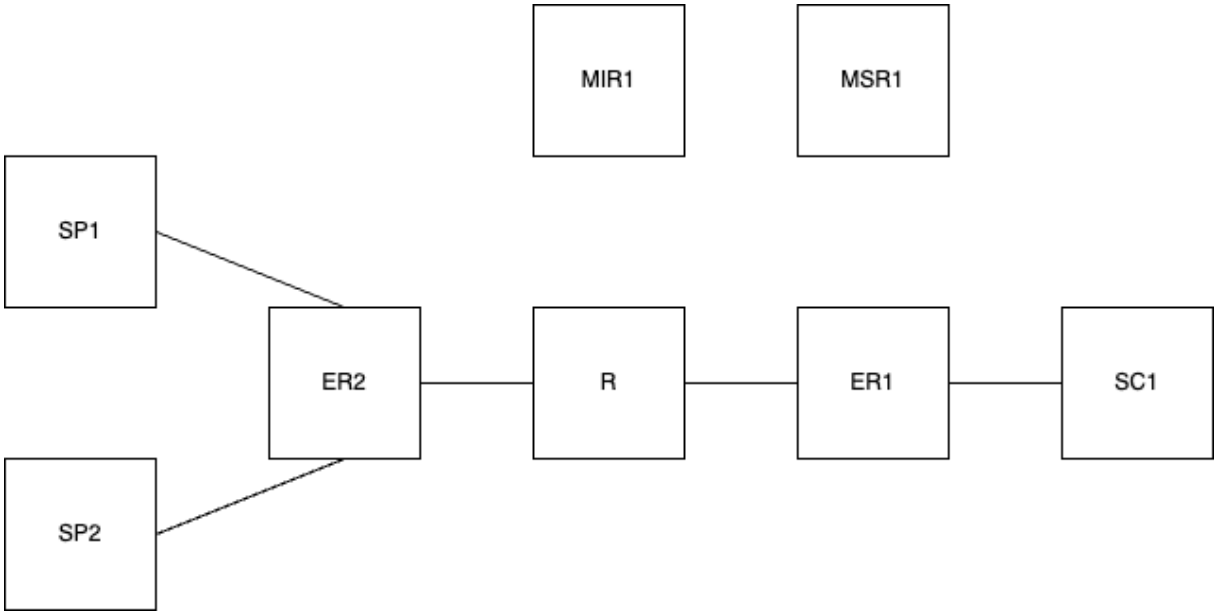

Figure 16 – UML diagram showing the test architecture.

9.2 Test: MRN Addressed Message SP -> SC

The purpose of the test is to test a real transfer from an SP to a SC happens within given limits with one MMS component as EUT and the others as TE.

9.2.1 Method of Test

A MRN addressed, unencrypted message with

1. source MRN(SP1),
2. destination MRN(SC1), and
3. payload being a known sequence S[] of size 100kB

is sent at a given time t_0.

9.2.2 Required Result

1. The MRN addressed message arrives at the SC after not later than t_a = t_0 + t_f + t_p
2. The source MRN in the received message is MRN(SP1)
3. Optionally, if SP has direct access to MSR: the SP may verify the existence of MRN(SP1) in the MSR
4. The destination MRN in the received message is MRN(SC1)
5. The payload is exactly the same sequence S[] of size [1 kB, 10 kB, 100kB] as sent,
6. the indicated priority is “normal”.

9.3 Test: Subject Addressed Message

9.4 Test: Local (no router) Subject Addressed Message

9.5 Test: Local (no router) MRN Addressed Message

10 Profiles

11 Implementation of use cases in MMS

This chapter will detail how the use cases can be implemented using the MMS protocol.

11.0.1 MUC 2.6 realization

Solution example draft: implement scaling in such way that a service splits its subjects into most important (short), important (middle sized), detailled (long), ideally not overlapping but complementing each other. The user equipment would subscribe to all three of them, however, with weak connectivity, only most important would be transported, with better connectivity, also the middle sized and with broadband all three.

Annex A

System Level Test Cases

Annex B

MMS Ship Agent for IP connections

Annex C

MMS Binding for VDE-TER networks

VDES contains a terrestrial component for ship to ship, ship to shore, shore to ship transfers of messages called VDE-TER, see [7], General section and Annex 4 for details.
This Appendix describes the bindings and functionality that shall be implemented by MMS equipment providing transport of MMS messages over a VDE-TER network.

C.1 Entities overview

This chapter introduces the entities that shall provide additional functionality to support MMS messages over VDE-TER.

C.1.1 VDE-TER Shore Base Station

VDE-TER Shore Base Stations provide the VDE-TER radio access on the non-mobile shore side.
Note: VDE-TER Shore Base Stations are used in harbours and on the shore line to provide terrestrial coverage such that VDE-TER mobile equipment can use the services provided by the VDE-TER Shore Base Stations.
VDE-TER Shore Base Stations coordinate the VDE-TER ressources for all connectivity between mobile VDE-TER equipment and themselfes in the radio coverage area of the base station according to [7].
MMS complient 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 [29], Annex B.3.1 to a VDE-TER enabled MMS Shore Edge Router for MMS processing.
MMS complient VDE-TER Shore Base Stations shall allow a VDE-TER enabled MMS Shore Edge Router 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.

C.1.2 VDE-TER Shore Network

A VDE-TER Shore Network consists of:

- one or multiple VDE-TER base stations,
- connections between these VDE-TER base stations, and
- one or multiple VDE-TER enabled MMS Shore Edge Routers to connect the VDE-TER Shore Network with the MMS

Router Network.

C.1.3 VDE-TER enabled MMS Shore Edge Router

A VDE-TER enabled MMS Shore Edge Router provides a link between the MMS Router Network and one or multiple VDE-TER Shore Base Stations.
A VDE-TER enabled MMS Shore Edge Router shall conform to Section 5.2 and additionally perform at least follwing 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 about available services and MMSI mappings applicable,
2. maintain routing and MMSI mapping to reach subscribed own MRN's via VDE-TER as long as these are reachable 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 [29], Annex B.3.1,
6. prioritiy 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 a VDE-TER enabled MMS Shore Edge Router may provide and announce to be available through VDE-TER broadcasts are:

- MIR query service to retreive 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 retreive service certificates for services transported over that VDE-TER Shore Network

C.1.4 VDE-TER Mobile Equipment

VDE-TER mobile equipment facilitates communication to other mobile equipment and shore base stations through VDE-TER as defined in [7].
Through such a VDE-TER communication, the MMS Edge Router is able to transport MMS messages to and from other MMS Edge Routers that are connected to a VDE-TER mobile or shore base station equipment.
Note: MMS message exchange over VDE-TER is enabled to use:

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

VDE-TER mobile equipment shall confirm with [7] General section and Annex 4, and shall be type approved by [30].
VDE-TER mobile equipment shall provide a Presentation Interface to the MMS Mobile Edge Router as defined in [30].
Note: the VDE-TER presentation interface is based on VDE-TER specific sentences as defined in [30], transported over lightweight ethernet [31] standard providing NMEA/UDP/IP.

C.1.5 VDE-TER enabled MMS Mobile Edge Router

A VDE-TER enabled MMS Mobile Edge Router is a MMS Edge Router providing the MMTP interface to MMS Agents as described in Section 5.2, that is capable to use VDE-TER for transport of MMS messages to other VDE-TER equipment that is connected to VDE-TER enabled Shore and Mobile Edge Routers.
To use VDE-TER transport in the MMS, a mobile MMS Edge Router shall support VDE-TER mobile equipments' NMEA interface as defined in [30] 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 send through a MMS MIR revocation service,
3. update the local certificate storage based on certificates received from trusted VDE-TER enabled MMS Shore Edge Routers, for services the Edge Router itself subscribes to,
4. provide access to the local certificate storage for local MMS Agents, using the MMS certificate query service interface,
5. decide to use or not use a VDE-TER Shore Base Station based on local trust settings as to which VDE-TER networks to trust, based on the VDE-TER bulletin board signature received from each VDE-TER Shore Base Station,
6. receive and apply MMS capability broadcasts from VDE-TER enabled MMS Shore Edge Routers,
7. connect to a VDE-TER enabled MMS Shore Edge Router if in connectivity range,
8. use VDE-TER connectivity to a VDE-TER enabled MMS Shore Edge Router

C.2 VDE-TER transport specific function details

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

C.2.1 VDE-TER enabled MMS Shore Edge Router

This section defines the functionality an VDE-TER enabled MMS Shore Edge Router shall implement for managing a VDE-TER Network.

MMS Capability Broadcast

Routing and MMS MRN Mapping

Maintain Subscriptions

VDE-TER Broadcast VDE-TER supports the transferring of a digital payload to multiple receivers in the same radio range from a by only transmitting the message once over the air interface. The concept is called a VDE-TER broadcast message in [7].
All VDES receivers in reception range of the VDE-TER Shore Base Station receive the broadcast message and deliver it to the connected VDE-TER application for further processing over the Presentation Interface, see [VdesIec].

- ☐ describe the mapping between MMS subjectcast and VDE-TER broadcast, using the MMSI = 0 in VDES
- ☐ describe how a VDE-TER network side Edge Router does subscribe to the broadcast subjects it is considered to broadcast and the necessary parameters and configurations (repetition time, area, MRN, MSR, MIR)
- ☐ describe how a VDE-TER network transmits the list of broadcast services and the associated certificates and revocation lists
- ☐ describe how the VDE-TER mobile side Edge Router caches the service lists and certificates, and broadcasted payloads until expiration
- ☐ describe how the VDE-TER mobile side Edge Router handles subscriptions to subjects and own messages for the VDE-TER case
- ☐ describe the concept of fitting larger MMS messages into the maximum message sizes for VDE-TER
- ☐ describe how to build the VDE-TER digital payload from the VDE International Function as described in [29], Annex B.3.1

VDE-TER Direct Messages

- ☐ describe direct messaging

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

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

Therefore, the VDE-TER Shore network edge router shall maintain a status about the VDE-TER mobile station reachability through the VDE-TER shore network containing at least:

1. the position of the VDE-TER mobile station based on the latest 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 VDE-TER edge router, and.
3. the last time, a valid AIS position was received.

Automatic Clean-up

Monitor Connection States

Annex D

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 [7], General section and Annex 5 for details.
This Appendix 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.

D.1.1 VDE-SAT Satellite

VDE-SAT Satellites provide the VDE-SAT radio access for mobiles.
Note: VDE-SAT Satellites 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 Satellites coordinate the VDE-SAT ressources for all connectivity between mobile VDE-SAT equipment and themselfes according to [7].
MMS complient VDE-SAT Satellites shall route received VDE-SAT traffic that is sent to their own VDES MMSI with a VDE-SAT payload data identified as MMS according to [29], Annex B.3.1 to a VDE-SAT enabled MMS Shore Edge Router for MMS processing.
MMS complient VDE-SAT Satellites shall allow a VDE-SAT enabled MMS Shore Edge Router to send:

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

D.1.2 VDE-SAT Satellite Network

A VDE-SAT Satellite Network consists of:

- one or multiple VDE-SAT Satellites,
- connections between these VDE-SAT Satellites, and
- one or multiple VDE-SAT enabled MMS Shore Edge Routers to connect the VDE-SAT Satellite Network with the MMS Router Network.

D.1.3 VDE-SAT enabled MMS Shore Edge Router

A VDE-SAT enabled MMS Shore Edge Router provides a link between the MMS Router Network and one or multiple VDE-SAT Satellites.
A VDE-SAT enabled MMS Shore Edge Router shall conform to Section 5.2 and additionally perform at least follwing functions:

1. broadcast information about MMS capabilities for VDE-SAT enabled MMS Mobile Edge Routers over all VDE-SAT Satellites 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 Satellites,
5. using the VDE protocol format header layer to identify MMS traffic according to [29], Annex B.3.1,
6. prioritiy 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 Satellitees 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 a VDE-SAT enabled MMS Shore Edge Router may provide and announce to be available through VDE-SAT broadcasts are:

- MIR query service to retreive 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 retreive service certificates for services transported over that VDE-SAT Shore Network

D.1.4 VDE-SAT Mobile Equipment

VDE-SAT mobile equipment facilitates communication to other mobile equipment and satellites through VDE-SAT as defined in [7].
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 confirm with [7] General section and Annex 4, and shall be type approved by [30].
VDE-SAT mobile equipment shall provide a Presentation Interface to the MMS Mobile Edge Router as defined in [30].
Note: the VDE-SAT presentation interface is based on VDE-SAT specific sentences as defined in [30], transported over lightweight ethernet [31] standard providing NMEA/UDP/IP.

D.1.5 VDE-SAT enabled MMS Mobile Edge Router

A VDE-SAT enabled MMS Mobile Edge Router is a MMS Edge Router providing the MMTP interface to MMS Agents as described in Section 5.2, 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 equipments' NMEA interface as defined in [30] and 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 a MMS MIR revocation service,
3. update the local certificate storage based on certificates received from trusted VDE-SAT enabled MMS Shore Edge Routers, for services the Edge Router itself subscribes to,
4. provide access to the local certificate storage for local MMS Agents, using the MMS certificate query service interface,
5. decide to use or not use a VDE-SAT Satellites 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,
6. receive and apply MMS capability broadcasts from VDE-SAT enabled MMS Shore Edge Routers,
7. connect to a VDE-SAT enabled MMS Shore Edge Router if in connectivity range,
8. use VDE-SAT connectivity to a VDE-SAT enabled MMS Shore Edge Router

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 enabled MMS Shore Edge Router

This section defines the functionality an VDE-SAT enabled MMS Shore Edge Router shall implement for managing a VDE-SAT Network.

MMS Capability Broadcast

Routing and MMS MRN Mapping

Maintain Subscriptions

VDE-SAT Broadcast VDE-SAT supports the transferring of a digital payload to multiple receivers in the same radio range from a by only transmitting the message once over the air interface. The concept is called a VDE-SAT broadcast message in [7].
All VDES receivers in reception range of the VDE-SAT Satellite receive the broadcast message and deliver it to the connected VDE-SAT application for further processing over the Presentation Interface, see [VdesIec].

- ☐ describe the mapping between MMS subjectcast and VDE-SAT broadcast, using the MMSI = 0 in VDES
- ☐ describe how a VDE-SAT Network Shore Edge Router does subscribe to the broadcast subjects it is considered to broadcast and the necessary parameters and configurations (repetition time, area, MRN, MSR, MIR)
- ☐ describe how a VDE-SAT Network transmits the list of broadcast services and the associated certificates and revocation lists
- ☐ describe how the VDE-SAT mobile side Edge Router caches the service lists and certificates, and broadcasted payloads until expiration
- ☐ describe how the VDE-SAT mobile side Edge Router handles subscriptions to subjects and own messages for the VDE-SAT case
- ☐ describe the concept of fitting larger MMS messages into the maximum message sizes for VDE-SAT
- ☐ describe how to build the VDE-SAT digital payload from the VDE International Function as described in [29], Annex B.3.1

VDE-SAT Direct Messages

- ☐ describe direct messaging

VDE-SAT Mobility Management The link between a VDE-SAT Satellite and a VDE-SAT mobile station is subject to permanent changes due to:

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

Therefore, the VDE-SAT Shore Network Edge Router shall maintain a status about the VDE-SAT mobile station reachability through the VDE-SAT Network containing at least:

1. the position of the VDE-SAT mobile station based on the latest AIS received position,
2. the best VDE-SAT satellite to use to send messages to the VDE-SAT mobile station, according to the configuration of the VDE-SAT edge router, and.
3. the last time, a valid AIS position was received.

Automatic Clean-up

Monitor Connection States

Annex E

Quality of Service profile

This Appendix describe the use of the Quality of Service fields provided by the MMTP.

Annex F

MMS Motivational Use Cases (Informative)

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

F.1 MUC1: User group - Navigator

F.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.

F.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.

F.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.

F.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 safe the lives of my crew.

F.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.

F.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.

F.2 MUC2: User group - Maritime Service Provider

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

F.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.

F.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.

F.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.

F.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.

F.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.

F.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.

F.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.

F.3 MUC3: User group - Pilot

F.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.

F.4 MUC4: User group - Ship Owner

F.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.

Annex G

MMS Binding for ITU-R M.2116 [1]

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 that utilize the band 4400-4800 MHz. The International Radio Regulations designate this 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 4400-4800 MHz, 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 4400-4800 MHz 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 H

MMS Binding for NAVDAT

NAVDAT [32] is a broadcast service operating in the MF band, with very large range >1000km. It is an evolution of NAVTEX, which is part of SOLAS today.
This appendix describes which MMS components need adaptations to allow the transport of secure and trusted maritime services over MMS and NAVDAT, such that ships can:

1. identify the data and encodings of transmissions clearly,
2. authenticate the source of the data, and
3. check for authentity and integrity of the data.

Annex I

MMS Binding for SECOM

Under development.

Annex J

Protobuf Definition of MMTP

```
syntax = "proto3";

message ApplicationMessage {
  ApplicationMessageHeader header = 1;
  bytes body = 2;
  string 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;
  }
}

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 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;
}

message ResponseMessage {
  string responseToUuid = 1;
  ResponseEnum response = 2;
  optional string reasonText = 3;
  repeated MessageMetadata messageMetadata = 4;
  repeated ApplicationMessage applicationMessages = 5;
  optional string reconnectToken = 6;
```

```
}

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

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

Bibliography

[1] 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.

[2] M. Thomson. Version-Independent Properties of QUIC. https://datatracker.ietf.org/doc/html/rfc8999.

[3] J. Iyengar and M. Thomson. QUIC: A UDP-Based Multiplexed and Secure Transport. https://datatracker.ietf.org/doc/html/rfc9000.

[4] M. Thomson and S. Turner. Using TLS to Secure QUIC. https://datatracker.ietf.org/doc/html/rfc9001.

[5] J. Iyengar and I. Swett. QUIC Loss Detection and Congestion Control. https://datatracker.ietf.org/doc/html/rfc9002.

[6] Eddy Wesley. Transmission Control Protocol (TCP). https://datatracker.ietf.org/doc/html/rfc9293.

[7] 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-I/en.

[8] IMO. Imo e-Navigation strategy implementation plan.

[9] Maritime Connectivity Platform Consortium. Mcc identity management and Security, revision 2.

[10] S. Cheshire and M. Krochmal. Multicast dns. https://datatracker.ietf.org/doc/html/rfc6762.

[11] S. Cheshire and M. Krochmal. Dns-based service discovery. https://datatracker.ietf.org/doc/html/rfc6763.

[12] E. Rescorla. The transport layer security (TLS) protocol version 1.3, 2018. https://www.rfc-editor.org/rfc/rfc8446.

[13] Google LLC. Protocol Buffers Documentation. https://protobuf.dev/.

[14] P. Leach, M. Mealling, and R. Salz. A Universally Unique IDentifier (UUID) URN namespace. https://www.rfc-editor.org/rfc/rfc4122.

[15] 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.

[16] National Institute of Standards and Technology. Fips 186-5 - digital signature standard (dss). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf.

[17] R. Housley W. Polk and L. Bassham. Algorithms and identifiers for the internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. https://www.rfc-editor.org/rfc/rfc3279.html.

[18] Protocol Labs. libp2p. https://libp2p.io/.

[19] Protocol Labs. Connection establishment in libp2p. https://github.com/libp2p/specs/blob/master/connections/README.md.

[20] Protocol Labs. libp2p tls handshake. https://github.com/libp2p/specs/blob/master/tls/tls.md.

[21] Protocol Labs. libp2p kademlia dht specification. https://github.com/libp2p/specs/blob/master/kad-dht/README.md.

[22] Protocol Labs. Pubsub interface for libp2p. https://github.com/libp2p/specs/blob/master/pubsub/README.md.

[23] 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.

[24] I. Fette and A. Melnikov. The WebSocket Protocol. https://www.rfc-editor.org/rfc/rfc6455.

[25] 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.

[26] Tim Bray. The JavaScript object notation (JSON) data interchange format. https://www.rfc-editor.org/rfc/rfc8259.

[27] MCP Consortium. Maritime identity registry of the maritime connectivity platform. https://maritimeconnectivity.net/.

[28] MCP Consortium. Maritime service registry of the maritime connectivity platform.

[29] IALA. Guideline G1117: G1117 VHF DATA EXCHANGE SYSTEM (VDES) OVERVIEW. https://www.iala-aism.org/product/g1117/.

[30] IEC. Iec 63514 draft: Maritime navigation and radiocommunication equipment and systems – VHF Data Exchange System – Requirements and Methods of testing for shipborn mobile station.

[31] 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.

[32] 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.

[33] IALA guideline G1128, 2018. https://www.iala-aism.org/product/g1128-specification-e-navigation-technical-services/, **The Specification of e-Navigation technical services**, edition 1.2.

[34] Maritime Connectivity Platform Consortium. Mcc identity management and security: Public key infrastructure (pki), version 1.02.