D2.11 - Specification of Protocols for ship-to-shore communication

Project no.	636329
Project acronym:	EfficienSea2
	EFFICIENSEA2 – efficient, safe and sustainable traffic at sea
Funding scheme:	Innovation Action (IA)
Start date of project:	1 May 2015
End date of project:	30 April 2018
Duration:	36 months
Due date of deliverable:	25 April 2017
Actual submission date:	
Revised submission date:	-
Organisation in charge of deliverable:	Partner 21, DANELEC

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

DOCUMENT STATUS

Authors and contributors

Name	Organisation
Henrik Bech Helnæs (editor)	Danelec Marine
Erik Styhr Petersen	Wärtsilä
Anton Karelskiy	Transas
Timo Kostiainen	Furuno
Peter Andersen	Cobham

Document History

Version	Date	Initials	Description
0.01	2016-09-19	HBH	First Draft
0.02	2016-09-23	HBH	Update after Hamburg meeting
0.03	2016-09-17	HBH	50% review
0.04	2017-03-03	HBH	75% review
0.05	2017-04-06	HBH	100% review
1.00	2017-04-25	HBH	Final Deliverable

Reviewers

Name	Organisation
Andy Winbow	CIRM
Krzysztof Bronk	NIT
Soeren Schweigert	OFFIS
Timo Kostiainen	FURUNO
Peter Andersen	COBHAM
Axel Hahn	OFFIS

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

Contents

1 DEFINITIONS AND ACRONYMS 5

2 INTRODUCTION 7

3 SCOPE 8

4 LOGICAL ARCHITECTURE AND DESIGN 9
4.1 Simple implementation 9
4.2 Roaming function 11
4.3 Cyber Security and IEC-61162-460 Firewall/Gateway 12
4.3.1 HTTPS Proxy Server Requirements 13
4.4 Helper Components 14
4.4.1 Almanac 14
4.4.2 Reaching on-board services from shore 15
4.4.3 Transport of large amounts of data 17
4.4.4 Large Data Transport Service 19
4.4.5 Replication between Databases on-board and on-shore 20

5 INTERFACES 22
5.1 REST 22
5.2 SOAP 22
5.3 Conclusion on Interfaces 23

6 NON IP MEDIA GATEWAYS 24
6.1 MMS Client Component using non IP Media Gateway 26

7 MARITIME CLOUD DEMONSTRATOR COMPONENT 28

8 EFFICIENT PROTOCOLS VESSEL/SHORE 29
8.1 TCP and FTP over high latency, low bandwidth communication channels. 29
8.2 TLS over high latency, low bandwidth communication channels (hereunder HTTPS). 29
8.3 Virtual Private Networks (VPN) 30
8.4 UDP over high latency, low bandwidth communication channels. 30
8.5 Privacy vs. compression 31
8.6 Vessel Public or Local IP Address and IP v4 vs. IP v6 31
8.7 IP v4 vs. IP v6 32
8.8 IP Traffic over VDES 32
8.8.1 IP Addresses and VDES 33
8.8.2 Routing of IP traffic between VDES nodes 34

9 DEPLOYMENT CONSIDERATIONS AND ARCHITECTURE UPDATE 36

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

10 PROPOSED DEMONSTRATOR 37

11 IDENTIFICATION OF POTENTIAL AREAS FOR STANDARDIZATION 38

12 CONCLUSION 39

BIBLIOGRAPHY 40

13 APPENDIX A –REVIEW REPORT 41

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

1 Definitions and Acronyms

AE	Architectural Element
AIS	Automatic Identification System (IEC 62320:2008)
ASM	Application Specific Messaging
DMZ	Demilitarised Zone
E2	EfficienSea2
ECDIS	Electronic Chart Display and Information System (IEC 61174:2015)
FTP	File Transfer Protocol
FTPS	File Transfer Protocol over SSL (now TLS)
FW	Firewall
GPS	Global Positioning System
GW	Gateway
HTTP	Hyper Text Transfer Protocol
ICS	Integrated Communication System
IETF	Internet Engineering Task Force
IR	Identity Registry
MC	Maritime Cloud
MCC	Maritime Cloud Client Component
MCDC	Maritime Cloud Demonstrator Component
MMS	Maritime Messaging Service
MSP	Maritime Service Portfolio
NAS	Network Attached Storage
NAT	Network Address Translation
NAVTEX	Navigational Telex
OSI	Open Systems Interconnection
PKI	Public Key Infrastructure
QoS	Quality of Service
RADAR	Radio Detection And Ranging (IEC 62388:2013)
REST	Representational State Transfer
RD	Roaming Device
SFTP	Secure FTP or FTP over SSH
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SOLAS	Safety of Life at Sea (SOLAS Convention, 1974, with amendments)
SR	Service Registry
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transport Connection Protocol
TLS	Transport Layer Security

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

UDP	User Datagram Protocol
VDE	VHF Data Exchange
VDES	VHF Data Exchange System
VDR	Voyage Data Recorder (IEC 61996:2013)
VLAN	Virtual Local Area Network
VPN	Virtual Private Nework
VTS	Vessel Traffic Service
W3C	World Wide Web Consortium
WAN	Wide Area Network
Wi-Fi	a trademark of the Wi-Fi alliance (WLAN or Wireless Local Area Network)
XML	Extensive Markup Language
Zeroconf	Zero-configuration networking

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

2 Introduction

This document is a deliverable produced by WP2 Task 2.4 – shipboard system integration and on-board networks.
In short, the Task 2.4 is about shipboard system integration in terms of cyber security, on-board network integration and firewalling as well as integration of systems with the shipboard component of the MC concept.
The first deliverable of Task 2.4 was D2.10 Recommended On-Board Network Architecture and this deliverable is capturing the succeeding work in defining the on-board architecture as well as the protocols for vessel to shore communication.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

3 Scope

The deliverable D2.11 as described in the E2 consortium agreement is to provide the specifications for the protocols for vessel-to shore communication for the different types of equipment on board the vessel.

Since other Work Packages in E2 are developing service architecture and some service descriptions, including interface specifications, the scope of T2.4 D2.11 has been changed to include a more elaborate on-board logical architecture/design with discussion of various types of helper components and what services they could provide for on-board MC clients.

Work done in WP2 and WP3 has shown that there is a need to elaborate more on the on-board architecture and that the definition of the MC, in particular with respect to the Maritime Cloud Demonstrator Component (MCDC), needed to be refined.

With upcoming low bandwidth VDES communication channels there is a wish to be able to extend internet communication to progress via this channel and maybe even allow MC services to use this.

A definition of a Maritime Messaging Service (MMS) are being developed, both by parties in the EfficienSea2 project, but also in other organisations and projects.

The D2.11 scope is thus:

- Develop and describe the on-board logical architecture/design
- Describe requirements for standard interface to the MC IR and SR
- Describe requirements for standard interface to the T2.3 RD
- Discuss and recommend efficient communication protocols (in IP domain) to be used between clients and services in the MC
- Review and update the T2.4 D2.10 Recommended on-board network architecture
- Describe proposed demonstrator implementation D2.12 to be delivered in M36
- With the current understanding of the MMS, demonstrate how this component is located in the on-board architecture/design

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

4 Logical Architecture and design

This chapter describes the proposed logical architecture and top level design on the components of the MC with focus on the on-board components and how they interface/communicate to/from shore components of the Cloud.

The various diagrams show relations on the transport level only and hence the components and communication done to enable establishment of transport connections on lower OSI layers are not shown.

In summary, the proposed logical architecture and design, will only allow transport layer endpoints. E.g. the implementation of messaging via VDES in AIS and NAVTEX must be done in a similar way so that it adheres to the OSI model and that endpoints in this type of messaging are always on the transport level.

4.1 Simple implementation

The simplest implementation of a client of the MC using a service that has been discovered using the SR and authenticated using the IR is shown in Figure 1.

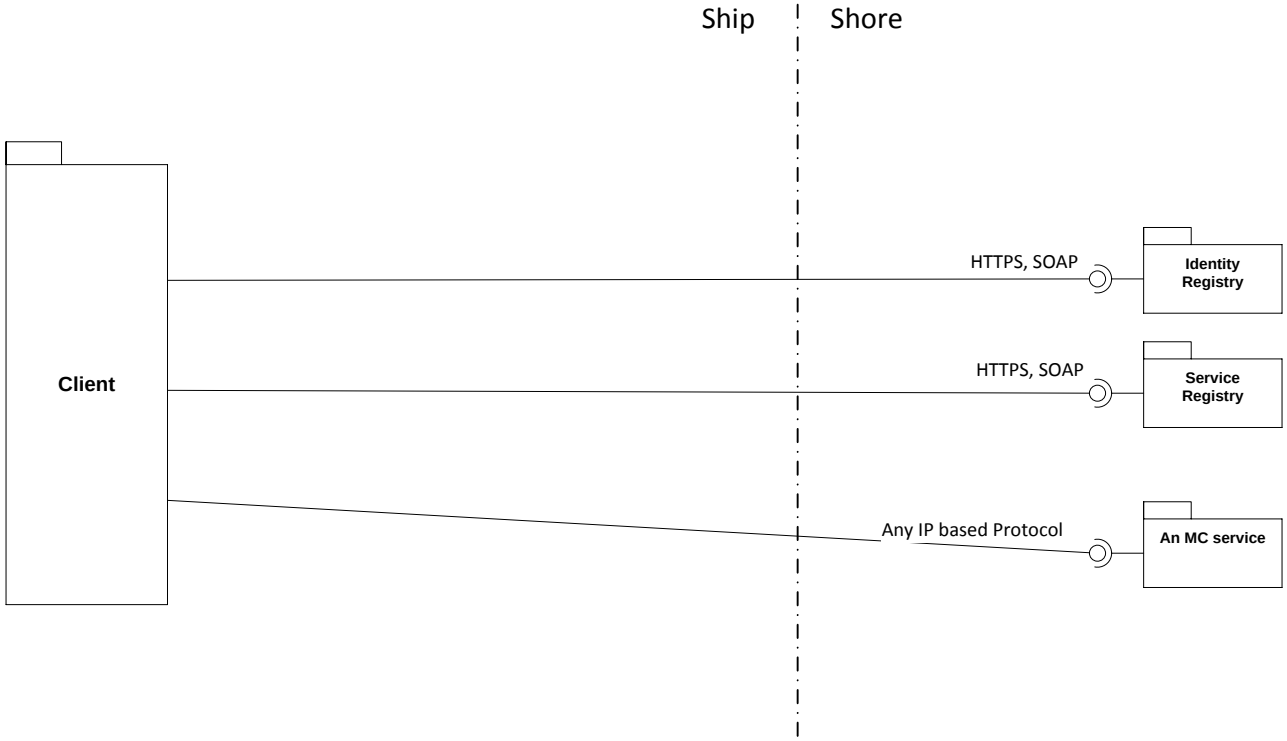

Figure 1 Simplest implementation of a maritime cloud client

Note that the diagram does not implement any cyber security using a firewall, nor does it contain a RD. It should be pointed out that a RD is not an essential part of MC

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

communications; indeed, it does not have to be present at all. The purpose of a RD is to reduce/optimize bandwidth requirements in balance with communications cost, and while a MC solution undoubtedly would benefit from this enhancement, it is exactly what it is: an enhancement, not a basic requirement without which the MC communications cannot work.

The following chapters will add the RD and firewall to the architecture.

The diagram depicts the simplest use of the MC as described in (E2-T3.1-D3.2, 2015). Also note that the diagram also defines that protocol and interface to the IR and SR are HTTPS and SOAP. The rationale for that is described in chapter 5.

Since the Conceptual model of the MC does not specify how particular services are implemented – i.e. it does not require for example HTTPS and SOAP. The protocol and interface used to communicate with the service could be any IP-based one. For example, part of a service interface could be REST based and another part could be based on FTP and even UDP protocols.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

4.2 Roaming function

Figure 2 illustrates how to accommodate seamless roaming of traffic between various communication channels, and how a client can use the roaming components interface to setup QoS for the communication that it needs to make for services/ components on shore.
The RD protocol and interface to the MC i.e. the on-board clients, are required to be SOAP using HTTPS as the application layer protocol. The rationale is described in chapter 5. The EfficienSea2 deliverable (E2-T2.3-D2.8, 2016) D2.8 Interface to Maritime Cloud, amongst others, specifies that interface.

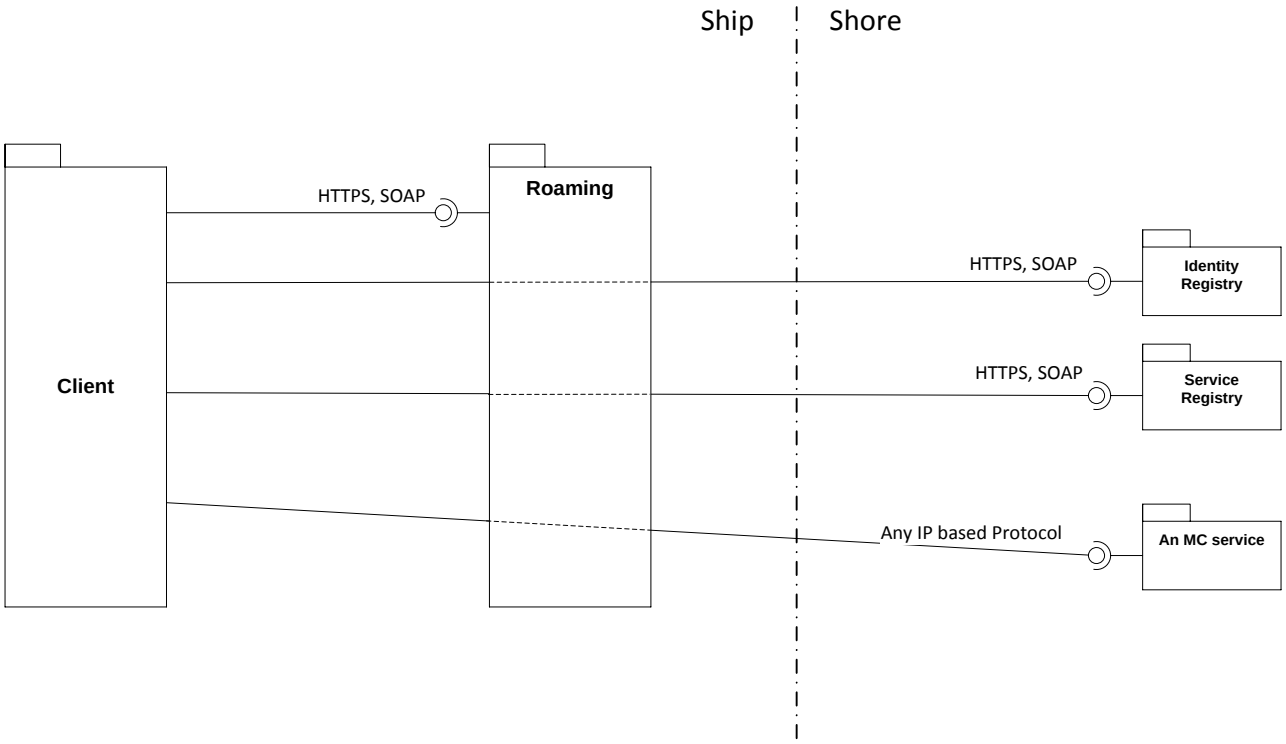

Figure 2 RD to manage multiple communication Channels and QoS

Apart from the Interface to setup QoS for communication, the RD acts transparently to any IP-based communication to/from the vessel. This includes the communication with the IR and SR.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

4.3 Cyber Security and IEC-61162-460 Firewall/Gateway

The Cyber Security considerations in (E2-T2.4-D2.10, 2016) D2.10 Recommended On-Board Network Architecture, found that use of IEC62216-460 Firewall/Gateways to ensure Cyber Secure protection of network zones was needed. Since clients often reside in a secure zone, Figure 3 shows how such a Firewall/Gateway can be applied.
Clients that are cyber secure can of course exist on the unprotected side.

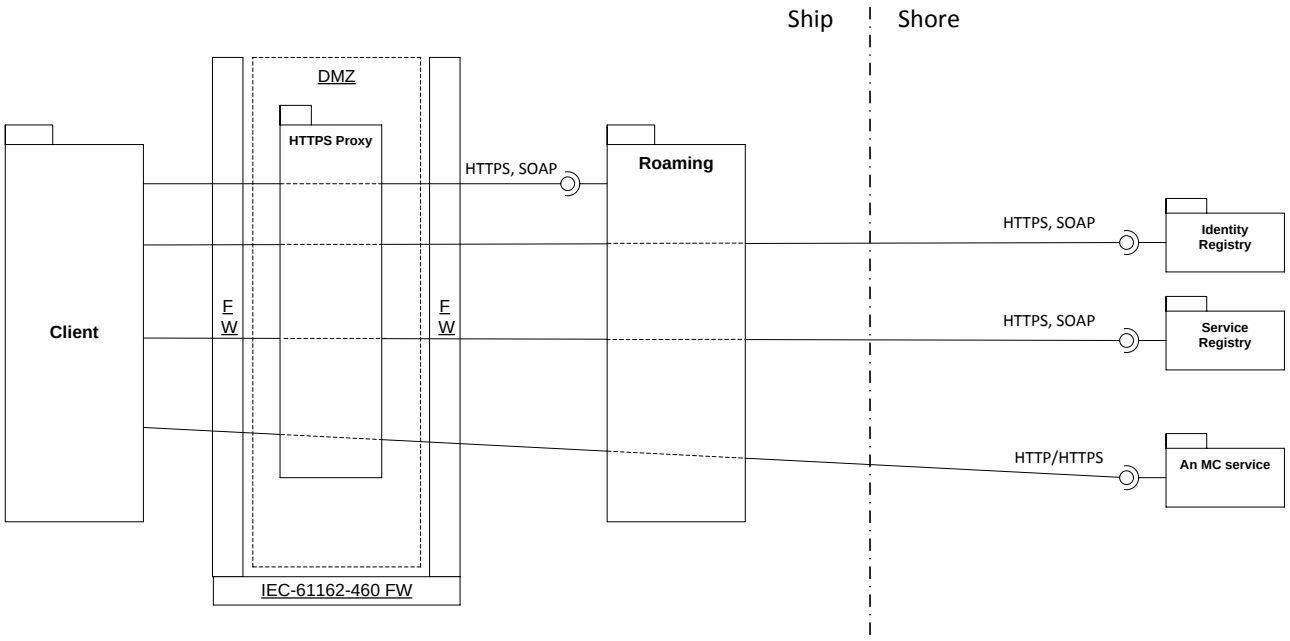

Figure 3 Client Communication through -460 Firewall

The -460 firewall is a dual firewall, partly due to the need to deny direct IP-based connections through the firewall. This is done so that the same IP ports are not open on both the inside and outside the FW. The -460 standard is very specific on this topic when it comes to e.g. VPN connections through the firewall – which would violate the above IP port opening restriction. The -460 standard then describes that such VPN connections e.g. should be time limited.

On top of the basic Packet Filtering function of a dual firewall, it traditionally also contains Application Gateways that apply security mechanisms to specific applications such as FTP and Telnet servers.
Further, it contains Circuit-level gateways that apply security for TCP or UDP connections that are established. Circuit-level gateways also include state-full inspection functionality that tracks the state of each connection and its protocol, and only allows “legal” state transitions.
The latest in traditional firewalls include threat management that also includes abilities to apply filters for malware and viruses as well as detection and blocking of denial of service attacks.

“This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 636329”.

Next-generation firewalls or, one should rather say, present day firewalls also include:

- Integrated intrusion prevention
- Application awareness and control to see and block risky apps
- Upgrade paths to include future information feeds
- Techniques to address evolving security threats

Two of the basic techniques in a firewall are network address translation (NAT) and proxy servers.

The following will describe the requirements for a HTTPS proxy server, in a -460 Gateway.

4.3.1 HTTPS Proxy Server Requirements

A proxy can keep the internal network structure of a network secret by using network address translation, which can help the security of the internal network. This makes requests from machines and users on the local network anonymous.

There are several types of proxy servers.

- A proxy server that passes requests and responses unmodified is usually called a gateway or sometimes a tunneling proxy.

- A forward proxy is an internet facing proxy used to retrieve from a wide range of sources.

- A reverse proxy uses a front-end to control and protect access to a server on a private network. A reverse proxy amongst others takes care of authentication and en/decryption.

For the purpose of vessel to shore initiated communication, a reverse proxy is of little use. A basic network address translating gateway is sufficient. Application of a reverse proxy that terminates HTTPS sessions, just to forward the payload into other established HTTPS sessions to shore would be a security risk and not needed.

The network address translation is however needed to obtain cyber security.

For the purpose of shore to vessel initiated communication, where services on vessel are to be contacted by shore-based clients, the reverse proxy type in combination with VPN tunnelling will be required, as described later in this document.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

4.4 Helper Components

This chapter discusses various possible helper components that might be beneficial to have in the architecture for various reasons.

One reason could be that if clients would need to implement the same functionality and that functionality would be so significant that a shared component implementing the functionality would make sense.

Another reason could be that if clients would need to communicate the same information across the sparse communication links to shore, it would make sense that clients share a component that communicates and holds that information.

4.4.1 Almanac

One helper component that has been described in Pre-EfficienSea2 work and in the (E2-T3.1-D3.2, 2015) MC Conceptual Model is the Almanac.
The almanac could be as simple as an off-shore version of the IR and the SR, but it could also offer more sophisticated service discovery and authentication methods.
An Almanac could also expand the set of services offered via shore-based SR with on-board services (or local services).
An Almanac could also implement a service availability policy and hence require clients to be restricted to that policy on a vessel or a fleet of vessels.

It should be noted here that clients are not required to use the Almanac, and could still perfectly well communicate directly with the shore-based IR and SR.

In Figure 4 the recommended placement in the logical architecture is shown. Please note that in this example, the Client only uses the Almanac to get IR and SR information. It could as well communicate directly with the IR and SR on shore.

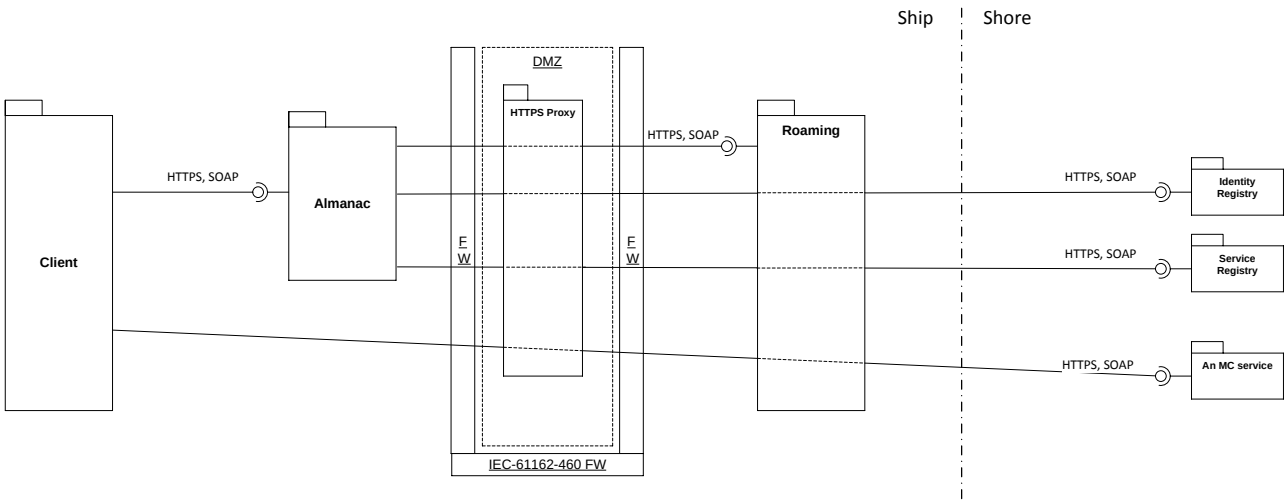

Figure 4 Almanac to simplify Clients and minimize communication

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

Since a protocol/interface to the almanac for the clients will be shared in a similar fashion as the IR and SR, the protocol/interface needs to be standardized. Hence the requirement for HTTPS and SOAP (ref. chapter 5)

4.4.2 Reaching on-board services from shore

For the majority of installations with IP communication over SATCOM and even 3g/4g, the vessel and services on the vessel do not have an endpoint reachable from shore or other vessels.
Since the vessel communicate through multiple medias, with different providers, it is not possible to allocate one static public IP address across those providers, that makes it possible to give the vessel an endpoint reachable from shore. See chapter 8.6 and chapter 8.7

To achieve a flexible architecture/design, it is desirable that the architecture appears symmetric in the sense that one could place as service on-board a vessel and it would appear just the same as if it was located on shore without requirement for change or additions to the service interface.
Clients that use an MC Service on-board a vessel discover the service using the SR, just as any other MC Service. Authorisation and Authentication is also using IR and the defined methods of the MC, just as if the service was located on shore.

An exercise to prove such a property of the architecture could be to exchange the vessel and shore sides and demonstrate that MC services on-board a vessel was reachable from shore.

The following describe that one example method of achieving symmetry is to establish a shore based non mobile entity with a static public IP address.

The IEC61162-460 standard does not allow permanent VPN connections through the -460 Gateway/Firewall. To overcome that limitation in a cyber secure way, a helper component could be a VPN Service e.g. in the simplest form of a VPN Router in the -460 DMZ as shown in Figure 5. See chapter 8.3 for discussion of VPN and VPN properties.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

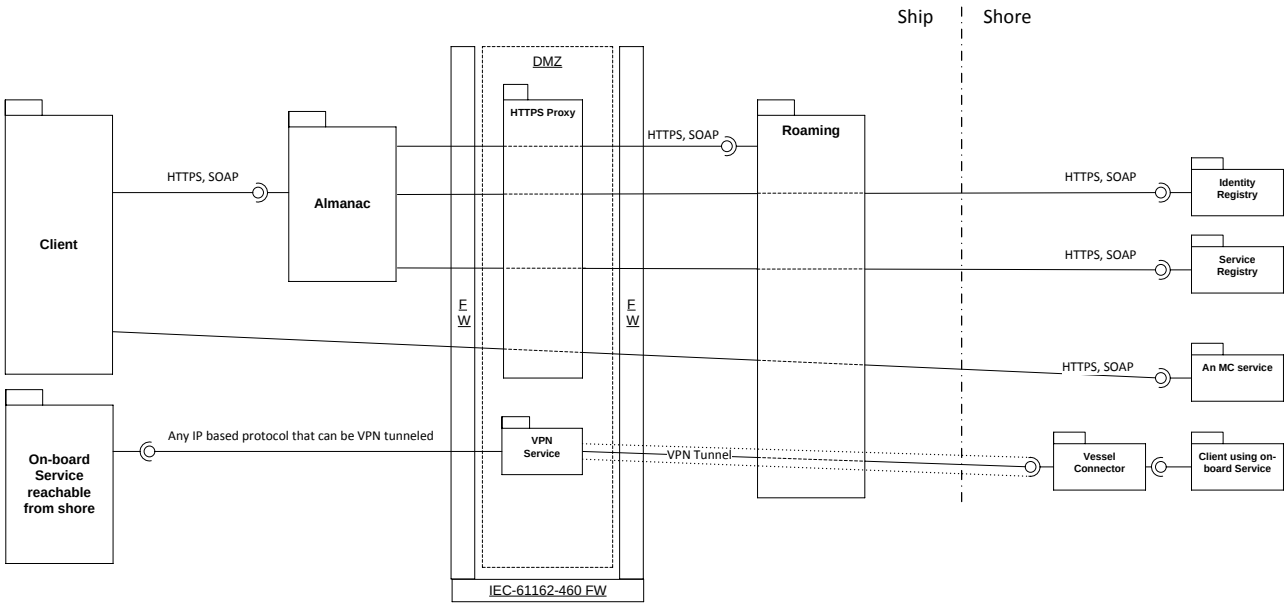

Figure 5 Reaching an on-board Service from shore

Since the VPN service component is in the DMZ, it would be allowed to create a permanent VPN tunnel to a shore-based entity. It could then allow for shore initiated transport sessions to on-board services with a proper cyber secure authentication as shown using the shore based “Vessel Connector”.

With the VPN Service setup in Figure 5, the Vessel Connecter needs to be sufficiently Cyber Secure, since access to a secure zone on the vessel is provided, even though the in-bound Firewall only provides access to the on-board Service to be reachable from shore. Alternatively a higher level of cyber security can be achieved by adding a reverse proxy server in the DMZ so that shore-based clients are forced to authenticate with this server, before the on-board service can be used.

Figure 17 shows how a VPN Service can be implemented securely by combining a VPN Client with a Reverse HTTPS Proxy Server.
Initially, the VPN Client establishes a VPN Tunnel to the Vessel Connector, allowing shore-based clients to initiate connections to the on-board services. The VPN Client may also want to establish appropriate QoS for the VPN connection by setting this up with the RD.
The Reverse Proxy may require authentication of incoming connections before allowing traffic to on-board services. This, however depends on the security level of the zone that the Vessel Connector and the shore based client is in.

“This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 636329”.

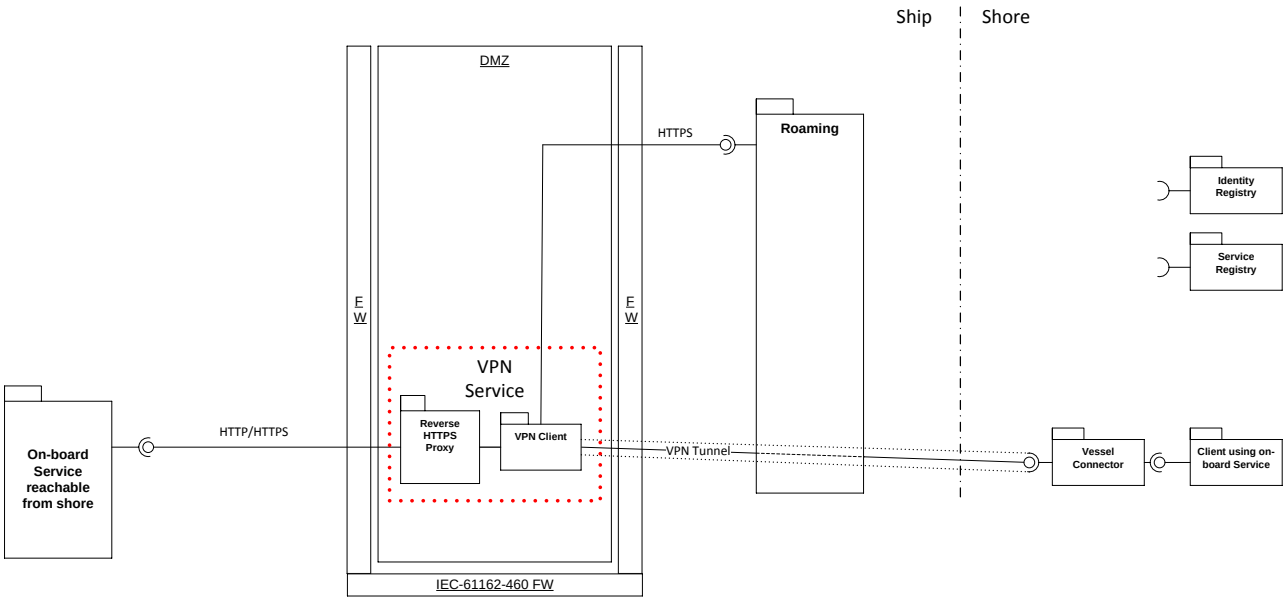

Figure 6 VPN Service Implementation Example

The Sea Traffic Management (STM) validation project (STM Communications, 2017) has defined a component similar to the Vessel Connector and has named it SeaSwim Connector. At the time of writing, the specification of the SeaSwim Connector has not yet been finalized, but here a reference to the draft specification (Fabio Renda, 2016).

The requirement as set out by the scope of EfficienSea2 is to provide standardized and preferably open-source to enable easy implementation, integration with existing IT infrastructures and wide acceptance of the MC. However, the establishment of a VPN connection to a shore based Vessel Connector is considered highly dependent of the particular vessel owner IT infrastructure and requirements for cyber security. It is therefore left out of scope of this document to recommend or promote any standard solution.

4.4.3 Transport of large amounts of data

This chapter discuss some of the service types offered by many SATCOM providers today that support transport of large amounts of data.
The services offered are using standardized interfaces on-board and on-shore, but implementation methods are often proprietary.

4.4.3.1 Data mirror services

Some of the services offered by SATCOM providers are works as file repository mirror service.
A file server is located on-board the vessel with standardized SMB or NAS interface accessible by clients on the vessel. Similarly a file server is located on shore with similar standardized SMB or NAS interfaces towards clients on shore. The two file repositories

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

are synchronized, so that any changed content on either side is synchronized to the remote side. The synchronization service is proprietary and highly optimized to reduce sat-com bandwidth usage.
The mirror services may offer multiple shore instances. E.g. the file repository on-board the vessel may contain separate folders that gets synchronized with different shore file servers.
The synchronization traffic is of course encrypted and the client uses the standardized authorization with the file servers to gain access to the synchronized content.
The advantage of this type of service is that control of QoS is quite straight forward and can be given lower priority so that large data transfer can occur in background in a similar manner as e-mail traffic.

4.4.3.2 FTP Proxy servers

Some of the services offered by SATCOM providers are using instances of FTP proxy servers.
The FTP proxy servers terminate the FTP connections from the clients, but are transporting the FTP data and commands in an optimized manner to the shore-based FTP proxy counterparts.
The traffic between two FTP proxy servers are then highly optimized to reduce SATCOM bandwidth and introduce higher reliability for the FTP connections, given the latency and dropout characteristics of SATCOM connections.
The advantage of this latter service is that it has a standardized FTP interface and is able to transport media to any shore based FTP server.
Variants of services based on FTP is FTP over SSH (SFTP) and FTP over SSL (FTPS).
If the service is implemented as FTP over SSH (SFTP), the proxy servers involved would need to terminate the SSH sessions locally if any optimizations providing higher efficiency than plain SFTP is to be done.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

4.4.4 Large Data Transport Service

This chapter describes and demonstrates how a Large Data Transport Service, dedicated to move large amounts of data to/from shore efficiently, can be constructed.

It can be imagined that a MC Service might involve moving larger amounts of data between the service and the client. The example in this chapter can then be considered a helper service to the MC Service.

The idea with the service is that large data amounts can be posted for transfer and that the transfer can be executed asynchronously to the client / service communication (A service similar to an UPS service, just for digital payloads).
This type of service could be centralized and standardised.

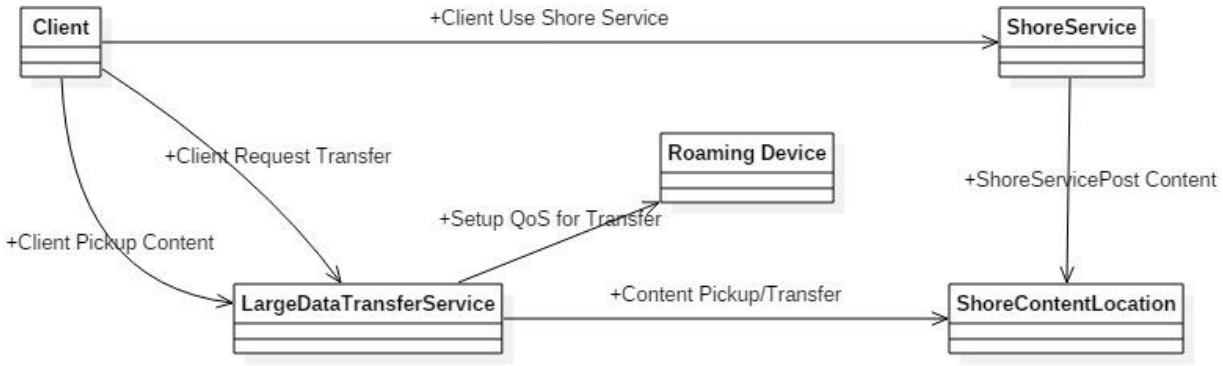

Figure 7 Classes and Associations for a Large Data Transport Service

Figure 7 illustrates a Client that is in the process of using a shore service (assuming IR and SR already used to establish the association). As a result of the Client's use of the shore service a large data amount has to be delivered to the client. The Shore Service provides information to the Client on where the data content is located (URL) alongside with metrics and credentials to use to get access to the data. The client then uses a local on-board service (Large Data Transfer Service) that is specialized in handling transfer of data to/from shore efficiently.
The Transfer Service provides the client with estimated time of arrival of the large data and transfer session identification/handle for later reference.
The Large Data Transfer Service is of course able to setup the QoS required for the particular Transfer by using the RD Configuration Interface.

Figure 8 shows a sequence diagram of the communication involved in an asynchronous transfer of large data content. Note that the diagram does not include details on service discovery, authentication etc. These details can be found in (E2-T3.3-D3.7, 2016) Technical Specification of the Maritime Cloud. Also it does not describe any particulars of the Shore Service. One can imagine that the Shore Service could be a sea chart provider and the sea charts then constitute the large data to transfer.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

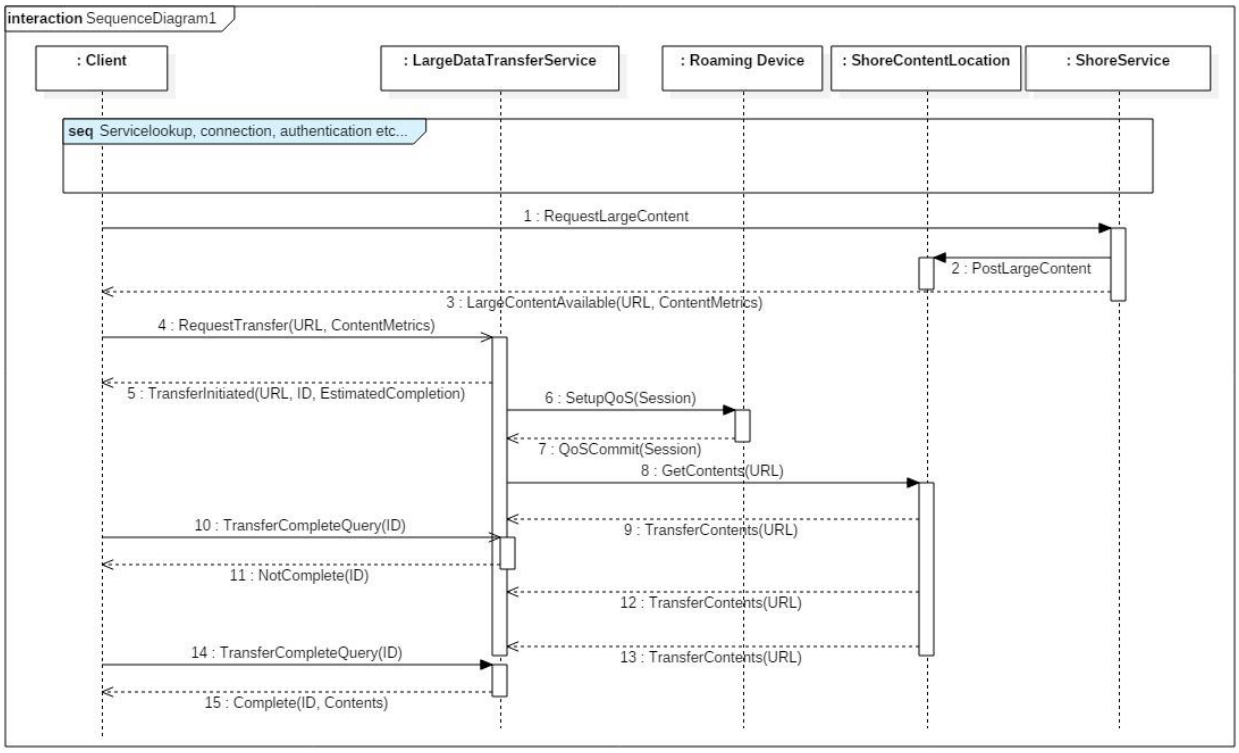

Figure 8 Sequence Diagram for the communication involved for a Large Data Transfer Job

A large data transfer service as shown in Figure 7 could very well be implemented with available open source based SFTP client and servers with additional simple service applications.

4.4.5 Replication between Databases on-board and on-shore

A use-case derived from work in E2 Task 5.1 and 2 Development of a new common port database concept and structure (E2-T5.1-D5.3, 2016) and identified in liaison work between WP5 and WP2 T2.4 is the need for replication of databases on-board and on-shore.
It is imagined that a general structure of databases containing information needed to generate a large range of documents to be submitted in relation to port reporting as well as information needed to operate and plan vessels port of call efficiently.
Much of the information is confidential and owned by the vessel owner/operator and other information is publicly available.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

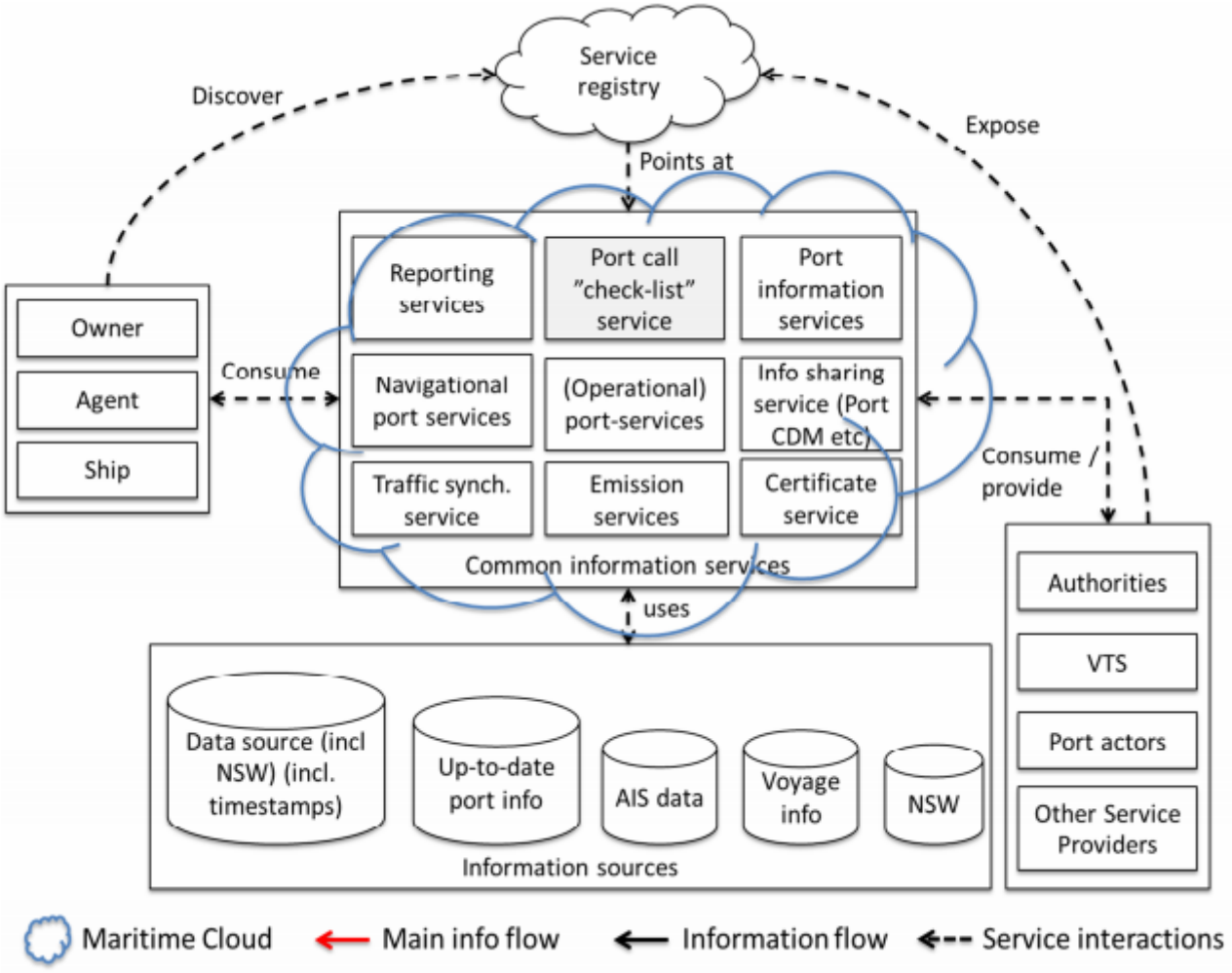

Figure 9 An architecture as illustrated in E2 D5.3

In Figure 9, the relation to ship/shore communication and protocols, the Box containing the Owner, Agent and Ship becomes the focus.

In discussion with WP5, it is agreed that the communication between the entities Owner, Agent and Ship in relation to port reporting, port databases etc. are of administrative nature. The administrative infrastructure and related communication are very dependent of the vessel owner and are not in scope for T2.4. The only requirement is that the T2.4 recommended on-board architecture and related communication does not prevent and can co-exist with the administrative infrastructure.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

5 Interfaces

This chapter describe requirements for the interface provided by the generic services of the MC, namely the IR, the SR, the on-board RD and the various on-board helper components.

The E2 WP3 has had early discussion on the pro's and con's of various choices and there has been a strategic decision on HTTP/HTTPS based communication where choices landed between SOAP and REST.

5.1 REST

Representational state transfer (REST) or RESTful web services are one way of providing interoperability between computer systems on the internet. REST-compliant web services allow requesting systems to access and manipulate textual representations of web resources using a uniform and predefined set of stateless operations.
By making use of a stateless protocol and standard operations REST systems aim for fast performance, reliability, and the ability to grow, by using reusable components that can be managed and updated without affecting the system as a whole, even while it is running.

REST is an architectural form, and is not an international standard.
Interface/implementation has to live up to certain criteria before it can be called RESTfull.

5.2 SOAP

SOAP (Simple Object Access Protocol) is a protocol specification for exchanging structured information in the implementation of web services in computer networks. Its purpose is to induce extensibility, neutrality and independence. It uses XML Information Set for its message format, and relies on application layer protocols, most often Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission.

SOAP allows processes running on disparate operating systems (such as Windows and Linux) to communicate using Extensible Markup Language (XML). Since Web protocols like HTTP are installed and running on all Operating systems, SOAP allows clients to invoke web services and receive responses independent on language and platforms.

SOAP is a W3C Recommendation and as such, precise and standardized.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

5.3 Conclusion on Interfaces

Since one of the goals of E2 is to deliver inputs to standardization, and it is obvious that the interfaces to generic entities of the MC are subject for standardization. Hence it is recommended that the following interfaces must be specified using the SOAP standard:

- Interface to IR
- Interface to SR
- Interface to RD
- Interfaces to generic on-board Helper Components

This conclusion does not prevent the existence of MC services that are REST based only. In fact, it is believed that a majority of services developed, will be REST based initially. As services mature and some move into navigation and safety related services, and become standardized, it is believed that these will be required to provide SOAP based interfaces.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

6 Non IP Media Gateways

In the E2 project, there has been quite some debate on end-points and discussions to solve the problem of clients wanting to both communicate with IP-based services as well as over non-IP radio links, such as VDES, AIS/ASM. Especially the worries have been how to integrate the legacy NAVTEX and AIS with the IP domain of the maritime cloud. The outcome has led to confusion and mixing layers of the OSI model as well as giving a hard time defining the parameters when specifying QoS in the RD interface to MC.

This chapter will attempt to provide a solution to this problem.

Until now, the list of possible communication endpoints as defined in D2.8 (E2-T2.3-D2.8, 2016) is a mix between endpoint types in the IP domain and endpoints in the non-IP domain.
This means that the client no-matter what, has to distinguish between endpoint types and act differently depending on the nature of the communication media.

The mesh of nodes in the IP domain (the network and the internet), with forwarders and routes, always ensures that traffic gets routed through from one endpoint to another, no matter what type of lower layer OSI model communication media is applied. (Copper, Wireless, fibre, …).
The routing function in the network is provided by the router nodes in the network.
When dealing with non-IP communication links, such as that used for the VHF AIS/ASM, there is no routing function available. The requirement for communication is that endpoints are within VHF range. The VHF AIS/ASM is also a broadcast media. This means that all radios within range of the transmitter, will receive the communication. VHF AIS endpoints do not relay/transpond messages, and hence it is not directly possible to build a VHF AIS/ASM network/mesh of nodes like nodes in the MC where traffic/messages are routed. See chapter 8.8.2 for a more detailed discussion.

This means that for a client that wants to send/receive messages via VHF AIS/ASM, it cannot communicate with VHF AIS/ASM endpoints that are not in VHF Range.

This leads to the conclusion that clients that wants to send messages via VHF AIS/ASM do not need to see other endpoints than VHF AIS/ASM and are aware that this is a very different endpoint than an IP-based MC Service. If the Client wants to send a message to another vessel via the VHF AIS/ASM media, it cannot be guaranteed delivery.

The above leads to the idea to structure the on-board architecture, so that the RD does not need to roam anything other than IP-based traffic. This will help avoid the definition of the hybrid that is on the drawing board right now, lead to a simpler definition of endpoints and avoid the mixing of QoS from different OSI layers.

Figure 10 shows the first step in the idea. An AIS/ASM Gateway component is introduced. The Gateway is providing a HTTPS, SOAP based interface/service for clients on-board the vessel. The service offers means to transmit AIS/ASM messages as well as means for the client to listen to AIS/ASM messages. The client can setup the RD so that the communication with the AIS/ASM Gateway, gets the right QoS.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

The prioritisation/QoS of messages sent through the AIS/ASM Gateway are not the responsibility of the Roaming Component, but is managed by the AIS/ASM Gateway. This then leads to the fact that no matter what, the client both has to specify the QoS for the communication between Client and Gateway AND the QoS for traffic through the AIS/ASM Gateway.

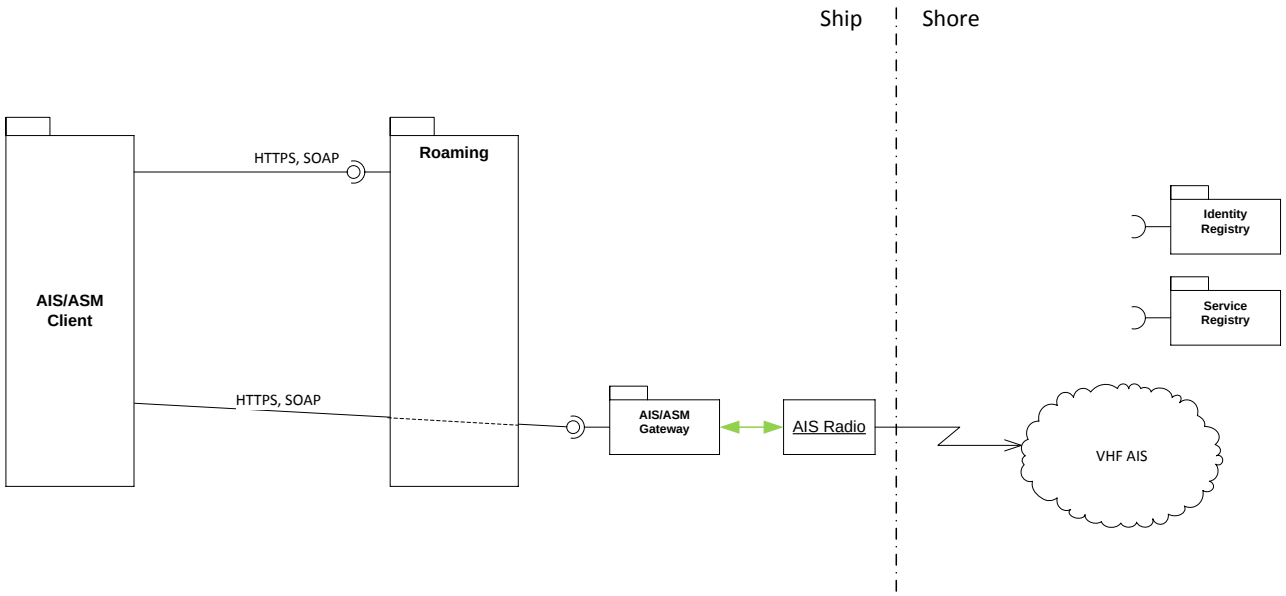

Figure 10 Client using an AIS/ASM Gateway

This also illustrates that the current specification of the RD is trying to integrate two different functions in a hybrid manner that leads to confusion.

Figure 10 also illustrates that the AIS/ASM Gateway, would then be a local service offered on-board the vessel, and hence it would make no sense that the shore-based IR and SR should have anything to do with the client's use of the AIS/ASM Gateway service. The immediate solution to that is the Almanac helper component (chapter 4.4.1), that can provide information on local vessel services.

Figure 11 summarises and includes local on-board non-IP Media Gateway Services in to the Architecture/Design. The hybrid clients shown are using the Almanac to search for services and then use shore-based MC services as well as local non-IP Gateway services. The figure also shows with blue dashed lines, what is being discussed right now in E2 as being the RD, where the red dashed line area could as well be a more logical and structured approach.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

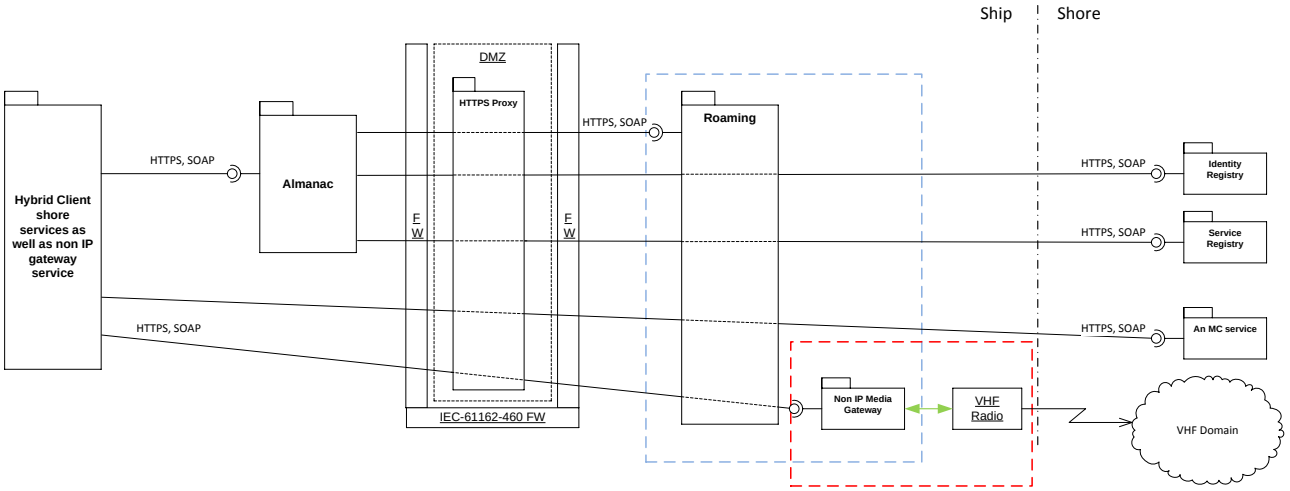

Figure 11 Architecture/Design including non IP Media Gateway

6.1 MMS Client Component using non IP Media Gateway

Most of the motivation for including the legacy non-IP domains is to support messaging as for example done with ASM. A client of the MMS system should see this service of the MC as being seamless of communication media. Building upon the architecture in Figure 11, the hybrid client could grow into the on-board MMS Client Component as discussed many times in E2. Figure 12 show how an MMS Client Component could encapsulate the IP and the non-IP domain messaging and create one seamless interface for an on-board Client that use MMS.
Note that MMS Client Component implementation might not make use of an Almanac, but use the shore-based IR and SR directly.

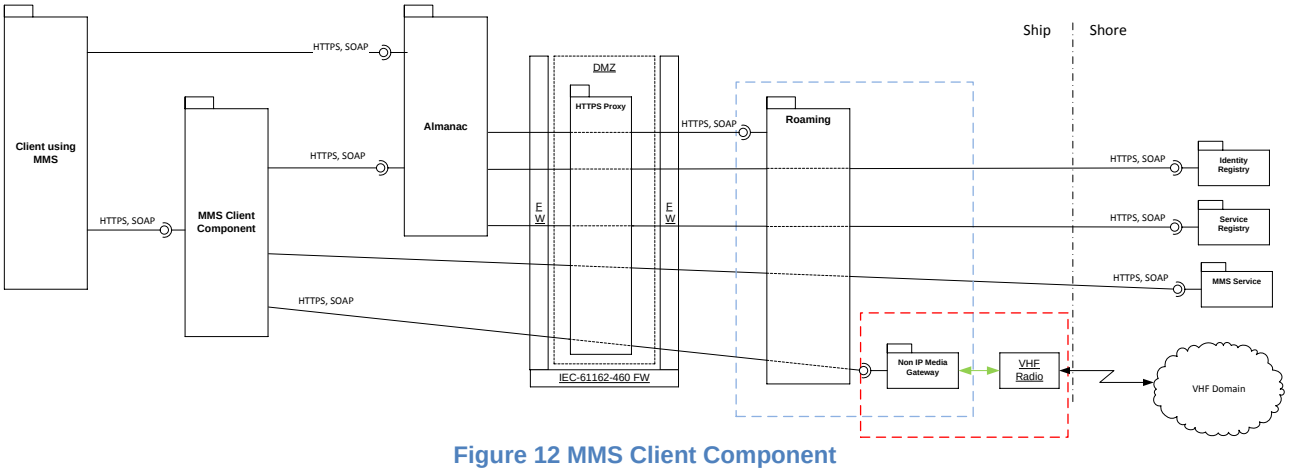

Figure 12 MMS Client Component

If we compare Figure 12 with the layered perspective developed by WP3 shown in Figure 13, it can be seen that they match very well, only with a few differences.

1. MMS communicates over Non-IP media through RD
2. Firewall/Gateway

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

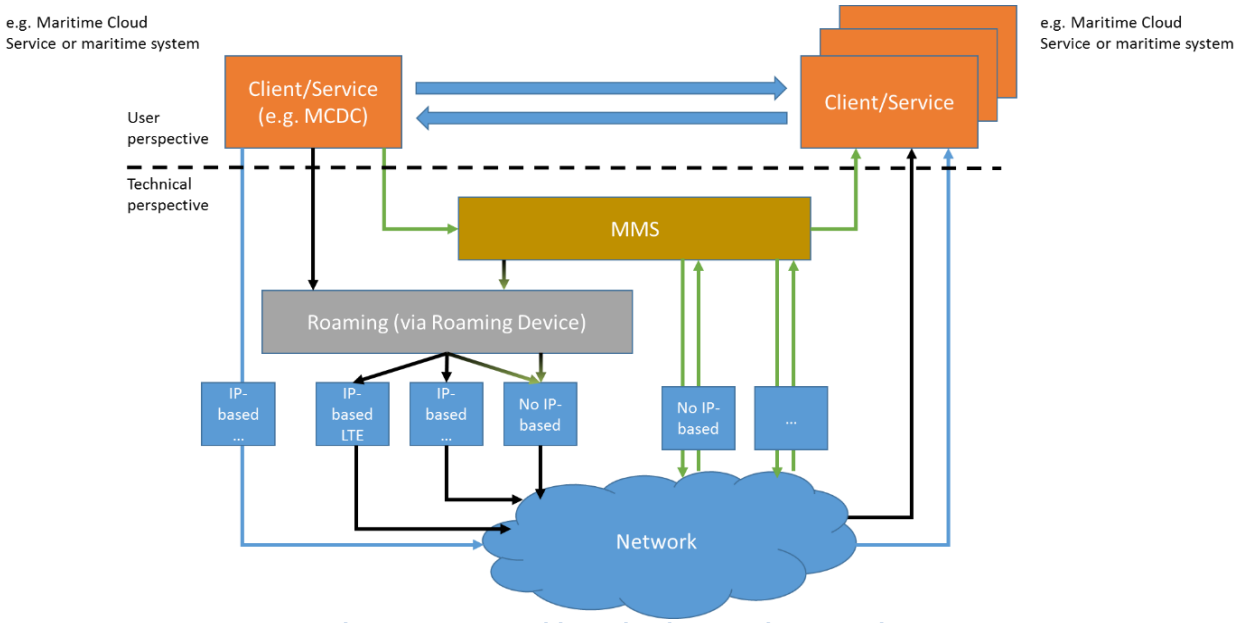

Figure 13 WP3 Maritime Cloud Layered perspective

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

7 Maritime Cloud Demonstrator Component

In previous E2 deliverables, such as (E2-T3.1-D3.2, 2015), a Maritime Cloud Client Component (MCC) has been defined. In (E2-T3.3-D3.7, 2016), this component is being further defined and renamed to Maritime Cloud Demonstrator Component.

Quote: “The Maritime Cloud Demonstrator Component serves as a reference implementation on how to use the other Maritime Cloud core components and can further be used by application developer (for example provider of ship equipment) to ease the usage of MC functionality. For this purpose the MCDC realizes some convenience functions, and takes the RD into account, to ensure a maximum of connectivity. “

There are several purposes to have the MCDC as an architectural element. One is to have a reference implementation of a MC client as a deliverable in E2. Another reason is that the MCDC in an on-board architecture may ease the implementation of MC clients by having the MCDC implementing components/functionality that can be reused amongst clients. The (E2-T3.1-D3.2, 2015) lists two of the obvious areas:

- Secure authentication, signing and encryption support through online use of the Maritime IR or means to provide the same services offline.
- Service discovery through online use of the Maritime SR or means to provide the same offline.

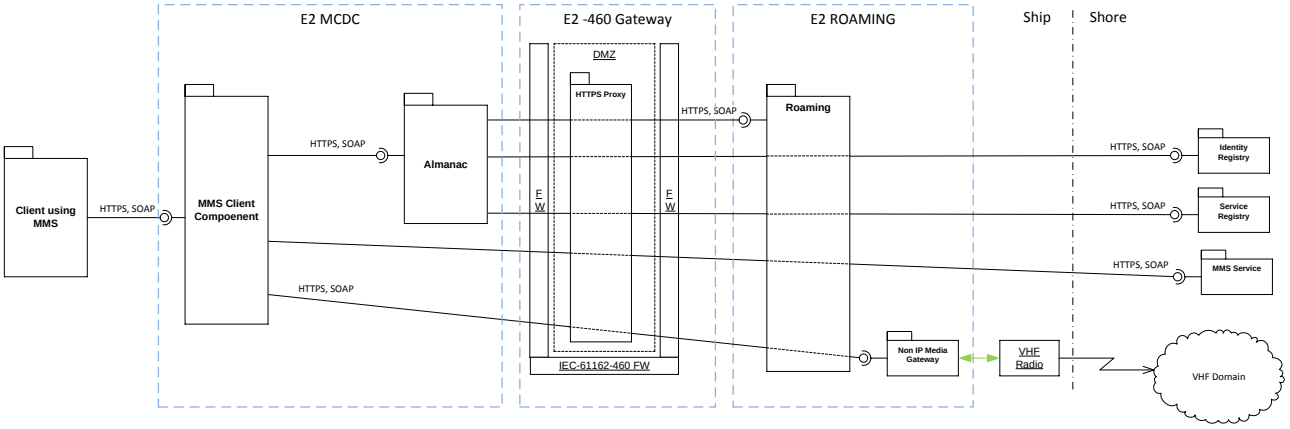

Figure 14 EfficienSea2 Entities

In Figure 14, the blue dashed boxes identify proposed entities for use in EfficienSea2. Note that the MCDC by this is the collection of helper components identified in previous chapters.

“This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 636329”.

8 Efficient Protocols vessel/shore

This chapter discusses some basic properties the internet and of relevant protocols in relation to vessel/shore communication.

All internet communication is based on (RFC1122, 1989). There is a desire that the services offered as part of the MC is internet based. Therefore the discussed protocols are from that domain.

8.1 TCP and FTP over high latency, low bandwidth communication channels.

The Transport Connection Protocol is the most widely used transport protocol on the internet. It forms the basis for application protocols, such as HTTP, FTP and TCP is accompanied by the Transport Layer Security Protocol (former “Secure Socket Layer” SSL).

When using TCP over SATCOM communication channels some problems arise due to the higher latency and higher error rate compared to high data rate land connections.

Many works and even modification of TCP have been suggested to solve these problems. Two works are referenced here: (Katz, 1999) “TCP Performance over Satellite Channels” and (Latour, 2000) “Enhancing TCP Performance over Satellite Channels”.

Both works conclude with recommendations on TCP configuration parameters as well as introduction of TCP spoofing methods.

When using FTP for transporting larger files over communication channels with high latency and even have dropouts (packet loss), transport may be disconnected from time to time. It is recommended to utilize the ability to “resume” a file transfer in the FTP protocol, to avoid losing data already transferred.

8.2 TLS over high latency, low bandwidth communication channels (hereunder HTTPS).

Since TLS is an “extension” of TCP, the considerations stated in chapter 8.1 are also valid. It is much more bandwidth consuming to establish a TLS connection than a plain TCP connection. The overhead depends highly on the PKI methods used for the particular TLS session. In many applications it should be considered to keep a TLS session open for longer periods where there is no data transferred between the client and service, since it may require less bandwidth to keep the session open than to tear it down and reopen later.

“This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 636329”.

8.3 Virtual Private Networks (VPN)

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network.

A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption.

VPN systems may be classified by:

- The protocols used to tunnel the traffic
- The tunnel's termination point location
- The type of topology of connections, such as site-to-site or network-to-network
- The levels of security provided
- The OSI layer they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity
- The number of simultaneous connections

There exist many variants of VPN on both the Layer2 and Layer3 types.

Many router manufacturers, including Asus, Cisco, Draytek, Linksys, Netgear, and Yamaha, supply routers with built-in VPN clients. Some use open-source firmware such as DD-WRT, OpenWRT and Tomato, in order to support additional protocols such as OpenVPN.

OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls. It was written by James Yonan and is published under the GNU General Public License (GPL).

8.4 UDP over high latency, low bandwidth communication channels.

Universal Datagram Protocol (UDP) can be used to transfer single datagram messages to/from shore. The protocol only guarantees that content in a single datagram is intact. The benefit of UDP is that it has a smaller overhead.

UDP is used heavily in the IEC61162-450 based navigation/vessel network to propagate NMEA sentence, automation system data as well as RADAR and ECDIS imaging.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

UDP may be used for streaming applications where data loss is acceptable.
UDP has many benefits in a multiple talker and multiple listener architecture.

Usage of UDP over high latency, low bandwidth communication channels may be considered for very particular applications such live data streaming in special situations.

UDP might also very well be considered in the design of MMS communication over non-IP VDES links, since it have demonstrated single message broad- and multicasting so well on vessel networks.

8.5 Privacy vs. compression

To obtain privacy, the data to be transferred must be encrypted. To minimize bandwidth usage, the data must be compressed.
Encryption turns data into high-entropy data, usually indistinguishable from a random stream. Compression relies on patterns in order to gain any size reduction. Since encryption destroys such patterns, the compression algorithm would be unable to give much (if any) reduction in size if it is applied to encrypted data.
In other words, for any type of compression protocol known today, the efficiency is lowered very significantly if the data is encrypted before the compression. This is due to the nature of encryption, that is practically outputting a scrambled data stream with no data segment repetitions, a property that makes compression inefficient.
Therefore to be able to transfer data efficiently, the compression must be done before data is encrypted.
To obtain complete end-to-end privacy and avoid man in the middle attacks, the encryption must be done at source client and decryption at destination client. To obtain low bandwidth usage, this then requires that compression and de-compression are also done at the source and destination clients respectively.
TLS standard (RFC5246, 2008) includes methods that support compression before encryption, see (RFC3749, 2004).

8.6 Vessel Public or Local IP Address and IP v4 vs. IP v6

The current infrastructure of various communication providers such as SATCOM, WLAN and 3,4G providers varies. Since the aim of the T2.3 RD is to provide seamless connection from Vessel to Internet, the roaming between the different providers, needs to take into account the fact that the vessel communication entry/exit node may be assigned different IP addresses dynamically.
If no action is taken, an established transport session from the vessel to shore cannot be kept alive if the RD changes to a media where the vessel node gets a different IP address than the one used when the transport session was established.

It is not possible to assign one static public IP address that works across the suite of media in discussion here.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

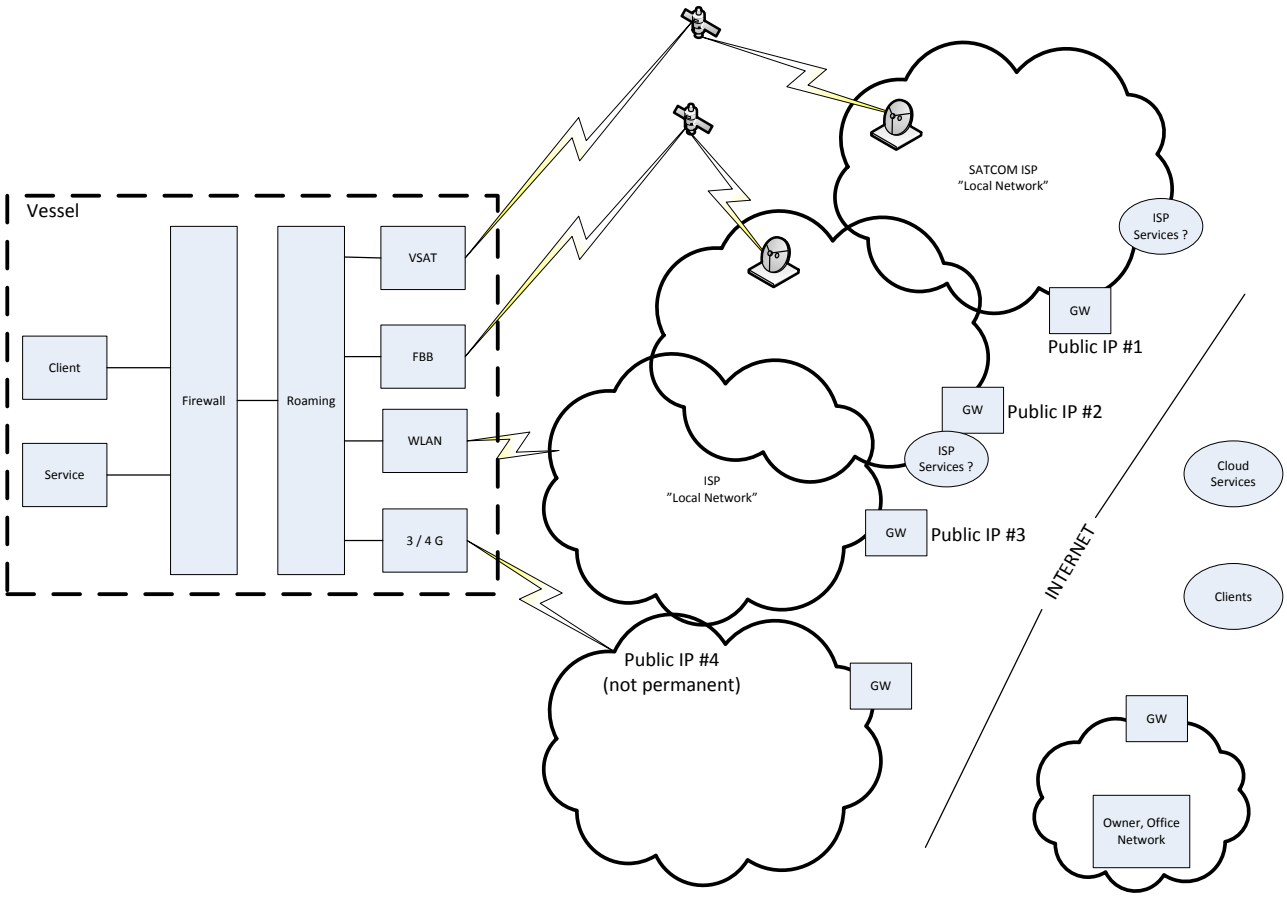

Figure 15 Roaming and IP Address scenarios

8.7 IP v4 vs. IP v6

The amount of available IPv4 addresses is rapidly getting smaller and everything internet is in the process of migrating to IPv6
It is yet to be investigated if IP v6 addressing is possible in relation to SATCOM.

8.8 IP Traffic over VDES

VDES offers a low bandwidth data communication channel between VDES nodes within VHF range. From VDES draft standard, the estimated bandwidth is 150kbps shared between vessels within the VHF region.

The main envisioned goals of VDES is:

- To protect the AIS basic function of ship to ship collision avoidance
- To enhance maritime communication applications, based on robust and efficient digital transmission at a much higher rate than the current AIS

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

The wish list of applications of VDES is:

- SAR Communications
- Marine Safety Information and Notice to Mariners
- Automated Reporting
- VTS Service Portfolio
- Updated charts and publications
- Ship Reporting
- Route Exchange Ship to Ship
- Logistic services

Since VDES is packet based, it is possible transmit/receive IP data packets over VDES. This leads to a wish to base all of the applications of VDES on IP, since IP based communication is the most widely used and probably easiest to implement.
It is of course not at this point clear how exactly the applications envisioned is going to look like, and what communication needs they have.
For several applications, like e.g. Updated charts and publications it is clear that some form of transport layer protocol is needed, since information size is much higher than packet size, and there is a need to ensure data integrity.

Common sense say that establishment of many robust TCP connections over VDES is not possible with the bandwidth available.
This then rules out a use case that many ships all contacting a chart update service using standard web service methods.
In a “vacated” area with very few vessels, the situation is quite different. TCP connections over VDES might become very handy indeed.

8.8.1 IP Addresses and VDES

A basic requirement for nodes in an IP network to communicate with each other is that they have a unique IP address. Since VDES stations will appear as nodes in a public VHF VDES space, each of the VDES stations would be required to have a static public IP address, unless special techniques, such as implementing zeroconf in the VDES nodes was applied. (Note: zeroconf is a protocol suite to handle assignment of unique ip addresses and hostnames in a local area network domain).
Since the vessel and its VDES node is mobile and can move from being in just the local domain in the VHF VDES range to also be in the public internet domain, zeroconf alone would not be sufficient.

As described in 8.6 it is not possible to apply one single static public IP address across multiple internet providers, however it is possible that the vessel would apply one static public IP address to use for the VDES node AND the on-shore vessel connector.

“This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 636329”.

8.8.2 Routing of IP traffic between VDES nodes

Communication over VDES links are limited, not only by bandwidth, but also the VHF range.

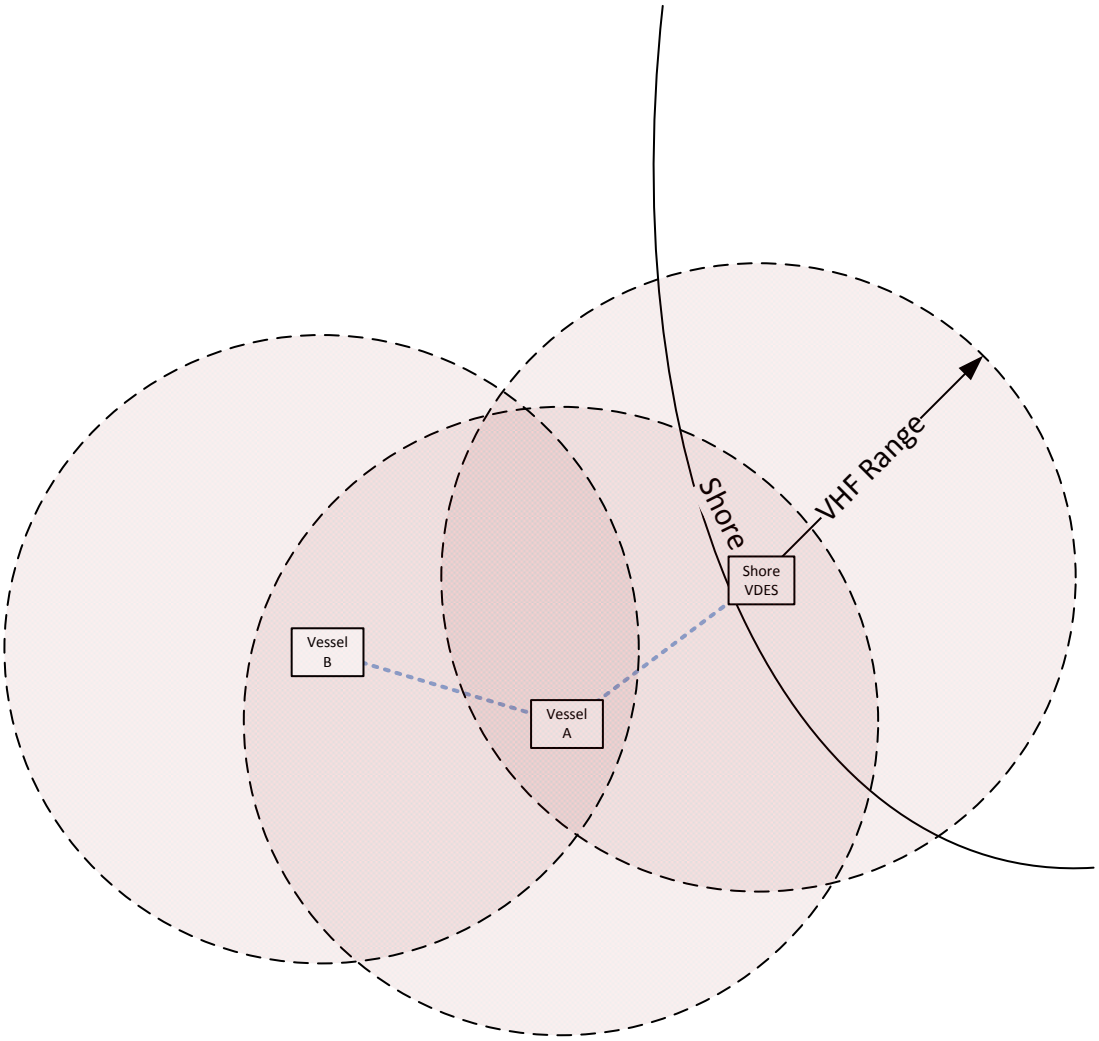

Figure 16 VDES Range limitations

Figure 16 VDES Range limitations Illustrate a situation where a Vessel A is in VHF range with a shore VDES station and a Vessel B that is not in range of the shore VDES station. Vessel B are in range of the Vessel A station. In this situation, it would be beneficial if Vessel A were able to route the communication to/from Vessel B to/from the shore VDES station.

The most intuitive approach would be to use the properties of the IP network layer and the same methods as is being used on the internet for routing of traffic. The protocols used on the internet for routers to exchange information on how to route traffic, can be quite demanding with respect to bandwidth and is probably not applicable for VDES. It is worth

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

mentioning that alternative and less bandwidth demanding routing methods such as source routing exists.

A second approach would be to apply methods similar to the GSM roaming technologies, since the vessels are mobile and normal IP network layer routing methods are heavily challenged.

A third and probably the right approach are to realize that the routing problem is a “mesh network” routing problem. This problem has been research heavily in the last decade or two and there are many competing schemes at this time of writing.

An approach that seem to be what is being discussed in the MC forums are the MMS and as understood at this point in time, is an application layer messaging service. It is important at this point to be very clear and distinguish between application layer messaging and network layer messaging.

For a MMS service to be able to route messages between MMS nodes, each node would need to contain a routing component and will face the same problems to solve as with mesh network routing.

“This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 636329”.

9 Deployment considerations and Architecture Update

This chapter reviews the on-board network architecture as described in (E2-T2.4-D2.10, 2016) and discusses considerations on deployment.

The logical architecture/design developed in the previous chapters, does not require the existence of either the MCDC (helper components), or the RD.
Nor does it put restrictions on the number of instances of MCDC and 460 gateways. This is considered an advantage of the architecture/design, since it allows multiple vendors to build integrated systems with propriety implementations of MCDC and -460 Gateway functionality.

Further, the logical architecture/design allows multiple RD instances, each tailored for specific needs. One could imagine a RD specifically allocated for Navigation-related communication and one allocated for engine systems communication.

An example deployment with two separate Vessel Systems (with separate security zones) are shown in Figure 17

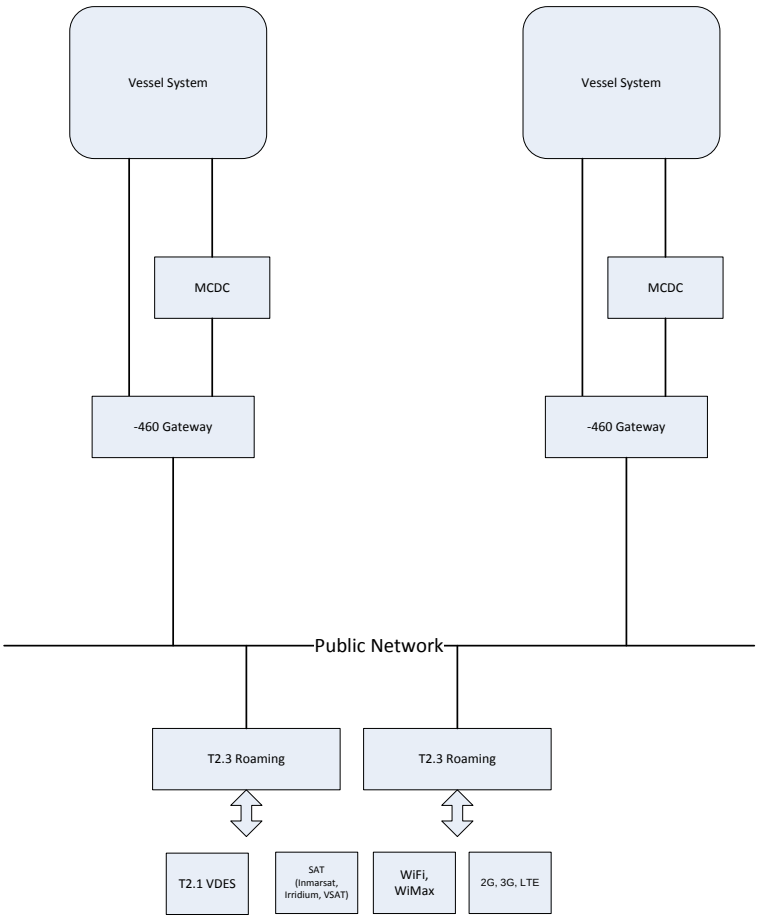

Figure 17 Example Network Architecture

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

10 Proposed Demonstrator

The M36 deliverable for T2.4 is an Implementation of a prototype which demonstrates vessel-to-shore communication for at least two different types of equipment using the Protocols defined in D2.4.2
Figure 18 provides an overview of the initial demonstration setup.
To enable simulation of communication through links with a variety of QoS, a WAN Emulator is applied. This component must be able to introduce relevant latencies and drop-outs with statistic variance that matches a true environment.
It is the intension that this initial setup is active from beginning of year 3 of the EfficienSea2 project and then evolves as components and services become ready.

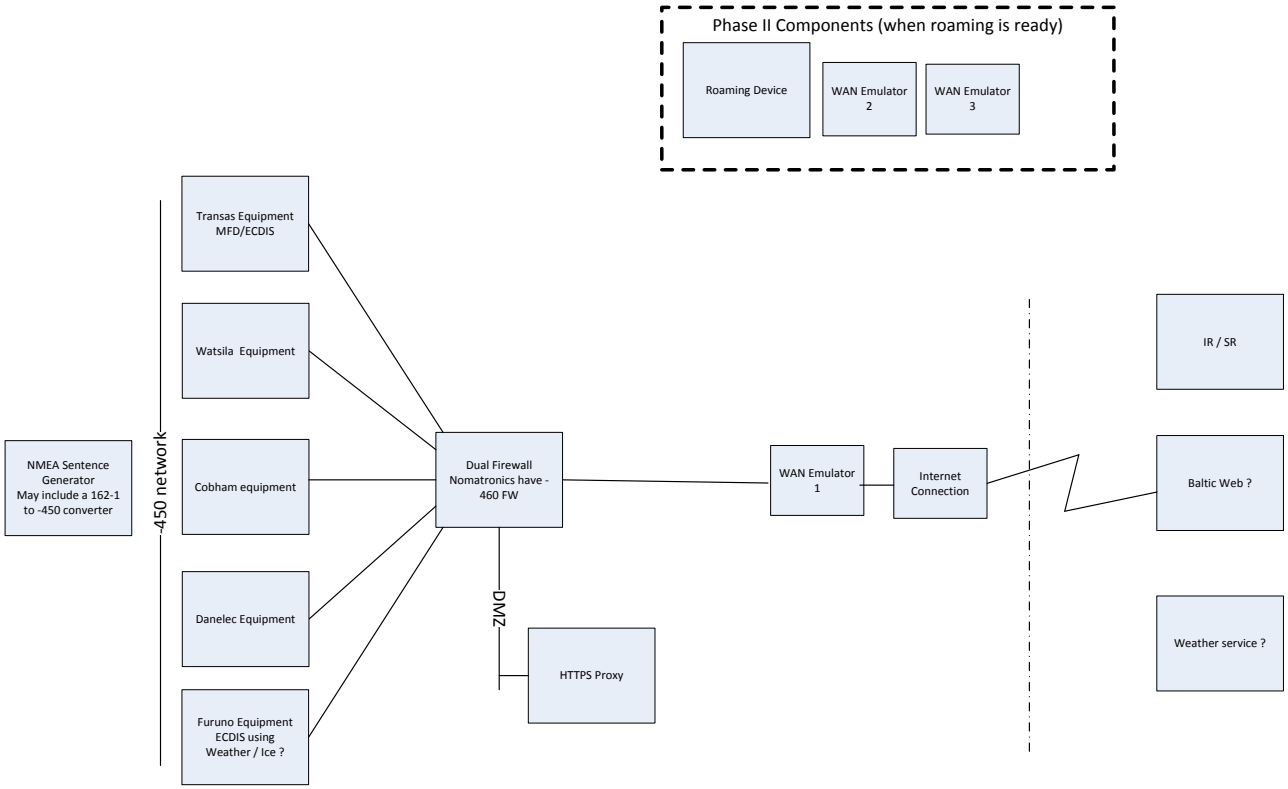

Figure 18 Initial Demonstrator Setup

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

11 Identification of potential Areas for standardization

There are several areas of the on-board architecture and protocols from vessel to shore as well as example services that can be topics for standardisation:

3. On-board architecture
4. Large Data Transport Service
5. Non IP Media Gateway
6. For AIS/ASM messaging
7. For MMS
8. Standardized method for reaching on-board service from Shore
9. The Vessel Connector Component
10. On-board MMS component
11. RD/Component

These areas will be discussed further during year 3 of the EfficienSea2 project and it has been agreed in WP2 to produce a final report on standardisation areas by M36.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

12 Conclusion

The D2.11 has developed an on-board logical architecture/design as set out in the scope of work for T2.4 for this deliverable. Various use-case scenarios have been discussed and have shown that the developed logical architecture is valid.
Requirements for efficient communication protocols between clients and services of the MC have been developed.
D2.11 does not describe detailed requirements for the interface to RD, but only demand that the interface must be HTTPS/SOAP based.

The T2.4 D2.10 recommended on-board network architecture has been reviewed and updated.
With latest information of the Korean SMART project definition of the application layer messaging service MMS, the architecture/design has been validated to be able to integrate the necessary components needed for implementation.

It is believed that the design is ready to be tested in demonstration as described in chapter 10.

An added deliverable for the work of T2.4 in the E2 project is a report identifying and describing areas for standardisation that will aid the recommended design to be realized in actual solution implementations.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

Bibliography

E2-T2.3-D2.8. 2016. *D2.8 Interface to Maritime Cloud.* s.l. : EfficienSea2, 2016.

E2-T2.4-D2.10. 2016. *D2.10 Recommended On-board Network Architecgture.* s.l. : EfficienSea2, 2016.

E2-T3.1-D3.2. 2015. *D3.2 Conceptual Model.* s.l. : EfficienSea2, 2015.

E2-T3.3-D3.7. 2016. *D3.7 Technical Specification.* s.l. : EfficienSea2, 2016.

—. 2016. *Technical Specification of the Maritime Cloud.* s.l. : EfficienSea2, 2016.

E2-T5.1-D5.3. 2016. *Development of a new common port database concept and structure.* s.l. : EfficienSea2, 2016.

Fabio Renda, CIMNE. 2016. *SeaSWIM Connector Service.* s.l. : STM, 2016.

Katz, Thomas R. Henderson and Randy H. 1999. *TCP Performance over Satellite Channels.* Berkeley : EECS, University of Calilfornia, 1999. 94720.

Latour, Maik Kammermann and Capt Hugues. 2000. *Enhancing TCP Performance Over Satellite Channels.* Ottawa : Defence Research Establishement Ottawa, 2000. DREO TR 2000-079.

RFC1122. 1989. *Requirements for Internet Hosts -- Communication Layers.* s.l. : IETF, 1989.

RFC3749. 2004. *Transport Layer Security Protocol Compression Methods.* s.l. : IETF, 2004.

RFC5246. 2008. *The Transport Layer Security (TLS) Protocol v1.2.* s.l. : IETF, 2008.

STM Communications, STM Validation. 2017. Sea Traffic Management. *http://stmvalidation.eu/.* [Online] 14 02 2017. [Cited: 14 02 2017.] http://stmvalidation.eu/.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

13 Appendix A –Review Report

This chapter contains review comments and actions from the 75% and 100% review.

N°	Reviewer Initials	Reference in document (General or Paragraph, Figure …)	Type (editorial, structural, formulation, error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
1	AW	General		Received a fully spell and formulation corrected version of the document from Andy that made the whole thing more readable and in English as it was supposed to.	All the following corrections is based on andy's version ☺ The corrections might very well introduce new spelling and formulation errors...
2	ESP	P10 , presence of roaming device		Perhaps you could elaborate a bit on this, maybe line 'It should be pointed out that a roaming device is not an essential part of maritime cloud communications, indeed, it does not have to be present at all. The purpose of a roaming device is to reduce/optimize bandwidth requirements in balance with communications cost, and while a maritime cloud solution undoubtedly would benefit from this enhancement, it is exactly what it is: an enhancement, not a basic requirement without which the maritime cloud communications cannot work.'	Suggestion included on P10.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Reviewer Initials	Reference in document (General or Paragraph, Figure …)	Type (editorial, structural, formulation, error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
3	ESP	P10 para 4		Very important – suggest some expansion here.	Little expansion added
4	ESP	5.4.2 para 1		I can agree to this chapter when it comes to special purposes like remote maintenance etc., but I'm not immediately charmed by the lack of symmetry between ship and shore when it comes to provide generic services (which is the point of the maritime cloud; the VPN solution being discussed here is essentially cloud-irrelevant?). The point is this: If the ship is offering a Maritime Cloud-like service, I cannot see why it cannot be implemented exactly like the ones ashore? (i.e. a Cloud, which could reside on the -460 FW DMZ?). In this world of abstraction, I believe it would be much preferable to use and reuse the same mechanisms for similar services. Take, for instance, providing instant weather information like wind, air pressure etc. If a particular ship would like this information, it could be available from a (number of) shore station(s), but ships could basically offer the same kind of service. Would it then not be reasonable to use the same access mechanism?	We discussed this at the warsaw meeting and came to an understanding that the proposal in the 5.4.2 chapter was to show an example implementation method that achieves a "symmetry". Action taken in this revision of document is to clarify that.
5	ESP	P16 para 4		Hm, it seems to be a 'doubtful' ☺ circumvention of the intention of the standard, if the 'Onboard service reachable from shore' sits on the same network as the 'Client'?	The method described is very often used in shore based VPN applications where it has an accepted cyber security risk level. It is most likely the method used by our own corporations to provide us with access to our company networks when we travel. Seen in the light of earlier comments

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Reviewer Initials	Reference in document (General or Paragraph, Figure …)	Type (editorial, structural, formulation, error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
					with requirements for symmetry, the text is left as is.
6	ESP	5.4.2.1 para 6		Quite, but for me, at least, it is an open question whether this function is really part of the maritime cloud? If not, then we should not make choices on the possible soluitons?	Changed according to our discussions in Warsaw. The chapter is now there to provide an example of how one could achieve symmetry with VPN.
7	ESP	5.4.3.1 para 1		Please elaborate?	Text expanded to be more explanatory.
8	ESP	5.4.3.1 last para on encryption		This must be implementation-specific? While I agree that encryption is prudent, is it a hard requirement coming from E2 and the work performed here?	In our D2.10 section of cyber security considerations, we made a requirement that it must be possible to implement the needed cyber security risk mitigations to reach an appropriate risk level. To me, this means that it must be possible to apply encryption if that is needed.
9	ESP	5.4.3.1		Is this section describing existing solutions? Is that part of the scope? Or should we rather discuss and describe what a generic data mirror service should look like, where it should sit etc.?	This section was intended to describe the existing methods used for transporting large amounts of data today. . I have tried to make this more more clear in the introduction of the 5.4.3 chapter. On method: It is important that we relate to the real world before we suggest standards
10	ESP	5.4.3.2 and 5.4.4		In repetition of the above, to a large extent, we should discuss the (reasonable) requirements to an onboard FTP site, and describe a neutral solution that in our view fulfills the objectives? I'm happy with establishing a set of pre-cooked	The goal of chapter 5.4.4 is to demonstrate that the architecture/design support that it is possible to design services for large data transfer. In this demonstration we need to regard the requirements

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Reviewer Initials	Reference in document (General or Paragraph, Figure …)	Type (editorial, structural, formulation, error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
				solutions for common services, but I suspect we should depart in a number of (artificial) use-cases, since the task that should provide the requirements (WP1.something?) didn't really made us that much more wiser?	we developed in D2.10 on e.g. cyber security. Therefore the cyber security considerations in chapter 5.4.3.2 Some reformulation has been done in text.
	ESP	5.4.5 page 23 on the 10min value		Where does this number come from?	Chapter completely changed. It is not in scope for T2.4 to define this type of communication as per. Discussions with WP5
11	ESP	Figure 12		I would like to extend this line of thinking to 'reduce' the VHF domain to 'just another kind of transport mechanism' – meaning that the endpoint becomes the same service that is/may be reached directly via IP based traffic. In other words, it seems to be the logic of things that as long as there is VHF connectivity to the cloud (global or indeed local on another ship), nothing is basically different?	I would like that also, but I think that the capabilities of the upcoming VDES has been hyped beyond what it can offer. It is a natural thing that happens when visionaries grow "simple" services over VDES into general web services over VDES. The limitations when not using standard internet protocols and their offerings of transport mechanisms, roaming, cyber security, data integrity etc.. are forgotten. The fact is that VDES will not be able to offer these basic things. This said, lets hear what they have found in the SMART project with MMS. We might be surprised.
12	ESP	8.3		Are there plans to discuss/add information about point-to-point, multicast, broadcast?	Did not plan to elaborate further. We decided to leave the details of potential MMS implementations out of scope, but I think that UDP might

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Reviewer Initials	Reference in document (General or Paragraph, Figure …)	Type (editorial, structural, formulation, error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
					become handy for the designers there. I added smaller comment on that in text.
13	AH	General		I would mark the Almanak as "optional" and	Almanac is described as optional, but not clearly enough obviously. Will make a better attempt. (Btw. roaming is optional and MMS is optional). The only mandatory for Client/Service to be using MC is their use of IR and SR
14	AH	General		perhaps bring up the figure we designed together in Hamburg about the MMS.	Included the drawing from WP3, but still want to recommend the use of Non IP Media gateways as proposed in D2.11 when communicating through Non IP. This will allow a pure IP based communication in the implementation of MMS (and roaming) and it will also enable standardization of the interfaces (APIs).
15	TK	5.4.2.		- What is the connection between the VPN client and the MC? Or is there any? Who manages the VPN? Service provider or ship owner?	As per ESP comments, and as agreed in Warsaw, it is made clear that the VPN is one method/trick to make vessel services seem as if on shore.. creating symmetry. The shore based client that access the on-board vessel service are imagined to discover the on-board service using the Service Registry.

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Reviewer Initials	Reference in document (General or Paragraph, Figure …)	Type (editorial, structural, formulation, error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
					Have added that to text
16	TK	5.4.3 & 5.4.4.		- The purpose should be clarified. Is the data transport between the ship and MC services?	Tried to clarify in text. The data transport is between a client and a MC service. If so happens that the two are separated because one is on vessel, and low bandwidth communication is the only
17	TK	8		- The transport protocols are now discussed separately from chapters 5.4.2-5. There should be some connection between these.	The chapter is refreshing general knowledge on transport protocols and forms some basis the other writing in the document. Tried to move chapter to start of doc, but it worked badly. Inserted some references to the chapter relevant places throughout the 5.4 chapter.
18	AW			Minor item: acronyms are: DOS, LOS but QoS (small o)	DOS and LOS was actually not used in doc, so removed from list
19	AW	Page 9,10,13,17,17,20		There is some inconsistency throughout the document with respect to using the acronyms in the Glossary; or spelling out in full; or spelling in full and following with acronym in ( ). As an example under 4 Scope: the text uses the acronyms E2, MC, VDES but also spells out some other items which are in the Glossary, such as Maritime Cloud Demonstration Project,.Maritime Messaging Service (MMS), EfficienSea2 Project, Identity and Service Registry…. Letter missing in para 5 (so) and in paras 5.1	Fixed as much as possible

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".

N°	Reviewer Initials	Reference in document (General or Paragraph, Figure …)	Type (editorial, structural, formulation, error)	Reviewer's Comments, Question and Proposals	Editor's action on review comment.
				and 5.2 further examples of inconsistency (Identity Register, Quality of Service…)	
20	AW	Page 22		..dependent on …(not of)	fixed
21	AW	Page 23		Inconsistencies.. There has been… (not…. have been – twice on page)	fixed
22	AW	Chapter 9		This chapter discusses some basic properties of the internet…..	fixed

"This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 636329".