Deliverable 3.1
Analysis Report

Maritime communication and infrastructure

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

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

Deliverable number 3.1

Analysis Report
Maritime communication and infrastructure

Due date of deliverable:	1 November 2015
Actual submission date:	30 October 2015
Organisation in charge of deliverable:	Danish Maritime Authority (DMA)

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

DOCUMENT STATUS

Authors

Name	Organisation
Jens K. Jensen	Danish Maritime Authority
Peter Pedersen	Gatehouse

Document History

Version	Date	Initials	Description
0.1	2015-10-12	JKJ	Draft requirements collected from use cases
0.2	2015-10-13	JKJ	'Lessons learned' section added to document
0.3	2015-10-14	JKJ	HLUG comments summary added
0.4	2015-10-19	JKJ	Gatehouse 'lessons learned' incorporated. Document sent for review
1.0	2015-10-29	JKJ	Restructured to address review comments
1.1	2015-10-30	CS	Corrected typos, fine-tuned layout and updated to the new EfficienSea 2 template adhering to the ISO 2145 standard

Review

Name	Organisation
Kaisu Heikonen	Finnish Transport Agency
Erik Styhr Petersen	Lyngsø Marine A/S
Bjørn Borbye Petersen	Danish Maritime Authority
Christoph Rihacek	Frequentis

Approval

Name	Organisation
Christopher Saarnak	DMA

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

Contents

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

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

1 Executive summary

This report describes needs related to infrastructure functions related to the ‘Maritime Cloud’ to support effective digital interactions in the Maritime Domain. The source of the needs identified are use cases collected within the project as well as external projects.

The needs collected primarily point towards strengthening the capability to

- Uniquely identify and validate the identity of entities that need to interact
- The ability to ensure integrity and in some cases confidentiality related to information transfer
- Define standardized information services, and provide mechanisms to discover the availability of such services
- Support seamless roaming – automatic transport of information regardless not dependent on single communication links or communication service providers
- Address cyber security

It has not been possible to conclude a definitive set of requirements for the development of the Maritime Cloud, but the needs collected should be prioritized and further qualified within the project, to define the conceptual model for the Maritime Cloud and creating a technical specification.

Part of this process will be to determine which functions are within scope of this project, and which functions to be considered outside the scope.

Further, the collected information indicates a need for identifying a possible business case for establishing and operating the Maritime Cloud. A roadmap for its evolution is requested.

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

2 Introduction

The ‘EfficienSea 2’ project aims ambitiously – and in collaboration with other initiatives - to establish sustainable infrastructures for evolving, demonstrating, validating and promoting interoperable maritime digital information services. The final goal is to facilitate an evolution of the maritime transport chain towards even higher standards of safety at sea, security and also efficiency.

The aim of this report is to identify needs and requirements related to the first objective of the EfficienSea 2 project: “Create and implement a ground-breaking communication framework – the ‘Maritime Cloud’ that will enhance information sharing in and around the maritime sector for smarter traffic management, facilitating a comprehensive e-maritime and e-navigation environment, enabling the maritime internet of things.”

The report describes and summarizes needs that relate to infrastructure and communication, which can be derived from ongoing development of related maritime information services.

The contents of this report are based on:

- Deliberations on the MSPs (Maritime Service Portfolios) listed in the IMO e-navigation Strategy Implementation Plan [IMO SIP]

- Needs derived from initial draft designs of information services under development in the EfficienSea 2 project, as well as related previous projects:
  - MarNIS
  - Flagship
  - EfficienSea
  - MonaLisa
  - ACCEAS
  - MonaLisa 2.0

- Lessons learned from other domains, facing similar challenges of achieving interoperability between various systems distributed amongst many actors

2.1 Consensus

A primary goal of this report was to gather requirements that describe an infrastructural setup, that will facilitate transition towards harmonized service development within the scope of the Maritime Domain, and be practically usable and acceptable to a large part of the stakeholders on a worldwide basis. However during the writing of the report, it has been realized that the material gathered does not qualify to conclude a comprehensive description of prioritized requirements for the ‘Maritime Cloud’. Instead, a set of common needs have

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

been identified, which will need further analysis in order to break down hard requirements, and a process for prioritization during the conceptual modelling and technical specification phase of the project, to achieve consensus on priority and scoping of what can be achieved within the lifetime of the EfficienSea 2 project. Hence, this report will only recommend priorities based on a subjective evaluation of the material gathered, rather than conclude normative requirements.

2.2 Definition of terms

In order to classify the priority of needs/requirements identified that relate to a maritime digital infrastructure, through study of various use cases, the terminology from ISO/IEC Directives Part 2:2011 has been adopted:

- Requirements are expressed by "… shall…";
- Recommendations are expressed by "…should…";
- Permitted or allowed items are expressed by "…may…";
- Possibility or capability to carry out an action is expressed by " … can …".

2.3 Scoping of the Maritime Domain

In defining the scoping of infrastructure functions needed to support the maritime domain, the scoping of domain boundaries have been proposed as follows:

At Sea

The prime focus is merchant shipping, carrying goods and/or passengers. Also included are fisheries and Off Shore activities, leisure boating activity, and other floating or fixed activities on the surface of the water, including aircraft operations related to maritime Search And Rescue (SAR) or boarding / disembarking of pilots. Deep Sea, coastal as well as inland waterways are considered inside scope.

Military and submarine activities are recommended to be considered outside scope.

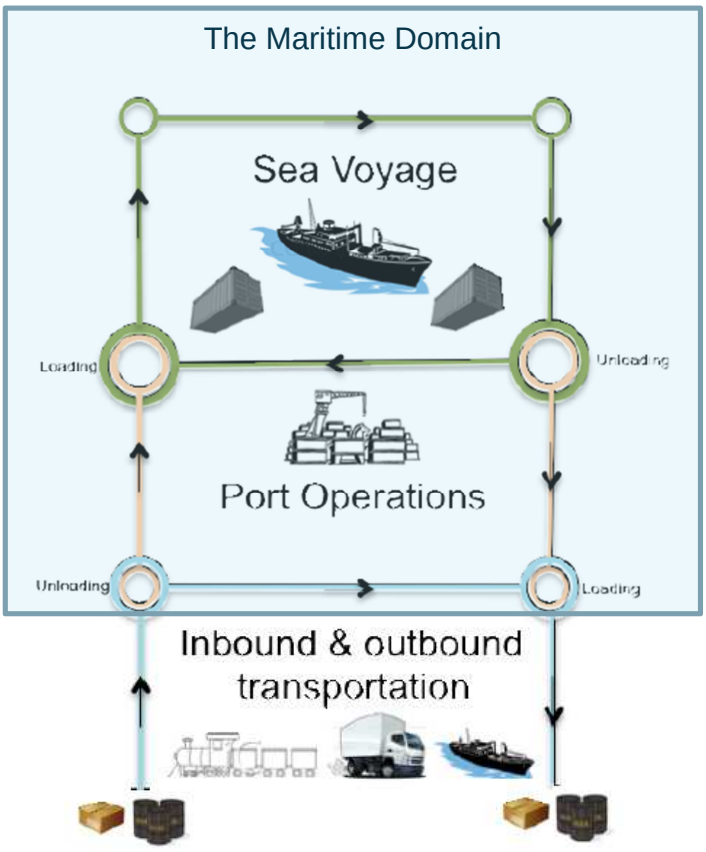

Figure 1 The Maritime Domain

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

Port operations, ‘links’

Operations related to arrival/departure from port, loading/unloading, waste management, etc., as well as physical communication & monitoring stations and other systems or activities that link the Ship and Shore side activities are considered inside scope of the maritime domain.

On Shore

Activities on shore, that relate directly to maritime operations, such as VTS (Vessel Traffic Service), MRCC (Maritime Rescue Coordination Centre), Pilot booking office, Hydrographic office, Maritime and Aids to Navigation Authorities, Back end network nodes of communication or monitoring networks, Monitoring operations related to maritime traffic, Cargo management, Locks & bridges operations, Ships agents, etc. are considered on shore actors inside the Maritime Domain. Also the interfaces to inbound & outbound logistics (hinterland logistics) as well as national single windows for reporting, customs, immigration authorities etc. are considered inside scope, while the full extent of systems and responsibilities of activities that do not specifically relate to maritime transport or offshore operations, are not considered within scope of the Maritime Domain.

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

3 Needs derived from recent projects

This section describes requirements that have been derived from interviews or official outputs of previous projects, either related to the EU e-maritime initiative, the IMO e-navigation strategy or maritime communication.

3.1 MARNIS – Maritime Navigation and Information Services

A project (2004-2008) supported by the European Commission through the 6th RTD Framework programme.

This project described a Maritime Information Management (MIM) concept, intended to prevent frequent reporting of the same information, through reporting once to a National Single Window and distribution through the SafeSeaNet in a European e-maritime context.

The Final report of the project can be found at ref. [MarNIS_final_report]

Another report, [MarNIS D2.2.C-1] describes requirements for maritime broadband communication and mandatory communication capabilities. The report concludes:

"Passenger ships will probably have passenger demand, revenue generating services and possibly safety as driving forces for even higher bandwidth requirements; Cargo ships will most likely have efficient operation and legislative requirements as most important driving forces. *In all cases it is mainly economic factors that determine the use of communication*."

The report notes that communication needs can basically be differentiated between

- Safety critical communication
- Business related communication
- Entertainment

It is further noted that cellular and port broadband networks are likely to play an important role in the future, and that bandwidths in the order of 64kbps are considered 'broadband' for most cargo ships, while the Entertainment segment of passenger ships pose quite different requirements.

The [MarNIS D-HA3F] "Final report on the MarNIS e-maritime architecture" an architecture supporting the e-maritime solutions proposed by the project, with a focus on generic responsibilities and how these responsibilities are to be fulfilled in a European context.

This report is quite detailed on the needs for role based access control to information services in the e-maritime context.

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

The following needs have been deducted from these reports:

Infrastructure functions

Ref. no.	Priority	Need
MN#1	Should	Ownership of information elements, and authorization to pass it on should be managed
MN#2	Should	User identities should be associated with roles
MN#3	Should	A role belongs to a responsibility domain
MN#4	Should	A responsibility belongs to just ONE role
MN#5	Should	A responsibility involves executing certain tasks
MN#6	Can	Roles support different levels of automation (of tasks)
MN#7	Can	Actors may fulfil one or more roles

Communication

Ref. no.	Priority	Need
MN#8	Could	Excluding infotainment and ENC downloads, communication bandwidths of 64kpbs should be sufficient for 'broadband' business and navigation related communication (as evaluated by MarNIS project)
MN#9	Can	Ship – to – Ship communication via intermediate medium (shore service) is considered rarely necessary, except for emergency cases
MN#10	Could	There are clear benefits in particular SAR work in having a broadband communication with the distressed ship, but the benefits depend on whether available to all or only to some ships

3.2 EfficienSea

The first 'EfficienSea' project (2009-2012) was funded by the EU Baltic Sea Region Programme 2007-2013, see more at reference [ESea].

One prime focus of this project was to establish a test bed, testing draft solutions for operational e-navigation services. AIS was used as a communication carrier in many trials, but practical experience revealed that AIS Application Specific Messages were less suitable in an operational context. For moving quantities of more than approx. 68 bytes of data, the link was too unstable. Many services required a more robust delivery of information, and generally a more persistent communication capability was needed to test the services, rather than struggle with communication malfunctions.

It was observed, that using AIS as a communication carrier restricted the ability of especially shore based actors without an MMSI number as an identity – to interact.

Further, encoding / decoding of AIS ASM was noted to lack thoroughly tested standard implementations and requires complex software efforts, prone to software errors. Making

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

matters worse, the operational context and presentation of information contained in ASMs are seldom well described.

In general, the project recommended to enable the use of a selection of other communication carriers, better standardized data formats, based on proven algorithms for parameter encoding/decoding, together with harmonized presentation libraries, and better described operational contexts, for future e-navigation test beds.

The following needs have been deducted from the project:

Infrastructure functions

Ref. no.	Priority	Need
ESea#1	Should	Interaction between other identities than MMSI numbers must be supported
ESea#2	Should	An e-navigation service description should as a minimum include a functional description, user presentation, operational context and definition of data formats
ESea#3	Should	Support for using alternative communication carriers between actors should be provided (roaming)
ESea#4	Should	Support for 'broadcasting to an area' should be provided, even if actors are using different communication links

Communication

Ref. no.	Priority	Need
ESea#5	Should	A communication carrier capable of delivering higher amounts of data than AIS is required
ESea#6	Should	AIS is in itself not sufficiently robust for transport of larger quantities of data
ESea#7	Should	Information transfer between two actors related to an e-navigation service should be carrier agnostic (i.e. not linked to a specific communication carrier.)

3.3 ACCSEAS - Accessibility for Shipping, Efficiency Advantages and Sustainability

A project (2012-2015) supported by the European Commission through the ERDF, under the INTERREG IV B North Sea Region Programme. See ref. [ACCSEAS]

Figure 2 The ACCSEAS logo

The concept of the 'Maritime Cloud' was first conceived in the scope of operating e-navigation test beds, and described by the ACCSEAS project, as "*a proposed technical framework enabling efficient, secure, reliable and*

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

seamless electronic information exchange between all authorized maritime stakeholders across available communication systems, refining an instance of the overarching e-navigation Architecture in the North Sea Region.", see [ACCSEAS MC]

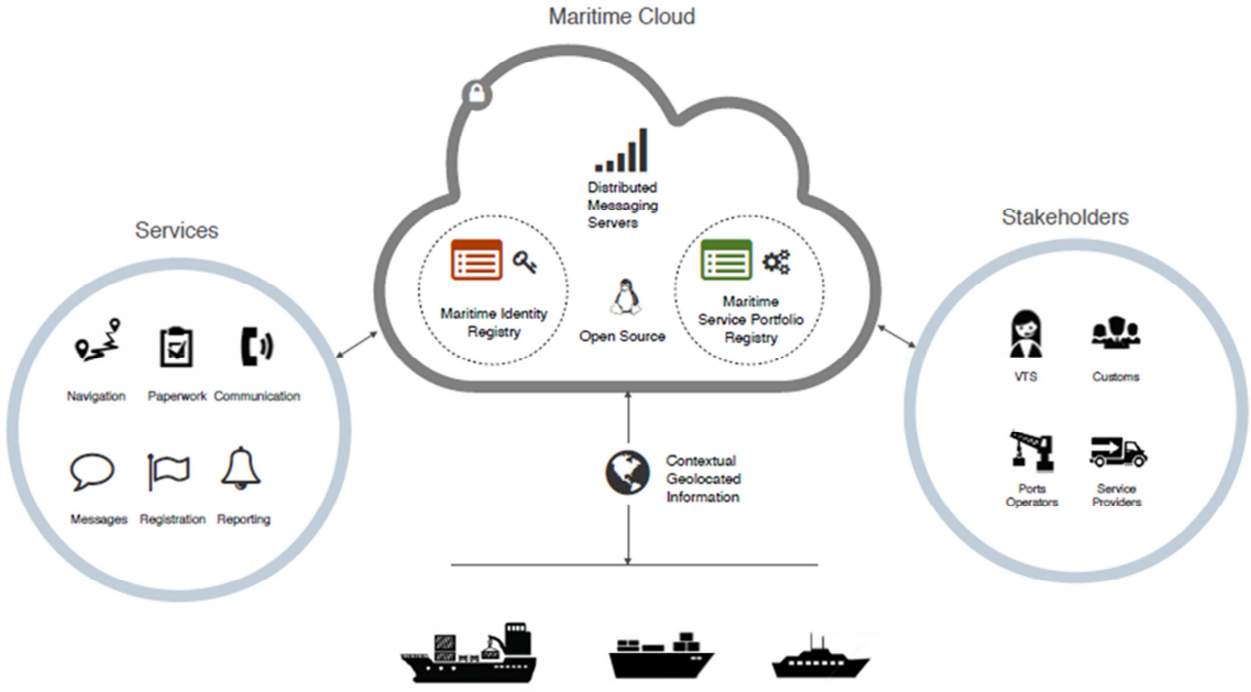

Figure 3 'The Maritime Cloud'.

The report recommends four functional elements as global supporters of service interactions between actors:

- A Maritime Service Portfolio Registry
  - A digital 'yellow pages' directory of services (service type, service providers, electronic address)
- A Maritime Identity Registry
  - A digital 'white pages' directory of actors,
  - Support for Authentication & Encryption

(It was observed that current identifying keys for ships such as IMO and MMSI numbers, ships name, call signs, etc. can be used for lookup, but do not cover a lot of stakeholders, and means for authentication are lacking.)

- A Maritime Messaging Service
  - Carrier agnostic messaging service with geographic multicasting capability and prioritized store-and-forward messaging queue
- A Maritime Cloud Almanac

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

- An offline digital copy of the subscribed sections of Maritime Service Portfolio Registry and Maritime Identity Registry

3.3.1 The Maritime Cloud Client Component (MCCC)

The ACCSEAS e-navigation architecture report [ACCSEAS Architecture] recommends the construction of a 'Maritime Cloud Client Component' as a client application offering a set of APIs (Application Programming Interfaces) for end user applications to interact with the application of other actors, via the central functions of the Maritime Cloud.

- Security through the access to the Maritime Identity Registry (online or via Almanac)
- Service discovery via access to the Maritime Service Portfolio Registry (online or offline via Almanac)
- Messaging API offering a persistent connection seamlessly roaming across available communication carriers with bandwidth optimization of standardized services

3.3.2 Needs derived from the ACCSEAS project

Based on interview with service developers from the ACCSEAS project, and the official reports, the following needs have been derived:

Infrastructure functions

Ref. no.	Priority	Need
AC#1	Could	A service on shore (the proposed MMS - Maritime Messaging Service) could enable forwarding of messages to other identities (point-to-point or multicast) connected to the MMS, regardless of their position and current choice of communication carrier
AC#2	Could	The MMS could enable geocasting (multicasting based on a geographic area)
AC#3	Should	The infrastructure should provide an Identity Registry, which supports Unique Identifiers for different identities (actors), as well as services, etc.
AC#4	Should	The infrastructure should provide means for Authentication of identities, to enable access control to restricted / commercially confidential information
AC#5	Should	The infrastructure should provide standardized means to support encryption or signing of data, to support confidentiality and/or validation of authenticity of transferred data.
AC#6	Should	The infrastructure should provide means to publish / discover a service
AC#7	Should	Privacy of confidential information transfer Should be addressed – technically as well as legally
AC#8	Could	Vetting of identities would increase the credibility of identities and facilitate a higher degree of trust in sharing of information within the industry

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

Communication

Ref. no.	Priority	Need
AC#9	should	An application or device on board ships should enable roaming – i.e. automatically select suitable communication carrier, without requiring manual attention of end users
AC#10	Could	The roaming application/device could inform the Maritime Messaging Service of its position or area of interest to support geocasting (multicasting based on a geographic area)
AC#11	should	The roaming application/device should offer API's for end user applications to interact with other services. These API's should be standardized.
AC#12	Should	Any roaming application / device should apply a protocol which handles acknowledge of reception of data
AC#13	Should	Any roaming application / device should apply protocol(s) which handles bandwidth efficient transfer of data and persistence of the connection (reconnect if connection temporarily lost, without resending packages already transferred)
AC#14	Should	To take into account Cyber Security, the roaming application/device must not accept any external connect request, but must initiate any external connection

3.4 MonaLisa / MonaLisa 2.0

The MonaLisa project (2010-2013) and its successor – the MonaLisa 2.0 project (2012-2015) focused on solutions for enhancing the safety and efficiency of the maritime transport chain in the context of Sea Traffic Management (STM) – see ref [MonaLisa_2.0].

The official output of the MonaLisa 2.0 project is in the process of being published at the time of writing, and links cannot be provided yet.

These projects have developed target concept and key performance indicators for four STM strategic enablers:

1. Voyage Management services aimed at providing support to individual ships in both the planning process and during a voyage including: route planning, route exchange, and route optimization services
2. Flow Management services aimed at supporting both land organizations and ships in optimizing overall traffic flow through areas of dense traffic and areas with particular navigational challenges
3. Port Collaborative Decision Making (Port CDM) services aimed at increasing the efficiency of port calls and departures for all stakeholders through improved information sharing, situational awareness, optimized processes, and collaborative decision making during port calls and departures.
4. SeaSWIM (System Wide Information Management) aimed at ensuring interoperability of services

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

The MonaLisa 2.0 project will be followed by the 'STM Validation Project' (2015-2018), see ref. [STM_validation_project]. The aim is to validate the target concepts using a fleet of hundreds of ships and 10 ports. Please note that the 'SeaSWIM' concept has many similarities and significant overlap with the 'Maritime Cloud' concept. Concrete efforts are being made, towards cross project collaboration between the EfficienSea 2 and the STM Validation Project, to establish common infrastructure standards and demonstrate/validate a common solution rather than developing competing solutions. However the SeaSWIM concept includes several functions or provisions for service definitions, which are specific to the STM concept. The STM validation project therefore foresees a process of determining which requirements and provisions relate to the core of the Maritime Cloud concept, and which are purely STM related.

3.4.1 Requirements derived in STM Validation project

Based on internal documents currently being drafted in the STM Validation Project, based on the outcome of the MonaLisa 2.0 projects, the following draft requirements have been derived for SeaSWIM (please note that these are still 'work in progress'). The requirements are direct quotes from a specific project context, and terminology used reflects that particular project context. The priorities of these drafted STM requirements in relation to the Maritime Cloud infrastructure scope have not yet been determined.

Infrastructure functions

Ref. no.	Priority	Requirement
STM #1	TBD	#1: SeaSWIM must manage authentication and identity/identifier management processes #1.1: Identity/Identifier Management • SeaSWIM shall provide global management of identities for key domain concepts. Key domain concepts include actors (such as information provider and consumers), voyage, vessel, and port call #1.2: Actor authentication • SeaSWIM shall provide trusted mechanisms for authenticating actors, i.e. to ensure an actor is who they claim to be
STM #2	TBD	Req. #2: Access Management • SeaSWIM shall provide mechanisms for defining who shall be allowed to provide and access information Req. #2.1 • SeaSWIM enable that the owner of the information can determine accessibility of the information • SeaSWIM shall provide mechanisms for information owners to manage who get access to that information • SeaSWIM shall provide mechanisms for nominating collaborators, who shall be allowed to provide / access information or delegate the nomination to other service providers which may do some intermediate processing of the data • The right to delegate a nomination is likely to be established in a Service Agreement between the information owner and the service provider. It needs to be evaluated if it is suitable and technically achievable to control the delegation of access right, or if this needs to build on trust based on the agreement

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

STM #3	TBD	Req.#3: Secure information transfer from point-to-point (cyber security) • SeaSWIM shall ensure that the information being communicated is adequately protected from unauthorized access in all communication links from end-point to end-point
STM #4	TBD	Req. #4: Discoverability of services and identities • SeaSWIM shall provide mechanisms for discovery of identities and services based on various criteria, such as role, geographical area (which in turn require that identities location is available), used application, time as well as mandatory/compulsory information exchanges
STM #5	TBD	Req. #5: Different types of services interactions SeaSWIM shall support different types of services. Such types include: • Push type services based on a publisher-subscription interaction • Request-response type services based on responding to a client's request • Broadcast type services based on making information available to everyone in (for instance) a selected geographical area
STM #6	TBD Possibly STM specific design criteria	#6: Structures and updates of data/information objects #6.1: Keep the reference to the larger information structure • SeaSWIM shall ensure that access to and provision of single information objects which exists in a larger information structure is done in relation to the larger information structure #6.2: Allow multiple services to use the same information • SeaSWIM should facilitate that the information content contains the latest updates and that the services use the same information
STM #7	TBD Possibly STM specific design criteria	Req. #7: Enabling communication about states • SeaSWIM shall enable sharing information about intentions and actual performance associated with different aspects of the sea voyage (including the port call) enabling distributed coordination of different forthcoming actions
STM #8	TBD Possibly STM specific design criteria	Req. #8: Access to historical information • SeaSWIM shall allow service providers to record/log different performances given that the information owners allow that in their agreement with the service provider
STM #9	TBD Possibly service specific design criteria	Req. #9: Monitor and evaluate service consumption • SeaSWIM shall provide mechanisms for capturing service interaction patterns and channel evaluations for the purpose of governing and monitoring service usage
STM #10	TBD	Req. #10: Allow third-party development and service portfolio management • SeaSWIM shall provide mechanisms allowing third-party developers to provide STM and SeaSWIM compliant services as part of service portfolio management; this includes the use of a shared service specification language
STM #11	TBD	Req. #11: Provide information about the status of the communication • The SeaSWIM infrastructure shall allow distribution of information about the status of the communication
STM #12	TBD	Req. #12: Services for non-standardised message interaction • SeaSWIM shall support text messages with non-standardised content. The text-chat function could be used to clarify other standardised information exchange

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

		e.g. explain reason for changed time of arrival

Communication

The following observation related to communication with ships has been noted:

Ref. no.	Priority	Need
STM #13	Should	While terrestrial IP-based communication services are assumed available to actors in a port environment or ashore, ships connectivity may be interrupted. A persistent and robust data transport protocol should be applied to ensure data transfer between ships and their shore based collaborators

3.5 Flagship – European framework for safe, efficient and environmentally-friendly ship operations

The Flagship project (2007-2010) – see ref. [FLAGSHIP] - was an industry driven EU co-funded project focusing on improvement of safety, environmental friendliness and competitiveness of European maritime transport.

One project deliverable [FLAGSHIP D-D1.3] analysed communication requirements for various application classes; investigated current and emerging data carriers and compared the carriers' capabilities to the application requirements.

The report notes that a few safety critical operations require Real Time point-2-point communication capabilities, while most navigation and business related applications have more relaxed timing requirements. Further, the major driver for bandwidth is identified to be 'Infotainment' related to satisfy crew and passengers, rather than most other applications.

A related report [Comms_for_enav] written by MARINTEK discusses the needs for ship-to-shore digital communication and applicability of solutions to the IMO e-navigation strategy.

3.5.1 Needs derived

Based on the reports mentioned, the following needs have been derived:

Infrastructure functions

Ref. no.	Priority	Need
FS#1	Should	Support for Authentication of sender of information should be supported, preferably based on MMSI

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

Communication

Ref. no.	Priority	Need
FS#2	Should	A new e-navigation carrier should include mechanisms for authentication of sender, preferably based on MMSI
FS#3	Should	Redundancy in choice of communication carrier is requested (Roaming) No application can run on all carriers and no carrier can satisfy all application at any location at the sea More than one carrier will be needed to satisfy all requirements; one of these will typically satisfy GMDSS requirements Roaming capabilities will increase robustness
FS#4	Should	Internet based IP links via commercial service providers are not suitable for Real Time emergency operations (typically dedicated point-2-point communication needed)
FS#5	Should	Least cost routing based on cost/ datalink quality / capacity needed
FS#6	Should	Security of datalinks is an increasingly important factor Typical security implementations require VPN firewalling of connections from ships to shore

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

4 IMO e-navigation MSP's

In the process of evolving the IMO e-navigation strategy, a set of Maritime Service Portfolios (MSP) have been defined, encompassing the services related to ships navigation.

The following requirements or observations have been deducted from the MSPs.

Table 6
List of proposed MSPs

No	Identified Services	Identified Responsible Service Provider
MSP1	VTS Information Service (IS)	VTS Authority
MSP2	Navigational Assistance Service (NAS)	National Competent VTS Authority/Coastal or Port Authority
MSP3	Traffic Organization Service (TOS)	National Competent VTS Authority/Coastal or Port Authority
MSP4	Local Port Service (LPS)	Local Port/Harbour Operator
MSP5	Maritime Safety Information Service (MSI	National Competent Authority
MSP6	Pilotage service	Pilot Authority/Pilot Organization
MSP7	Tugs Service	Tug Authority
MSP8	Vessel Shore Reporting	National Competent Authority, Shipowner/Operator/Master
MSP9	Telemedical Assistance Service (TMAS)	National Health Organization/dedicated Health Organization
MSP10	Maritime Assistance Service (MAS)	Coastal/Port Authority/Organization
MSP11	Nautical Chart Service	National Hydrographic Authority/ Organization
MSP12	Nautical Publications Service	National Hydrographic Authority/ Organization
MSP13	Ice Navigation Service	National Competent Authority Organization
MSP14	Meteorological Information Service	National Meteorological Authority/WMO/ Public Institutions
MSP15	Rea-time Hydrographic and Environmental Information Service	National Hydrographic and Meteorological Authorities
MSP16	Search and Rescue Service	SAR Authorities

Figure 4 - IMO e-navigation Maritime Service Portfolios (MSPs)

Infrastructure functions

Ref. no.	Priority	Need
MS#1	Should	Ships as well as a multitude of shore based identities must be able to interact Not all have MMSI numbers
MS#2	Should	Actors should be able to interact peer-2-peer without using a point-2-point radio link or the same satellite system (roaming)
MS#3	Should	Several shore based services require the capability to broadcast information to actors inside or subscribing to information in an area or along a route, either via specific communication channel or via roaming function, preferably independent of the range of a specific broadcast station
MS#4	Could	Support for setting up dynamic multicast groups (like chat rooms) for multicasting information only to actors related to a particular operation (like a SAR operation) is requested

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

MS#5	Should	Although not part of the GMDSS, any roaming capability should support the operational priorities defined for GMDSS (Distress, Urgency, Safety, Routine) in executing queues of information transfer The roaming capabilities must respect the regulations of the GMDSS
MS#6	Should	Support for relaying distress or urgency related communication (in particular shore-shore communication) - requires high availability and acknowledge of message delivery
MS#7	Should	Several MSPs require the ability to validate origin, authenticity and integrity of received information
MS#8	Should	VTS centres require the ability to detect and identify ships passing a reporting line or entering a VTS area
MS#9	Should	To achieve automated reporting, ships need access to an updated, standardized list of Ship Reporting Systems (SRS), their geographic limitations and their requirements for reporting, to discover and detect passage of a mandatory reporting line The infrastructure should support discoverability of a SRS enable determining the related information to be reported, and the endpoint where to deliver the information
MS#10	Should	Support for overview of geographic domain awareness of actors (request/provide access to position information or route intentions) is requested by several MSP's (VTS, SAR, …)
MS#11	Should	Several MSPs require the recipient of transferred information to provide acknowledgement of information transfer Any roaming support service should support determining the information transfer acknowledgement level Differentiation should be made between datalink acknowledgement (data reached the communication destination), application level acknowledgement (an application which supports the format of data transferred acknowledged it's reception) or user acknowledgement (a user read / reacted to the information received)
MS#12	Should	Automated reporting requires support for non-repudiation (proof of the reporting transaction being completed)
MS#14	Should	Support for confidential transfer of information is required
MS#15	Should	Support for service providers to authenticate a requesting identity is required (access control)
MS#16	Could	Support for online discoverability of services, such as recognized publishers of standardized information services, is requested

Communication

Ref. no.	Priority	Need
MS#17	2 - should	Mechanisms supporting persistence in message delivery across unstable communication links should be considered for ship-shore communication

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

5 Needs gathered within the EffecienSea 2 project

This section describes needs that have been derived from a number of draft use case descriptions of information services under development by work packages 4, 5 and 6 in the EfficienSea 2 project. The needs gathered are partially specific to the related services (i.e. not necessarily related to a generic infrastructure), but to ease service implementation an attempt has been made to derive commonalities, which can be generalized and where appropriate addressed by centralized functions.

5.1 Enhanced Navigation Support Information & Route exchange

The following requirements have been derived from initial input on experience from the ENSI – Enhanced Navigation Support Information (provided by EfficienSea 2 partner no. 6, the Finnish Transport Agency). A presentation of the initiative is available in ref. [ENSI].

Infrastructure functions

Ref. no.	Priority	Need
ENSI#1	2 - should	VTS should be able to collect route intention of ships in VTS area The sensitivity of this information requires secure identification and authentication of involved parties, and confidential information transfer

Communication

Ref. no.	Priority	Need
ENSI#2	Should	Seamless use of different communication carriers (roaming) should be supported
ENSI#3	Should	Data compression should be applied to exchange of information
ENSI#4	Should	No cost (or at least very low cost) of communication should apply to reception of Maritime Safety Information – yet high certainty of delivery is desirable

5.2 Space weather service for the Arctic

The following have been derived from a draft warning service related to risk of space weather disruption to communication and satellite navigation services.

Infrastructure functions

Ref. no.	Priority	Need
SWS#1	Should	The ability to distribute warnings to ships outside range of stable connectivity is required (persistent message delivery)

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

5.3 Commercial services

A draft overview of requirements to service interactions from the viewpoint of EfficienSea 2 partner no. 32, the UKHO, a commercial service provider:

Infrastructure functions

Ref. no.	Priority	Need
COM#1	Should	The infrastructure should support publishing a service, to make it discoverable for users
COM#2	Should	The infrastructure should support distributing a data product to subscribers A standardized method for setting up a subscription to a service should be supported
COM#3	Should	Billing should be facilitated, at least through secure authentication of users requesting a service/product

5.4 NW-NM service

Based on draft input from **WP4** (by Danish Maritime Authority) on Navigational Warning – Notice to Mariners service (relation to IMO MSP5/MSP12):

Infrastructure functions

Ref. no.	Priority	Need
NW#1	Could	Identity and authorization management by the infrastructure could facilitate interactions between actors not necessarily belonging to the same organisations, such as editors, Navarea and subarea coordinators, etc. before publication
NW#2	2 - should	Support for broadcasting warnings as well as unicasting / multicasting to ships in an area or entering an area should be supported
NW#3	2 - should	Recipients of NW-NM information should be able to validate authenticity and integrity of the broadcast or published information
NW#4	2 - should	Notices to Mariners is traditionally a subscription service – subscription and billing mechanisms need to be supported, at least through secure authentication of requesting users

5.5 S-101 / S-102 ENC and MiO services

Based on draft input from **WP6,** by EfficienSea 2 partner no. 2 the Danish Geodata Agency, on an Electronic Nautical Chart service and Maritime Information Overlay service the following has been derived (relation to IMO MSP11):

Infrastructure functions

Ref. no.	Priority	Need
MiO#1	Could	A push version of an ENC or MiO services would need the ability to detect ships entering (or intending to enter) a new chart area, or area where certain Nautical

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

		publication is relevant, is requested. (A pull version where ships initiate requests for updates does not share this need.)

5.6 Port Reporting

Based on draft input from **WP5** (compiled by E2 partner no. 14, BIMCO) related to Port Reporting, the following has been derived:

Infrastructure functions

Ref. no.	Priority	Need
PR#1	Should	To facilitate automation of port reporting based on standardized documents/data structures like the IMO FAL forms, it must be possible to discover/detect which documents are required when and by which authorities, when approaching a port
PR#2	Should	Authentication of who is providing reporting information is critical Certificates may need to be part of a data transfer
PR#3	Should	Support for encryption of data during transfer to address commercial confidentiality of information is required

Communication

Ref. no.	Priority	Requirement
PR#4	Should	Data compression is desirable
PR#5	Should	Data amounts for port reporting may be significant, but transfer is seldom repeated
PR#6	Should	Data encryption may be necessary to support commercial confidentiality

5.7 Weather services

Based on draft input for improving weather service from **WP4** and **WP6** (provided by EfficienSea 2 partner no. 3, the Danish Meteorological Institute), the following have been derived:

Infrastructure functions

Ref. no.	Priority	Requirement
WS#1	Should	Authentication of information provider must be included
WS#2	Should	Support for billing may be necessary to support commercial services (at least authentication of subscribing users)

Communication

Ref. no.	Priority	Requirement
WS#3	should	Data amounts are significant, and data compression is desirable

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

5.8 Emission monitoring

Based on draft input for an emission monitoring service from **WP5** (compiled by E2 partner no. 25, Litehauz), the following have been derived:

Infrastructure functions

Ref. no.	Priority	Need
EM#1	Should	Data encryption during transfer is required, to protect the confidentiality of information
EM#2	Should	Ships' identity must be authenticated
EM#3	TBD (service specific)	It should be possible to validate time stamping of information

Communication

Ref. no.	Priority	Need
EM#4	Should	Data compression is desirable

5.9 Other considerations

Based on brainstorming within the task group in **WP3** of the EfficienSea 2 project, the following additional requirements have been derived:

Infrastructure functions

Ref. no.	Priority	Need
MISC#1	Could	Setting up multicast groups to allow sharing operational information amongst a group of identities engaged in simultaneous operations in an Offshore Environment (SIMOPS) is desirable
MISC#2	Could	Many use cases request access to position (or intended route) information of ships or other mobile assets A common position service providing role based access to certain roles (like the Data Distribution Plan for the LRIT agreement) and allowing nomination of other collaborators' access to the same information, could be beneficial to a large number of applications
MISC#3	Should	Non-SOLAS ships and other actors within the Maritime Domain should be able to participate
MISC#4	Should	Introduction of the infrastructure should not require major modifications of existing systems It should rather allow a gradual transition towards better service designs, providing fewer but unified access control mechanisms, and automation of interactions not requiring user attention

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

6 Lessons learned

During the development of the Maritime Cloud as a set of infrastructural functions to support e-maritime, e-navigation, Port Collaborative Decision Making or areas of application within the Maritime Domain, it can prove beneficial to look at projects from other sectors.

Electronic solutions including communications and services are being implemented or have been implemented elsewhere, and lessons learned may provide valuable insights. This chapter collects some of the lessons learned from other areas of applying ICT to a specific domain, and compare to the state of the art in the Maritime Domain.

The purpose of this section is to evaluate whether this raises similarities, additional needs to be addressed or pitfalls to be avoided in establishing an infrastructure for interoperability within the Maritime Domain.

Cases from a few different industries and sectors have been studied, and lessons have been extracted in order to try to avoid some of the problems encountered in the past. Also more general and useful experience from involved organizations will be mentioned in the following.

6.1 Energy Sector

Experience from SMART GRID developments, provided by EfficienSea 2 partner no. 13, OFFIS.

The energy sector was until 2008 quite heterogeneous and fragmented, with different standards and national regulations. Work has since then been done towards a European and world-wide Smart Grid to improve interoperability between previously incompatible initiatives. This work has been successfully conducted through a Reference Architecture Model approach.

A Reference Architecture Model:

- Provides a common view and understanding concerning architecture and interoperability amongst all stakeholders
- Maps existing approaches/architectures in one reference architecture model
- Drives systematic development/enhancements of standards and regulations
- Provides methodology to develop use cases according to Ref. Arch. Model
- Provides engineering guidelines for implementation of interoperable applications and services
- Supports transition from legacy architecture/solutions to new interoperable architectures
- Provides means for checking interoperability conformance
- Exploits existing interoperability approaches and standards

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

- Aggregation of existing/new architectures into common framework
- Methodology for development of interoperable applications and services

The resulting Smart Grid Architecture Model (SGAM) has provided the mechanisms to compare different system architectures, and identify opportunities or gaps in standardization or harmonization, in order to achieve interoperability at different levels. To achieve interoperability between complex systems of many stakeholders, standards for interoperability must be sought in relation to business models and regulatory frameworks, functional/operational levels, information/data models, communication between system components as well as physical connections at component level.

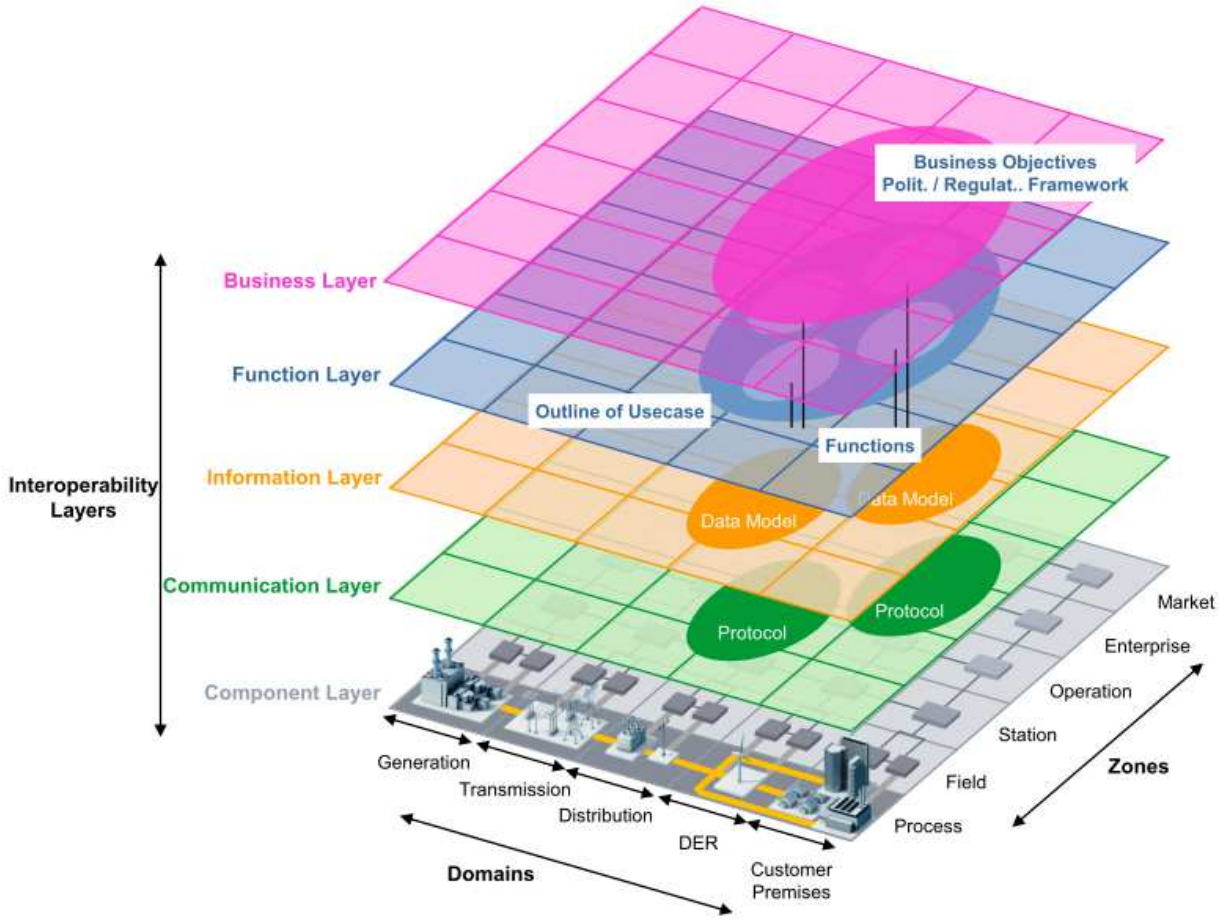

Figure 5 The SGAM framework

The establishment of a Maritime Architecture Framework (MAF) has been initiated by the EfficienSea 2 project, and is highly recommended in order to:

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

- Provides a common view and understanding concerning architecture and interoperability amongst all stakeholders
- Enable mapping of different architectures into one reference architecture model, allowing the inspection of how different standards on different interoperability layers support interoperability, or identify standardization gaps
- Drives systematic development/enhancements of standards and regulations
- Avoid Fragmented, incompatible developments – already in course of the EfficienSea 2 project
- Avoid High integration costs for industrial partners – in and beyond the EfficienSea 2 project

6.2 Emergency Service IP-Networks (Public Safety NENA NG911)

Compiled by EfficienSea 2 partner no. 22, Frequentis

6.2.1 International government cooperation

End users in telecommunication expect seamless and easy to use services independent of individual country's frontiers and provider companies. Maintaining and enhancing an almost worldwide interoperable emergency communication IP infrastructure requires coordination on government level. Standards need to be defined, agreed on and enforced by regulations.

In May 2011 the European Commission (EC) released Mandate 493 (M/493) [NG911 - 9], which updates the universal service directive (Paragraph 5 of Article 26). The objective of this Mandate is to stimulate further standardization work in this field and to support harmonized European solutions also with regard to cost effective implementations. The European Standardization Organization (ESO) was invited to prepare a coherent and complete set of specifications or standards containing the architecture, the interfaces and the protocols in use.

ETSI describes a functional architecture [NG911 - 10] to support requirements as outlined in the EC mandate M/493, and refers to public routing services that implement LoST (Resolver, Forest Guide and Authoritative Mapping, see ref.). The architecture covers VoIP access to emergency services, where the provider of voice service and the emergency services may be in different jurisdictions. This fact requires regulatory changes, and therefore cooperation of EU member states (government and regulators).

6.2.2 Drivers for cooperation

- Strategic technology alliances between firms (common interfaces but different domains – e.g. GIS/Mapping and VoIP/Routing)
- Co-operation agreements between public institutions (EENA, NENA, key persons are members of both organizations, same standards)
- International harmonization of access to emergency services

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

- Most important: better and more efficient emergency services for the public

6.2.3 Known risks

- Changes to national legislation may be required
- A long standardization process innovation may lead to proprietary solutions that quickly outperform solutions based on open standards (example: Google Maps geolocation API)
- Architecture may be too complex to be deployed
- Migration path not defined

6.2.4 Unexpected pitfalls

- The idea of location-based emergency services does not add value for the customer (highly unlikely)
- It does not reduce the operating costs (no real business model for location based emergency services, but can positively impact the national economy)

6.2.5 Time scale of implementing standards

Five to ten years – step-by-step approach, customer is currently asking for a NG story and how to migrate.

6.2.6 National protectionism

Each country or federal state maintains its own infrastructure and provides “authoritative mappings” for their jurisdiction areas (service boundaries). Common protocols support “roaming” – bilateral agreement (compare to international PSTN or mobile roaming).

6.2.7 Industrial driven (or lack of) cooperation

Not only the public access to emergency services requires coordination and cooperation, but also private networks of Emergency Response Organizations (EROs) require technical interoperability when responding to large scale disasters. For instance in order to manage a peak volume of emergency calls one could easily change the service boundaries and redirect calls to backup sites. To ensure interoperability in emergency communications not only international bodies like International Telecommunication Union (ITU) are involved in harmonizing approaches, exemplary two associations stand out in transnational activities:

- EENA (European Emergency Number Association) - Europe
- NENA (National Emergency Number Association) – North America

*EENA, the European Emergency Number Association, is a Brussels-based NGO set up in 1999 dedicated to promoting high-quality emergency services reached by the number “112” throughout the EU. EENA serves as a discussion platform for emergency services, public authorities, decision makers, researchers, associations and solution providers with a view to improving the emergency response in accordance with citizens' requirements. EENA is also promoting the establishment of an efficient system for alerting citizens about imminent or developing emergencies [*NG911 - *7].*

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

*The EENA memberships include more than 1000 emergency services representatives from 80 countries world-wide, 75 solution providers, 15 international associations/organizations, more than 150 Members of the European Parliament and 73 researchers [*NG911 - *7].*

Though EENAs is a European Organization, members are located all over the world, supporting international cooperation at all levels.

NENA's mission is to foster the technological advancement, availability and implementation of a universal emergency telephone number system (9-1-1). In carrying out its mission, NENA promotes research, planning, training and education. The protection of human life, the preservation of property, and the maintenance of general community security are among NENA's objectives. NENA has more than 8000 members worldwide.

Both organizations are well supported by the industry and organize joint events focusing on policy, technology, operations, education, and interoperability testing. NENA has set up a yearly Industry Collaboration Event (ICE) aimed at supporting vendors in testing with each other. Industry is invited to join test sessions in an open, supportive, and collaborative, environment that foster a spirit of technical co-operation [NG911 - 8]. So far over 40 vendors have participated in the events since 2009. This was a key enabler for ensuring both validation and early adoption of the proposed standards. The first NG911 solutions tested in ICE test beds are already in use in fully operational systems, evidence for the effectiveness of this coordinated and well established interoperability tests.

ETSI in cooperation with the European Emergency Number Association (EENA) is organising the 1st ever Plugtests™ event to be held in Europe with the support of ETSI SC EMTEL. This event will be located in Sophia-Antipolis from 14 - 18 March 2016. The concept of Next Generation 112 (NG112) has been identified as a potential answer to the increasing requirements and demands of content-rich emergency calling. The interoperability of such NG112 products and services has not been tested in Europe previously leading to this ideal opportunity. This NG112 Emergency Communications Plugtests™ event will see a testing campaign based on the use cases developed by ETSI and EENA, and is a unique chance for vendors of emergency communication equipment to test their product against different implementations and scenarios. The benefits for a vendor in participating include a chance to test early implementations in a neutral environment, to validate their understanding of next generation emergency calling requirements as well as a to communicate about and promote the technology. This activity is supported by the European Commission.

6.2.8 Observations in relation to a maritime information infrastructure

- Although an infrastructure for geolocated emergency services may have a positive impact on national economies, defining a business case for the actors involved in establishing the infrastructure for this purpose exclusively is difficult – the primary driver is a political desire to achieve better and more efficient emergency services.

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

- The introduction of infrastructural support for emergency services across jurisdictions may affect many levels of legislation.
- The harmonization process is at risk of being overtaken and outperformed by proprietary technology developments, as a result of a low speed of evolution of standardized solutions with a timeline of 5-10 years, compared to solutions targeting a better business case
- Test beds and developer forums / events with many vendors involved play an important role in detailing the relevant requirements, as well as testing and validating technologies

Derived needs related to Infrastructure functions

Ref. no.	Priority	Need
NG911 #1	Should	A business case for operating the infrastructure functions should be identified
NG911 #2	Should	Legal implications of establishing the infrastructure functions should be analysed and addressed
NG911 #3	Should	The roadmap towards establishing infrastructure functions should include establishing test beds and developer forums, where technologies can be tested and validated, and allow room for agile adaptation of technology developments
NG911 #4	Should	The level of criticality of the infrastructure functions must be defined. If Infrastructure functions are to support emergency services now – or in the future – basic design must take requirements related to such services into account, even if the initial operational scenario is not intended to target emergency services

6.3 Overview of ongoing standardization efforts

Standardization & harmonization activities within the Maritime Domain take place within numerous regional and international standardization and industry collaboration bodies, with each their own or overlapping responsibilities: IMO, ITU, IHO, IALA, CIRM, IEC, ISO, RTCM, NMEA, ETSI, BIMCO, to name a few.

As part of the EfficienSea 2 project, a report containing an overview of identified and ongoing standardization efforts related to the project (**deliverable D1.5**) will be published along with this report, and followed by a strategic roadmap for standardization efforts needed to support the evolution of an infrastructure for service interactions initiated by the project.

6.4 Maritime standardization, certification and type approval issues

A paper discussing constraints imposed by the current type approval regime has been provided by EfficienSea 2 partner no. 30, Transas Marine.

The paper discusses the relevance of the strict procedures and type approval regimes, and the apparently varying interpretation of the rules, which generate very long lead times to

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

introducing new technologies on the bridge of a ship. As example the first draft standards for ECDIS goes back to early 90s with standard adopted in 1996. We saw the first type approved ECDIS in 1999. The standard is/will be compulsory from 2012-2018 for most SOLAS ships. We talk about a technology transition period of more than 25 years. The paper argues that while strict enforcement of standards must govern safety and security of mission- and safety critical equipment, the speed of introduction of equipment to address less functions on board ships not defined as mission- or safety critical, should be increased by provided guidelines for a smoother way of introducing new technology using commercial off-the-shelf (COTS) equipment not necessarily adhering to the current test standards for bridge equipment.

The discussion paper provides examples of enablers of rapid introduction of new technologies such as in telecom where the Bluetooth standard was developed and introduced in less than 18 months. Another example can be found in the aviation industry, where iPads are used in the cockpit for non-safety critical information such as flight plans, weather information, airport maps, loading documents and much more.

Other industry members have however contested part of the validity of some statements and relevance of the issues raised in the discussion paper. This disagreement within the equipment vendor community in itself reveals the importance of addressing safety and certification issues as well as the need for type approval – not only related to on board equipment, but also the introduction of shore based services and allowing them to interact machine to machine with shipboard equipment.

Due to the disagreement expressed, the full text of the discussion paper has not been included in this report.

Derived needs related to Infrastructure functions

Ref. no.	Priority	Need
Cert#1	Should	The criticality of services must be defined, and use cases must address which the context of use in terms of equipment and their type approval constraints, as well as needs for certification of service designs or service providers
Cert#2	Should	Guidelines for designing services, should address implications of designing services to interact with type approved equipment

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

7 Comments from the High Level User Group

The draft conclusions of this report and their implications on establishing a digital infrastructure for the Maritime Domain were presented to the EfficienSea 2 project partners during the first week of October 2015, as well as to the High Level User Group (HLUG) associated with the EfficienSea 2 project. The HLUG consists of representatives from BIMCO, CESMA, IALA, ICS, Nautical Institute, Lloyd's Register, Ericsson, IBM, GS1 Denmark, Danish Maritime Authority, Swedish Maritime Administration, SMHI Weather solutions, and Maersk Maritime Technology. The aim was to collect feedback from the industry and other important maritime stakeholders, further qualifying or moderating any conclusions drawn by this report.

A brief and preliminary summary of the HLUG comments are included here. A more in depth summary of the HLUG inputs will be further progressed by the project.

7.1 SWOT analysis

The HLUG had been asked to provide input to a SWOT analysis of the whole concept of the 'Maritime Cloud' concept as an enabler of digital interactions in the Maritime Domain.

7.1.1 Strengths

- The ability to act as an all-inclusive enabler for door-to-door services
- A diverse group of interests – including cross project collaborations - seem to be working together towards a common goal, including organizations capable of drafting and publishing standards
- This concept appears to be a driver towards harmonization of data exchange, with potential for design of technology neutral solutions
- Real potential is perceived for reduction in administrative burden, which gives more time to bridge teams attention to the act of navigation
- EU support indicates potential for at least regional impact

7.1.2 Weaknesses

- The concept has a very broad scope, priority of focus seems unclear
- Many stakeholders involved with different or even contradicting interests
- Needs to be aligned with current certification regime for ships' on board systems
- Commercial benefit needs to be demonstrated, it needs to be 'sellable'
- Cyber security and privacy/confidentiality issues may pose significant challenges to the concept. (Emerging Industry standards need to be observed)
- Talk about the 'Maritime Internet of Things' is feeding cyber security concerns

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

- Warning not to reinvent the wheel, but rather involve industry partners from different sectors with relevant experience
- If advanced identity management is introduced, it is recommended to keep it simple for users!
- Must not introduce single points of failure
- If the project result is not perfect, it is feared to be just another book on the shelf in Brussels

7.1.3 Opportunities

- The ability to improve maritime connectivity with 'hinterland logistics'
- Seen as an opportunity to implement global standards and avoid regionalization
- The timing is right, similar developments taking place in the industry already – technological development WILL make this happen, so it is great if it could happen in a coordinated and somewhat controlled manner
- Cyber security solutions from other industries available could be applied
- Perceived opportunity to empower users by seamless provision of decision support information, not making decisions for users
- Real opportunity for making point-2-point mandatory reporting automatic

7.1.4 Threats

- Many 'competing' projects and initiatives – need to seek collaboration
- Single window concept is in need of progress – 'little kingdoms', even within countries, may pose a risk to the Maritime Cloud concept as well
- A business model for operation of the infrastructure is missing / difficult to imagine, without a business case fear of complexity driving excessive costs
- Without a lot of early adaptors, critical mass of users may never be reached
- Without proven ICT security, no insurance company will insure maritime assets – and no clients will buy in. Cyber Security must be proven

7.2 Considerations on business models and governance of an infrastructure

In general, the HLUG indicated that a convincing business model for establishing and operating a joint infrastructure was needed to achieve credibility. It was discussed whether setting standards for joining purely private clouds – or clouds established by major ports - could be the basic model. An alternative was public funding of establishing infrastructure was realistic, while continued operations, evolution and maintenance could be funded by 'pay per use' fees, similar to how the construction and operation of a major bridge could facilitate growth in the connected communities.

It was discussed if the infrastructure on the one end of the spectrum should be totally governed and controlled by an international authority like the IMO or at the other end of the spectrum should be totally market driven. The consensus was that most benefits would be

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

gained if the governance model could be somewhere between the extremes, in some kind of public private partnership or collaboration.

It was noted that it seemed unrealistic to agree internationally on establishing the infrastructure functions purely on the basis of a public funded mandatory requirement regime, similar to the LRIT agreement. More likely the concept would need to grow out of commercial benefits to the industry, however the functions of LRIT could be part of the infrastructure implementation and thus the related business case and governing agreement could form part of the solution.

7.3 Other recommendations

It was noted that if including safety critical functions such as those related to the GMDSS were included in the scope of developments, the whole bulk of mandatory requirements could weigh down the Maritime Cloud concept. The development and operational costs would increase significantly, and progress of solutions beneficial to the commercial industry would slow down. Therefore, it was recommended that while preparing infrastructure design to support safety functions in the future, it should deliberately be avoided to focus on pushing safety critical functions in the infancy of the concept.

It was recommended to the project that a strategic roadmap should be drafted, to indicate what needs to be achieved first, what could be achieved by other or future projects, and to isolate items not to be progressed by the EfficienSea 2 project, in order to sharpen the focus of the project.

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

8 Consolidated list of needs

The following is a list of consolidated needs identified in this report, that relate to functions that a digital infrastructure for the Maritime Domain should support, in order to lower system integration costs and facilitate service development. The needs have been grouped under headlines, outlining the primary topics to be addressed by infrastructure.

It has not been possible to perform a complete process of prioritization deriving formal requirements.

More specific communication needs related to capacity, etc. are not addressed in this report. This is a topic that will be dealt with separately in **WP2**.

8.1 Identity management and role based access control

No.	Ref. needs	Need	Notes
ID#1	ESea#1, AC#3, STM #1, FS#1, MS#1, NW#1, MISC#3	All types of Ships as well as a multitude of shore based or Off Shore entities must be able to interact, and Digital Identity of interacting actors must be manageable	See Wikipedia for an overview of definitions related to digital Identity Management. https://en.wikipedia.org/wiki/Identity_management In the maritime domain entities such as companies, authorities, ports, ships as well as employees or operators with assigned roles/responsibilities (such as ships' captain, VTS operator or harbour master) must be identifiable.
ID#2	AC#3, STM #1, MS#1	A digital UID (Universal Identifier) concept must be defined for the Maritime Domain, which is flexible, decentralized and forward compatible, yet provide unique identifiers for different actors.	An Identity concept that can provide one binding, unique identifier that can cover the Maritime Domain must be developed The identifier concept could be a maritime adoption of the URI (Universal Resource Identifier) https://en.wikipedia.org/wiki/Uniform_Resource_Identifier
ID#3	AC#3, STM #1, FS#1	A UID registry is needed, which can uniquely identify an actor, and facilitate lookup of secondary identifying attributes	Not all actors have MMSI numbers, however MMSI numbers play a significant role in several existing GMDSS and dedicated maritime communication systems In other cases identifiers such as terminal numbers, or e-mail addresses could be used to identify an actor The UID registry must enable binding (lookup) between existing identifiers and a unique UID It must be possible to decentralize the process of assigning identities As such, the UID registry may be decentralized, but lookup of identities and associated identifiers must be possible across the Maritime Domain.
ID#4	MN#2, MN#3,	It must be possible to associate identities with roles	Standardized roles may be defined by certain stakeholder groups to manage which identities are

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

	MN#4, MN#5, MN#6, MN#7	The role concept should be flexible, decentralized and forward compatible, allowing unique role definitions for different responsibility domains	associated with certain responsibilities and entitled to which level of access In using role based access management, a role belongs to a responsibility domain, where a specific responsibility belongs to one role, eg. IMO could define the roles of a 'Flagstate', 'Coaststate' or 'Portstate', and delegate authority to competent authorities of its member states to assign such roles to identities executing tasks related to those responsibilities EU could most likely reuse roles already defined relevant to information sharing within the e-maritime concept An actor/identity may be assigned more than one role
ID#5	STM#1	Unique Identifiers for virtual objects (such as information objects) are paramount for some use cases and should be considered in relation to developing a maritime UID concept	Example: A Voyage_IDs identifying a particular voyage of a particular ship, or a Persistent Universal Identifier for an Aid to Navigation Identities related to objects that are not actors and need authentication may belong to other registers, than the Identity register related to actors that need authentication.
ID#6	AC#4, STM #1, FS#1, MS#15, ENSI#1, COM#3, NW#1, NW#4, PR#2, WS#1, WS#2, EM#2	Standardized function(s) for Authentication of identities is needed	The ability to validate the identity of an actor requesting access to restricted information or a resource is needed by many use cases to facilitate access control Common authentication function(s) is(are) needed, to avoid all services implementing their own authentication function, requiring actors to maintain password lists for all systems they need to access.
ID#7	AC#5, MS#7, MS#12, PR#2, WS#1	Standardized function(s) for validation of authenticity and integrity of transferred information are needed	It must be possible to 'sign' a digital document in such a way, that the recipient can validate the origin of the information and detect if it has been modified Certificates may need to be part of some data transfers.
ID#8	AC#5, AC#7, STM #3, MS#14, EM#1	The infrastructure must provide standardized means to support encryption of data	In order to support transfer of confidential information
ID#9	MN#1, STM #2	Ownership of information elements, and authorization to pass it on must be managed	The infrastructure must not pass on information to unauthorized parties Privacy of confidential information transfer must be addressed – technically as well as legally, including requirements for legal interception (law enforcement). A digital service provided based on this infrastructure must be explicit about ownership of information and authorization to pass on information Standardized functions supporting Nomination of collaborators (roles or specific identities who are entitled to access my information) could ease implementation of many information services

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

ID#10	AC#8	Vetting of identities would increase the credibility of identities and facilitate a higher degree of trust in online business relationships or sharing of information within the industry	Vetting: Validation of relationship between legal entity and digital identity – for instance a flag state validating the relationship between a ship and an associated digital identity (identified by UID, IMO number or MMSI number, etc.)

8.2 Service definition and discoverability

No.	Ref. needs	Need	Notes
SD#1	AC#6, STM #4, MS#9, MS#16, COM#1, PR#1	The infrastructure should provide a Service Registry / lookup function	
SD#2	ESea#2, MS#9, Cert#1, Cert#2	A standardized description of a digital service should include a functional description, user presentation issues (where relevant), operational context and definition of data formats	Geographic context and level of criticality of a service could be part of the operational context
SD#3	STM #10	A standardized service description language could facilitate service implementation	
SD#4	MN#1, STM #3, ENSI#1	A standardized description of a digital service must describe how privacy of information is ensured, if confidential information is exchanged with the service	Technical as well as legal aspects must be covered including stating which national (or international) legislative regime cover the provider of the service
SD#6	COM#2	Standardized methods for setting up subscriptions to a service should be developed	

8.3 Seamless roaming

No.	Ref. needs	Need	Notes
SR#1	ESea#3, AC#1, STM #5, MS#2	Actors should be able to interact without using the same point-2-point radio link or the same satellite system (seamless roaming)	Seamless roaming - i.e. a carrier agnostic or cross carrier communication service - should be available (The proposed Maritime Messaging Service) This will require a shipboard messaging application, which can offer other shipboard applications a connection to a shore based messaging service, while automatically switching between a

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

			number of different communication links, based on availability, capacity, cost or other parameters
SR#2	ESea#4, AC#2, STM #5, MS#3, NW#2	A Messaging Service should support the capability to broadcast information to actors inside an area (or actors subscribing to information in an area or along a route)	Geocasting (broadcasting to an area) will require the roaming service to be aware of mobile actors location or the 'listening area' of fixed actors Precision and timing requirements for updating the location of mobile actors has not been determined
SR#3	STM #5, MISC#1	Support for setting up dynamic multicast groups for multicasting information only to actors related to a particular operation is requested	(like subscribing to a chat room for sharing certain operational information related to an operation)
SR#4	MS#5, MS#6	Although not part of the GMDSS, any roaming capability should be designed to support the operational priorities defined for GMDSS (Distress, Urgency, Safety, Routine) in executing queues of information transfer	Based on advice from the High Level User Group, the infrastructure functions should *not* initially aim for supporting safety critical applications, but its inherent design should not prevent upgrading the operational status at a later stage, if the functions prove successful and become widely used.
SR#5	STM #11, MS#11, MS#12	A Messaging Service should support requesting acknowledge of information delivery	Acknowledge mechanisms could exist at different levels - a communication link level acknowledge of information delivery, an application level acknowledge of information received at a relevant application, or a user acknowledge
SR#6	MS#12, NG911 #2	Legal implications of the components of a Messaging Service must be considered – including requirements in national or international law related to lawful interception.	
SR#7	SWS#1	A Messaging Service should support the ability to distribute messages to ships outside range of stable connectivity	May require store-and-forward queuing capabilities, and ability to provide 'delivery delayed' or 'not connected' statuses in relation to requirement for delivery acknowledge.
SR#8	ENSI#3	A Messaging Service should support methods for bandwidth efficient transfer of data	Efficient methods for encoding or compression of data should be applied In case of a temporarily lost connection during an ongoing transfer of a large data block, the process should be able to continue after a reconnect, rather than starting the transfer over.

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

SR#9	AC#7, STM #3, MS#14, ENSI#1, EM#1	A Messaging Service should support encryption for confidential transfer of data	
SR#10	STM #12,	A Messaging Service should support text messages with non-standardised content The text-chat function could be used to clarify other standardised	Standardized expressions, such as Maritime Standard Phrases, could be supported.

8.4 Miscellaneous

No.	Ref. needs	Need	Notes
MS#1	MISC#4	Introduction of the infrastructure should not require major modifications of existing systems	The infrastructure functions should rather allow a gradual transition towards better service designs, providing improved and unified access control mechanisms, enabling automation of interactions with minimal user attention
MS#2	Comments from HLUG	Introduction of the infrastructure should not introduce single points of failure, which may prevent interactions between maritime stakeholders due to disrupted operation	Infrastructure functions should as far as possible not require online access to centralized systems, but should be able to be replicated and function offline or in a decentralized manner
MS#3	NG911 #1	A business case for operating the infrastructure functions should be identified	Supported by comments from HLUG
MS#4	NG911 #2	Legal implications of establishing the infrastructure functions should be analysed and addressed	Supported by comments from HLUG
MS#5	NG911 #3, STM#10	The roadmap towards establishing infrastructure functions should include establishing test beds and developer forums, where technologies can be tested and validated, and allow room for agile adaptation of technology developments	HLUG also requested a roadmap
MS#6	NG911 #4, Cert#1	The level of criticality of the infrastructure functions must be defined	

8.5 Location service

Geographic location of ships has proven to be a valuable service for numerous applications, see for instance MS#8, MS#10 and MiO#1. Many such tracking services exist, LRIT is a specific example, other services based on collection of AIS data are well known, and many proprietary systems exist. The publication of collected AIS data has previously been condemned by the IMO, as the information is commercially sensitive, and should be kept confidential.

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

Noting that the request for a seamless roaming service (Maritime Messaging Service) includes the requirement for the capability to perform a 'logical broadcast' (multicast a message to actors in – or listening to – an area, but using different communication links); the knowledge of the location of mobile actors is needed. This offers an opportunity to develop a maritime tracking service, which could be made available to authorized stakeholders. This way the owner of a ships position – the ships' captain - could nominate a number of permanent or temporary collaborators, who are allowed to access or subscribe to position updates. This service could be considered an implementation of the LRIT function, if integrated with the International LRIT Data exchange, and thus there exists an opportunity to apply the business model as well as the role based access scheme (the data distribution plan) for the LRIT service as part of realizing a business case for establishing and operating the 'Maritime Cloud'.

The primary requirement related to such a service, would be to safeguard the privacy of a mobile actors' position information, and only reveal it to authorized collaborators or actors representing a legal role entitled to access this information, such as SAR authorities.

8.6 Cyber Security

While neither the use cases gathered - nor the reports studied - are specific in requirements related to Cyber Security, it is noted by several use cases, and emphasized by the High Level User Group, that Cyber Security threats are of significant concern and should be addressed.

It is noted, that disruption of infrastructure functions due to hacking or other types of cyber-attacks could affect a large population of users, and thus such services should be protected against Cyber Security risks. The level of protection should be at least equivalent to the level of protection required for those systems that depend on the infrastructural functions. Further, it is noted that good practice guidelines are under development by major industry stakeholders (such as EfficienSea 2 partner nos. 14 and 15, BIMCO and CIRM), and such guidelines should be taken into consideration.

As a general observation it is of particular importance, that 'key management' for access control can be a complex task, regardless of whether physical or digital keys are at stake. It is recommended that Human Centred Design principles are observed, and that levels of access control chosen that are relevant for any given purpose, in order to avoid complicated or unnecessary login procedures creating additional barriers or complexities to users in performing their daily work. Otherwise widespread 'workarounds' such as password lists being taped to workstation keyboards because complex passwords are too difficult to remember, will reduce security rather than improve it.

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

9 Conclusions

The needs collected from various preliminary use cases within the project and from external sources should be prioritized and further qualified within the EfficienSea 2 project in the coming process of defining the conceptual model for the Maritime Cloud and creating a technical specification.

An important part of this process will be to establish consensus within the project on which functions are realistic to complete within the project, and which functions to consider outside the realistic scope of this project.

The needs collected are primarily point towards strengthening the capability to

- Uniquely identify and validate the identity of entities that need to interact
- The ability to ensure integrity and in some cases confidentiality related to information transfer
- Define standardized information services, and provide mechanisms to discover the availability of such services
- Support seamless roaming – automatic transport of information regardless not dependant on single communication links or communication service providers
- Address cyber security

Apart from needs that relate to functions within an enabling infrastructure, the collected information indicates a strong need for identifying a possible business case for establishing and operating such functions. A roadmap for a potential evolution of the Maritime Cloud is requested, including identification of how governance structures and legal implications can be addressed.

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

10 References

[IMO SIP]: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/eNavigation.aspx

[MarNIS_final_report]: http://www.transport-research.info/Upload/Documents/201007/20100726_145227_7963_Marnis%20final%20report.pdf

[MarNIS D2.2.C-1] "Research report on broadband applications- Part1: State of the art":

http://freepdfs.net/deliverable-reference-number-d22c-1-research-report-on/3fe53eb7469c35b4e0223c8f08d5155f/

[MarNIS D-HA3F]: "Final report on the MarNIS e-maritime architecture":

http://www.mits-forum.org/resources/D-HA3F_marnis.pdf

[ESea]: http://efficiensea.org/default.asp

[ACCSEAS]: http://www.accseas.eu/index.html#sthash.NYDYXHI3.dpuf

[ACCSEAS MC] : http://www.accseas.eu/content/download/8217/74329/Service%2520Description%2520-%2520Maritime%2520Cloud%2520v1.pdf

[ACCSEAS Architecture]:

http://www.accseas.eu/content/download/8198/74171/ACCSEAS%2520e-Navigation%2520Architecture%2520Report%2520v1.pdf

[MonaLisa_2.0]: http://www.sjofartsverket.se/en/monalisa/monalisa-20/

[STM_validation_project]:

http://monalisaproject.eu/eu-grants-e21-million-to-new-sea-traffic-management-validation-project/

[FLAGSHIP]: https://ec.europa.eu/research/transport/projects/article_5014_en.html

[FLAGSHIP D-D1.3]: http://www.flagship.be/media/1138/deliverable_-_d1_3.pdf

[Comms_for_enav] : http://www.mits-forum.org/resources/efforts-enav-com-v22.pdf

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

[ENSI]: http://www.sjofartsverket.se/pages/46466/2014%20Finland%20ENSI.pdf

and http://www.lvm.fi/c/document_library/get_file?folderId=2460605&name=DLFE-19838.pdf&title=Efficient%20Traffic%20Management%20-%20Cooperation%20across%20borders

NG911 - 1] Moore, Linda K.: Emergency Communications: Broadband and the Future of 911, CRS Report for Congress, December 22, 2010.

[NG911 - 2] National Emergency Number Association (NENA): Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3. September 30, 2010.

[NG911 - 3] J. Rosenberg and H. Schulzrinne and G. Camarillo and A. Johnston and J. Peterson and R. Sparks and M. Handley and E. Schooler: SIP - Session Initiation Protocol. RFC 3261, 2002.

[NG911 - 4] H. Schulzrinne: Location-to-URL Mapping Architecture and Framework. RFC 5582, 2009.

[NG911 - 5] T. Hardie, A. Newton, H. Schulzrinne, H. Tschofenig: LoST: A Location-to-Service Translation Protocol. RFC 5222, 2008.

[NG911 - 6] H. Schulzrinne, H. Tschofenig: LoST: Synchronizing Service Boundaries and <mapping> Elements Based on the Location-to-Service Translation (LoST) Protocol. RFC 6739, 2012.

[NG911 - 7] European Emergency Number Association, http://www.eena.org , 2015

[NG911 - 8] National Emergency Number Association, http://www.nena.org , 2015

[NG911 - 9] EC, M/493 Standardization mandate to the European Standards Organisations (ESO) in support of the Location Enhanced Emergency Call Service, http://www.etsi.org/images/files/ECMandates/m493.pdf

[NG911 - 10] Functional architecture to support European requirements on emergency caller location determination and transport, http://www.etsi.org/deliver/etsi_es/203100_203199/203178/01.00.00_50/es_203178v010000m.pdf

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