D5.4 Online test of ship data transfer

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: 31.10.2017

Organisation in charge of deliverable: BIMCO
### 1 Document status

#### 1.1 Authors

<table>
<thead>
<tr>
<th>Name</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jeppe Skovbakke Juhl</td>
<td>BIMCO</td>
</tr>
<tr>
<td>Peter Krog-Meyer</td>
<td>Danish Maritime Authority</td>
</tr>
</tbody>
</table>

#### 1.2 Document history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Initials</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>15.09.2017</td>
<td>JSJ</td>
<td>Initial version</td>
</tr>
<tr>
<td>0.2</td>
<td>26.09.2017</td>
<td>JSJ</td>
<td>Draft for final review</td>
</tr>
<tr>
<td>0.5</td>
<td>27.09.2017</td>
<td>JSJ</td>
<td>Version including comments</td>
</tr>
<tr>
<td>1.0</td>
<td>27.09.2017</td>
<td>JSJ</td>
<td>Final delivery</td>
</tr>
</tbody>
</table>

#### 1.3 External review group

<table>
<thead>
<tr>
<th>Name</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ole A. Jensen (Partner, Senior Consultant)</td>
<td>SeaSolutions</td>
</tr>
<tr>
<td>Morten Larsen (Project Manager)</td>
<td>Gatehouse</td>
</tr>
<tr>
<td>Anders Rydlinger (Director)</td>
<td>TRANSAS</td>
</tr>
</tbody>
</table>

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

1 Document status ............................................................................................................... 2
  1.1 Authors ....................................................................................................................... 2
  1.2 Document history ........................................................................................................ 2
  1.3 External review group ................................................................................................. 2

2 Introduction ....................................................................................................................... 4
  2.1 E2 Work Package 5 – Administrative burdens and exhaust emissions ...................... 4
  2.2 Scope of the WP5 e-solution on information exchange .............................................. 5

3 The online test based on the concept ............................................................................. 10
  3.1 The ship’s IT management system ........................................................................... 11
  3.2 The authority’s IT platform ........................................................................................ 11
  3.3 The service provider’s system .................................................................................. 12
  3.4 The maritime connectivity platform ........................................................................... 12

4 Specific test setup for the WP5 solution ......................................................................... 14
  4.1 Identity Management and Security ........................................................................... 15
  4.2 The ship’s IT management system ........................................................................... 16
  4.3 SafeSeaNet.dk’s IT platform ..................................................................................... 19
  4.4 The BIMCO port database system ............................................................................ 21
  4.5 The APR developed in WP5 ..................................................................................... 23

5 Connecting the “machines” in the M2M solution ............................................................. 26
  5.1 System architecture .................................................................................................. 26

6 Status of the online test of the system ............................................................................ 29

7 References ..................................................................................................................... 30

8 Acronyms ........................................................................................................................ 31
  8.1 Acronyms .................................................................................................................. 31

Appendix A List of data elements ID used in the online test .............................................. 32
2 Introduction

The EfficienSea2 (E2) project aims at creating and implementing smart solutions for efficient, safe and sustainable traffic at sea through improved connectivity for ships. This is achieved by global collaboration between various stakeholders, use of open-source software and an explicit aim for standardised solutions.

2.1 E2 Work Package 5 - Administrative burdens and exhaust emissions

The focus of WP5 is the delivery of new e-solutions related to two important challenges: Reduction of administrative burdens and monitoring exhaust emissions:

- The aim is to develop, test and, where possible, implement administrative e-maritime solutions for automated transfer of information (reporting) to and from ports and for transferring port information from the port to the ship and other maritime stakeholders.
- The aim is to develop solutions for monitoring emissions with focus on SOX and to conduct validation trials in the Baltic Sea Region.

The two e-solutions are developed in parallel tracks.

WP5 is divided into 3 subtasks, of which ST5.1 and ST5.2 address solutions for reducing the administrative burdens imposed on seafarers. Subtask 5.3 is about regulatory limitations of the SOX content of ships’ exhaust gas.

This report has been prepared by the members of WP5 and consider the exchange of information between ship and shore in relation to port calls, referring to subtasks 5.1 and 5.2.

The general aim of the work in E2, WP5, is not to deploy sophisticated e-solutions, but to use readily available solutions under the current framework of e-navigation. The e-solution builds upon a “new common port database and structure” that relies on the distribution of information storage among many sources. The use of a so-called machine-to-machine concept (M2M) will allow users in both “ends” to use already established software platforms bound together through a common and unified registry – developed by WP5. Such a solution will benefit and be acceptable for most stakeholders as, initially, no new technology and equipment will need to be purchased when the e-solutions are implemented.

The first deliverable of WP5 described in detail the concept and structure of the E2 proposed e-solution. This report, D5.3, Development of a new common port database concept and structure, was delivered in M10, February 2016.

The second deliverable explained in detail the Draft S-100 product specification, D5.1. This report was delivered in M21, January 2017, and explains the technical service and product specification associated with the e-solution.

The current report, D5.4, provides a brief status on the online test of ship data transfer. The tests are ongoing and will be fully reported in later deliverables under WP5.
The two remaining deliverables from this work package/subtasks (D5.2 and D5.5) are all due in January 2018 and February 2018. The two reports will describe the final tests and also provide conclusions with regard to the reduction of administrative burdens associated with use of the E2 e-solution.

2.2 Scope of the WP5 e-solution on information exchange

Deliverable D5.3 established a number of scenarios and tasked the E2 established High Level User Group to perform a cost benefit assessment taking into account a prioritization of the scenarios. Two scenarios were selected. As they are key to the understanding of the objectives of the concept (D5.1), they are briefly described below.

The first scenario described a service-oriented solution proposed for reducing the administrative burden imposed on seafarers. This solution allows the ship (and/or the agent) to use a service provider to compile accurate port documents. There are many ways to implement this, and one could be making ICT tools (Information and communications technology) available for use on board and by shore-based personnel to generate the necessary reports.

The solution stipulates that the compilation of these port documents is based on templates for port documents (comprising also pre-arrival and post-departure documents) issued by the port with its port actors. Such a solution would also cater for the different types of information necessary, given that the shipowner/operator provides access to diverse dimensions of voyage information. The information can be stored either on board, at the shipping company (information owner) or at different associated information storages pointed out by the information owner. The latter could be the service provider having a service in the cloud.

The information being handled directly by the information provider and at other (distributed) sources is to be seen as a “closed entity”.

This also means that the same data would be re-used as a source for compiling port-specific reports. It is also to be acknowledged that this solution provides flexibility in terms of whether the shipping company (or the agent) has interaction with the service providers. In figure 1 below the service interaction logic is depicted.
This solution also makes it possible to forward the “signed” reports in digital format into the National Single Window (NSW) database after having been signed-off by e.g. the ship’s master. This is already in place for a few countries, especially in Europe. Most other countries still require prints of at least PDF reports, whereas some countries allow for electronic submission of XML, spreadsheet, CSV or MS Word.

The IMO cannot dictate what reports/information need to be submitted and in what form. Even countries that are Party to the IMO FAL agreements require additional reports or additional information to be submitted on top of what is already in the FAL documents. Such additional reports are often required by local rather than national shore-based authorities. This means that any solution will need to accommodate (and streamline) submission of hard copy reports to reduce the burdens imposed on the mariner.

Electronic signatures would be introduced, avoiding the need for reports to be printed on paper before being signed. Electronic signatures will make written signatures superfluous. In figure 1 above, it is taken for granted that signed reports are submitted by the service
provider (e.g. hosting a one-stop document submission service), but the ship and/or agent could also submit the report directly to NSW on behalf of the owner.

The second scenario related to the fact that, in order to ensure that the port call is as smooth as possible, with minimal waiting times, high efficiency, optimal resource utilisation, and a fast turnaround time, situational awareness needs to be provided for. Building on the concept of Port Collaborative Decision Making (PortCDM), as part of the Sea Traffic Management (STM) concept, as proposed by MONALISA 2.0¹, PortCDM services are proposed to be used as a basis for the agent and other port actors to enable a well-coordinated port call.

Time-related port call information is one important source of information that is necessary for creating a basis for settling contracts and ensuring a smooth and efficient port call.

PortCDM provides information services enabling actors involved in port calls to share real-time data from different information sources for the purpose of enhanced coordination. The data concern time-related port information about different actors’ estimates of when a particular event is about to occur and the actual occurrence of that event.

The information is aggregated into an understanding of the situational awareness, enabling different actors to optimally plan and carry out upcoming operations. PortCDM is a concept facilitating digital collaboration among actors operating in and around the port as well as digital collaboration between the ship and the port as a hub. PortCDM could therefore be used for monitoring port calls from the moment they are declared and for recording states that are planned for.

By enabling port operators to collaborate and thereby provide the information required as regards planning, decision-making and execution, the proactive communication between the stakeholders will be eased. The PortCDM concept builds upon instant information sharing, giving all actors the same picture based on the information derived from different systems (including NSW) used by different operators, thereby reducing the burden imposed on the agent and giving him/her a more strategic and monitoring role.

In figure 2 below, PortCDM is depicted as a service-oriented solution allowing service providers to provide the PortCDM (compliant) services consumed by the different actors associated with the port call. These PortCDM services are complemented by services for sharing other types of information as well, thus enabling the port visit to be agreed upon and performed according to expectations.

¹ PortCDM Concept Description, MONALISA 2.0 – D2.3.1-4.4, 2015;
PortCDM Validation Report, MONALISA 2.0 – D2.7.1, 2015;
STM – The Target Concept, MONALISA 2.0 – D2.3.1, 2015.
Collectively, the two scenarios give rise to an architecture that connects service providers and service consumers in a peer-to-peer realisation of services where different information sources and information services are exposed, discovered, and consumed. In a fully implemented electronic reporting system, ships (possibly assisted by shore-based shipping company personnel and/or port agents) update their reporting information in a cloud or service provider based Common Maritime Data Structure (CMDS). Ship owners/operators expose parts of the information in CMDS to duly authenticated and authorised shore-based authorities. Shore-based authorities that are duly authenticated and authorised will be allowed to subscribe to “consume” the reporting service the ship provides.

Service consumers, service providers, and information owners need to be authenticated. Empowerment by a framework of maritime service infrastructure by building on the MCP components (especially the Identity Registry and the Service Registry) is proposed for meeting these challenges, taking into account secure information sharing among the parties involved. In principle, this means that the architecture should build upon the components depicted in figure 3 below.
Figure 3: Basic foundation for a service-oriented architecture building on the Maritime Connectivity Platform (MCP)

Figure 3 above also indicates the need to ensure standardised interfaces, connectors, for information owners providing data for service consumption – and a harmonized data element structure to ensure smooth exchange of information.
3 The online test based on the concept

In this report, we describe the testing of the ship data transfer when exchanging data between ship and shore enabling widespread use of computers instead of manually entering the same data again and again. The concept builds on the simplest machine-2-machine test case, described in the following chapters.

If the information to be exchanged is harmonized, structured and modelled in accordance with the service specification as described in D5.1, the exchange can – to a large extent – be handled by computers on the ship and ashore.

The concept is described in figure 4 below.

The concept consists of four main elements:

- The ship, the shipowner and his IT management system (to the right)
- The authority, the Maritime Single Window (MSW) and SafeSeaNet (SSN) and its IT platform (to the upper left)
- The provider of a service, in this case it is the BIMCO port database (at the bottom)
- The Maritime Connectivity Platform (MCP), formerly known as the Maritime Cloud (in the centre).

All connected in a simple M2M solution.
3.1 The ship’s IT management system
Most ships, if not all, have to some extent an IT management system on board, which holds the abundance of information required to operate the ship. This is normally established through an administrative software tool, often set out as a stand-alone computer. But a fully connected link to the shipowner’s office ashore (or similarly, to that of the ship manager) is becoming more and more frequent as the connectivity costs are getting lower (see also chapter 5).

The WP5 concept requires that the ship’s IT management system is structured in such a manner that all the data elements available have their own identification – associated with a so-called data element ID. This structure is well-described in the E2 D5.1 report.

The data element ID (e.g. the given name of the captain or his rank or telephone number of the pilot) will ensure that the data element can be exchanged/submitted individually. Drop by drop, the total amount of information will be exchanged.

Only “approved” data elements are exchanged. The actually supported/”allowed” data elements can be queried and listed by the local authority, making the ship aware of the requirements for calling at the port. If the data are not available in the management system (e.g. the colour of the ship), the element becomes highlighted. In such case, the captain can add the information manually and store it for later use.

This feature is solved through a supplied information checklist. The master on board the ship can then check and control which information to submit. He will thereby approve – and sign off – that the information exchanged with the stakeholders is correct.

3.2 The authority’s IT platform
At the other end of the M2M solution is the authority’s IT platform. This may vary as not all systems and platforms are the same.

At the 40th session of the IMO Facilitation Committee (FAL 40) in 2016, amendments were adopted to the FAL Convention. The amendments set out new mandatory requirements for electronic data interchange requiring public authorities to establish systems for the electronic exchange of information to assist ship clearance processes. The amendments will enter into force in the spring of 2019.

Following these amendments, FAL 41 discussed how to develop and implement such an interchange system, taking into account that some countries already now have so-called Maritime Single Windows (MSW) in place. The questions were whether a prototype of MSW should be established by reusing one of the existing systems and/or parts of such systems, or whether a completely new prototype (provided by the IMO) should be developed, taking
into account the experience of other MSW systems, or as a third option, whether nothing should be done, thereby allowing MSWs to be implemented without further coordination.

FAL 41 felt constrained from giving full support to any of the options presented because of a lack of information about the scope and plans, as well as budget and resource implications. But most attendees were of the view that MSWs should be permitted to be implemented without any further coordination. (Although the final decision is to be taken at the FAL meeting to be held in 2018, this is unfortunately a likely outcome).

FAL 41, however, agreed to develop new guidelines for setting up single window systems, and to develop guidance on authentication, integrity and confidentiality for the exchange of electronic information.

The 2019 scenario taken to the extreme may well be that shipping will have to report to more than 100 different MSWs which may have a similar number of IT platforms. Therefore, it is of the utmost importance to ensure a certain harmonization and standardization of the reporting to public authorities prior to port calls. Though the MSWs may differ, the electronic data interchange should use the same data models to ensure that all ships can make use of the same APIs.

The E2 WP5 solution developed should take account of that – should the IMO Parties to the FAL Convention decide to adopt the framework as described in detail in D5.1.

3.3 The service provider’s system
It is foreseen that any service provider can register its services at the MCP. The service provider can thereby offer a large variety of services from waste collection services, bunker services, and spare part services to weather, routing, satellite communication, and delivery of port information.

The many service providers will have to register with the MCP by offering their services for a certain geographical area/region. At the same time, some may offer their services if agreements or licences have been agreed upon, e.g. TRANSAS could offer ships using their systems one particular solution, whereas ships without the TRANSAS system on board may have to pay for the same service or have a reduced service. All this is well-described in D5.3.

For the proof of concept, we have made use of the BIMCO world port database, which is explained in a later chapter.

3.4 The maritime connectivity platform
The Maritime Connectivity Platform holds the identity management and authentication of the users.
Authentication includes any process by which a system verifies the identity of a user (human or machine) wishing to access it. Since access control is normally based on the identity of the user requesting access to a resource, authentication is essential to effective security. In contrast to identification, which refers to the act of stating a person or thing's identity, authentication is the process of actually confirming that stated identity. It might involve verifying the authenticity of a website by a digital certificate that it provides or validating a person’s identity documents.

Service registry, identity management and issuing of authentication certificates are currently controlled by the MCP. These elements are currently being tested with success within the projects EfficienSea2, STM and SMART navigation.

Following the service oriented architecture of the MCP, the alignment and integration of those elements between the different projects are established using common web service technologies. More information can be accessed by interested stakeholders on http://efficiensea2.org/solution/maritime-connectivity-platform.
4 Specific test setup for the WP5 solution

In chapter 3 we described the WP5 solution concept. In this chapter, we describe the individual elements used in the online test.

A simplified description of the setup is illustrated below in figure 5.

The figure 5 above shows that a number of APIs can be offered through the MCP; however, the WP5 test case considers only the “green” API.

In the following, the E2 WP5 API is called Automatic Port Reporting Demonstrator (APR).

The WP5 prototype applies the following scenario:

- A request message is sent from the SHIP API to the APR asking for a list of reporting formalities for a given port (pre-arrival documents and departure documents). This is done by entering the UNLOCODE for the port.
- The APR requests this information from the NSW API and/or PORT API.
- The APR also requests the BIMCO API whether information on this port is available.
- The NSW and PORT APIs return a list of data element IDs covering the information they want to receive.
- The BIMCO API returns information about what can be provided as part of the membership.
- The APR returns a list of port data elements to the SHIP API.
- The APR returns a reporting requirement list to the SHIP API.
• The SHIP prepares the required information from its management system, and following the Captain’s approval, the information is transmitted to the APR for distribution.
• The APR distributes the information to the NSW and PORT APIs.
• The APR validates that the information has been delivered and sends an acknowledgement to the SHIP API.
• The ship has now submitted its information and is cleared for calling at the port.

Obviously, this description is somewhat simplified, but it includes the relevant steps of the data transmission.

4.1 Identity Management and Security
The overall goal is that, if the exchange of data is done automatically, the sender and receiver of the data have to make sure that they are the only parties in the process having access to the information. Therefore, identity management is key to success. This is an area that deals with identifying individuals such as users, devices and computer systems and controlling their access to resources within some kind of organizational context such as a private company, a country, or a whole industry.

Computer security is the protection of information systems against theft, disruption or misdirection of the hardware, software, and information stored in these systems.

The identity of a ship is often addressed in terms of a ship’s name and IMO number. On communication systems, the identity of a ship may be a call sign, MMSI number or system specific terminal number. These identifiers are, however, just numbers – and there is no guarantee that a signal identified by a specific call sign or MMSI number corresponds correctly to a unique ship. Also, none of these identity systems or registers takes account of the need to deal with actors that are not ships and do not necessarily have their own radio station, such as ship owners, ship agents or service providers.

The lack of a global digital identity of users/vessels/systems is a serious bottleneck in starting a digital maritime evolution across different companies and individuals. Just like human to human communication on a worldwide scale would be impossible without having global unique telephone numbers/email addresses. The same may be the case when trying to integrate maritime systems on a global scale without a globally agreed upon concept of a digital maritime identity for all the various participating actors.

In order to alleviate this problem and to address other issues that require confidentiality and integrity, the MCP provides a Maritime Identity Registry (MIR). This registry provides an overview of managed identities of organizations, users, devices and systems that need to communicate with each other in some way. There is no requirement for the communication to
take place over MCP services such as the Maritime Messaging Service. The registry can be integrated with any form of external information carrier using standard security protocols.

The registry allows for managed human users to only need a single identity (password/certificate) that can be used across many maritime systems. While username/password is the initial focus, future versions will also support biometrics (fingerprints, etc.) or devices (cell phones, smart cards) to be used for authentication of users, as well as combinations of these into multi-factor security.

The identity registry also supports a public key infrastructure in order to provide digital certificates and support confidentiality through encryption. This is primarily used for machine to machine communication. For example, you can install a digital certificate on a ship or a shore-based station that will encrypt any message (if the communication protocol supports it) transmitted. Encrypted messages can then be decrypted only by intended recipients.

This infrastructure function also allows human actors to digitally sign messages or documents. Making sure that nobody has tampered with the contents of important documents is a mechanism that will allow other users or systems to validate messages for authenticity and integrity later on.

Another core functionality provided by the Identity Registry is the support for federated identity management. Most organizations that will use the MCP will already have their own Identity Management Systems managed by their IT departments. Since managing private and highly confidential data is a sensitive topic, handing over the Identity Management to a third party will not be possible for most organizations. Instead the MCP allows for integration with existing identity management systems in order to “reuse” the identities already set up internally in an organization.

Security aspects may also require addressing less tangible issues such as recommendations and guidelines on privacy or confidentiality of information shared, in order to facilitate provision of information services. For example, many potential services could be location-based. Locations might be considered sensitive, for example, when sailing in pirate-infested waters, or simply for reasons of privacy. Hence, it makes sense to provide (strict) guidelines for service providers’ handling of information about clients’ positions or other information shared between providers and consumers of services, since it is impossible to provide centralized control.

These important issues are duly taken care of in the E2 project through the MCP. The online test of the ship data transfer.

4.2 The ship’s IT management system
For the proof of concept, WP5 have teamed up with a global provider of specialized maritime IT solutions and services in order to get a correct baseline of the setup. The service provider,
SeaSolutions, has more than 25 years of experience within core shipping business areas, with its headquarters in Copenhagen and with offices in India and Malaysia. Providing software for more than 25 global shipowners and 800 ships, SeaSolutions was the best match for the test case.

As part of the test, WP5 got access to a test version of the SeaSolutions software whereby we could build the connection to the APR. SeaSolutions generously offered to develop a special interface for connecting through the MCP.

For the sake of testing, we had developed a data element ID list comprising 35 data elements only. This is set out in Annex A to this report. The data element ID list may be further extended later in the test phase.

The below figure 6 shows screen dumps from the SeaSolutions software system. The red markings refer to the comments found under the figure.

![Figure 6: Screen dumps from the ship IT management system](image-url)
Ref. 1

Many of the data relevant for the obligation to report to the local authority are already available in the management system because they are necessary for the operation of the ship.

Some of the data elements may be dynamic and change over time; while some are static by nature. For example, the next port of call, crew lists, and cargo lists are dynamic and change frequently, whereas port information such as pilot boarding areas, the ship’s IMO number or the registry number are more static. In any case, required details related to the individual data elements will have to be applied in a structured standard to facilitate a global trustworthy and agile exchange of information.

“Static” data are often added to the system upon delivery of the ship from the shipyard as they are (almost) never changed. “Dynamic” data may be updated either by the master on board or the shipowner or agent.

Ref. 2

When the ship “asks” for information about a given port, it will receive information about the requirements for information to be exchanged before being given clearance to the port.

The information will include, e.g.:

- General name of the data element
- Definition, describing the information
- The format of the data element to be submitted
- When to submit the information prior to the port call
- Data element ID.

The information is updated by the port itself when making the service registration in the MCP.

Ref. 3

This folder contains three different data fields: the black, the grey and the italic data fields. The black field contains information required by the authority (mandatory), and the grey field contains data elements not required to call at the port (voluntary). The italic data field, however, requires data to be added, as the information is not available in the ship’s IT management system.

In this case, the “Air Draft” is not provided for in the ship data list and, thus, the master has to add this information manually.
4.3 SafeSeaNet.dk’s IT platform
SafeSeaNet (SSN) is the vessel traffic monitoring and information system established in order to enhance:

- Maritime safety
- Port and maritime security
- Marine environment protection
- Efficiency of maritime traffic and maritime transport.

It has been set up as a network for maritime data exchange, linking together maritime authorities across Europe. It enables its stakeholders to provide and receive information on ships, ship movements, and hazardous cargoes. The main information elements contained in the SSN system and made available to licensed users are, inter alia, the following:

- Identification name and numbers, flag, dimensions, course, speed, dimensions, destination and ship type
- Estimated/actual times of arrival/departure
- Details of hazardous goods carried on board
- Information on safety-related incidents affecting ships
- Information on pollution-related incidents affecting ships
- Details of waste carried on board/to be offloaded
- Ship security-related information.

The information is used for many different purposes and distributed to many different stakeholders depending on their access rights.

The below figure 7 shows screen dumps from the SNN platform. The red markings refer to the comments under the picture.
The ship will submit information to the SSN about the estimated time of arrival. The necessity of this information is due to the new inspection regime for Port State Control. Those involved in ship inspections need to look at specific ships when they enter their ports. SafeSeaNet provides 72 hours, and 24 hours early warning information on specific ships’ arrival, as well as the actual time of arrival and departure. This progressively enables port State control officers to improve their planning.

The information could, however, easily be further expanded if the Port Collaborative Decision Making (PortCDM) is taken on board as part of the Sea Traffic Management (STM) concept (described in chapter 2.2).

Waste and garbage on board the ship must be discharged to reception facilities ashore in order not to pollute the oceans.

The ship therefore keeps record according to its mandatory garbage management plan. Such a plan comprises written procedures for collecting, storing, processing, and disposing of garbage generated on board ship as per regulations provided in Annex V of MARPOL.

The port is responsible for the operation of the individual terminals, piers and other port service businesses when it comes to ensuring the availability of proper reception facilities.
Waste notifications sent by ships to port/coastal authorities identify the types and quantities of waste and cargo residues being carried, and this enables more efficient waste disposal when ships are in port and; better management of pollutants, should they have accidents. It also provides useful information on pollutants that could potentially be illegally discharged, and thus acts as an additional pollution deterrent.

All this information is already stored in the garbage record management plan, and is therefore readily available through the ship’s IT management system. Each entity in the garbage record management plan has been assigned its own data element ID to ensure correct exchange.

Ref.6

Security is another important information item required by the authority. It is registered in order to be prepared to face threats of intentional unlawful acts such as acts of terrorism, acts of piracy or similar at all times. Much of this information, if not all of it is already stored on board.

In connection with the carriage of goods containing especially dangerous substances, such as chemical and radioactive substances, the potential consequences of any threats posed by intentional unlawful acts and the environment are very serious. In order to improve security prior to port arrival, ships provide advance notifications to SafeSeaNet with information concerning: their international ship security certificates; the levels of safety at which they operate and have previously operated, etc.

4.4 The BIMCO port database system

The BIMCO world port database currently holds information about more than 1500 ports. The information in the database consists of information provided by the port itself, which is being updated regularly.

Figure 8 below contains a screen dump from the BIMCO website showing some of the information available in the world port database. The red markings refer to the comments under the picture.
In the BIMCO world port database, one of the pieces of information most frequently searched for is the port’s working hours. This information is relevant for the shipowner when planning the operation. To avoid paying extra for the discharge of the cargo, the operator will seek to discharge the cargo during normal working hours.

For the online test, we have re-structured the information on the BIMCO port database in order to follow the data model standard.
The below figure 9 shows a screen dump from the API requesting certain port information. The red markings refer to the comments under the picture.

![API Request Screen Dump](image)

**Figure 9: Screen dump from the service provider API, the BIMCO world port database**

Ref.8

The API is requesting the specific port information by use of the data element ID: PortWorkingHours, in 2017, for Port of Aarhus (UNLOCODE: DKAAR).

Ref.9

The call is replied immediately, showing the relevant information regarding the working hours of the port of Aarhus, in 2017. This information will now be passed to the ship/shipowner’s IT management platform in order for a qualified decision to be taken when considering whether the Port of Aarhus would be the proper port in which to discharge the cargo.

4.5 The APR developed in WP5

The MCP offers a number of web solutions, so-called Web Application Programming Interfaces (Web APIs). The automated port reporting demonstrator (APR) is such an API.
Web APIs are the defined interfaces through which interactions occur between an enterprise and applications that use its assets. An API approach is an architectural approach that revolves around providing programmable interfaces to a set of services to different applications serving different types of consumers.

When used in the context of web development, an API is typically defined as a set of Hypertext Transfer Protocol (HTTP) request messages, along with a definition of the structure of response messages, which is usually in an Extensible Markup Language (XML) or JavaScript Object Notation (JSON) format.

One example might be a shipping company API that can be added to an eCommerce-focused website to facilitate the ordering of shipping services and automatically include current shipping rates or details related to the port or operation in general, without the site developer having to enter the information into a web database. While "web API" has historically been virtually synonymous for web service, the recent trend has been to move away from Simple Object Access Protocol (SOAP) based web services and service-oriented architecture (SOA) towards more direct representational state transfer (REST) style web resources.

The API developed for the test case will use a REST interface. 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.

Within the E2 project, Work package 3 had early discussions on the pros and cons of various interface choices and there has been a strategic decision on HTTP/HTTPS based communication, where choices landed between SOAP and REST.

The conclusion was not to restrict MCP services that are REST based only. In fact, it is believed that a majority of the services developed will be REST based initially.

The WP5 interface uses a REST architectural form and, although it is not an international standard, it is widely used and likely to become the general standard in the near future. Interface/implementation has to live up to certain criteria before it can be called RESTfull.

The JavaScript Object Notation (JSON) language has been used to transmit the data.

The product specification and the data element ID list have been implemented and tested by creating sample data and used to convey information between the systems. Although the solution is based on machine-2-machine elements, it is necessary to develop front-end and
back-end software applications to allow users to convert existing information/data into the product specification format and read the transferred data into user systems.

More details about this will be issued in the coming report related to the development of the WP5 demonstrator, D5.2, which is due in M33, January 2018.
5 Connecting the “machines” in the M2M solution
Ship-to-shore and shore-to-ship connectivity is vital for smooth operation. Many ships have to consider issues like:

- Latency, e.g. due to the vessel being offline.
- Bandwidth, e.g. in some areas the transfer rate is very low.
- Poor/unstable connections.
- Prioritized traffic. You do not want to block more important data.
- Cost. It is still expensive to send data over satellites.

To a large extent ships have to rely on the communication suppliers and their software suits: services like data and fax, Internet and intranet, private communications, voice, e-mail, text messaging. However, e.g. when working with emails, ships are facing some challenges, as they are bounded by:

- Policies for
  - size
  - attachment types (even for compressed files)
  - blocked senders and receivers
- Spam filters
- Mailbox size (in some cases, you are not allowed to send mails if the mailbox is full)

Thus, file/data transfer is/has been a main issue, though also supporting and maintaining software on vessels with poor or non-existing connections is a topic in itself.

As part of the E2 project, partners have developed a hybrid communication system to provide access to several services offered via MCP. The main concept of the system is based on the assumption that connections are set up automatically using different radio interfaces, and the current interface is selected from those available by sophisticated algorithms taking into account a number of parameters, including user preferences. The following chapter describes the system architecture as well as its components and the relevant communication protocols. Additionally, the proposed concept of the MCP interface will be discussed. The selection of the most suitable radio link will be performed through Seamless Roaming mechanisms which will be introduced in the chapter “Seamless Roaming concept”.

5.1 System architecture
The architecture of the hybrid communication system is illustrated in figure 10.
The hybrid communication system is comprised of three main segments:

- The coastal segment
- The on-board segment
- The satellite segment.

**The coastal segment** covers the infrastructure of the radio networks, whose technical parameters and base stations’ locations enable communication between users at sea. In particular, this segment comprises:

- Cellular networks (2G, 3G, LTE)
- VDE-Terrestrial (work underway)
- Other (might potentially become part of the coastal segment):
  - WiMAX networks
  - Wi-Fi networks (in the vicinity of ports only – due to limited operating ranges of these networks).

**The satellite segment** covers satellite systems that successfully provide communication links in areas where terrestrial systems are unable to do so. In particular, this segment comprises:

- VDE-Satellite (work underway)
- Iridium
- Inmarsat.
It goes without saying that it is way beyond the scope of the EfficienSea 2 project to modify or alter coastal and satellite segments so the following section will mainly concentrate on the description of the off-shore (on-board) segment.

The on-board segment includes systems and interfaces installed on board the ship. Those systems and interfaces enable communication via coastal/satellite infrastructure and also direct ship-to-ship communication (on the condition that all involved ships are equipped with compatible interfaces and are sufficiently close to one another). It is assumed that direct communication can be carried out via a VDE Ship-to-Ship link or using WiFi networks at 2.45 GHz or 5 GHz.

This is well-described in the E2 delivery D2.7 describing Seamless roaming.

Seamless Roaming is a mechanism in which the most suitable (for the given service at the given time and place) radio link (interface) is selected from among all those available on the vessel. The main task of Seamless Roaming is constant monitoring of the available radio links and switching between them to ensure optimal (given the selected set of criteria) conditions for the required maritime services. The Seamless Roaming algorithm will also address user preferences, e.g. minimization of the transmission duration or minimization of transmission costs.
6 Status of the online test of the system

The current report describes an early online test of the ship data transfer. We have tested all the various components and are in the process of combining the full structure. Individually the components work, and the full setup seems very promising.

Deliverables D5.2, “Demonstration of prototype application for automated port reporting”, and D5.5, “Prototype database on online port data”, will make use of the information in this report and will, to a certain extent, act as proof of concept of the deliverable put forward in D5.3.

It is foreseen that the efforts made to implement this proof-of-concept service are few since many of the components necessary for the solutions are already in place or are being pursued by means of contemporary efforts. The only show-stopper is whether ships’ IT management systems and the National Single Window platform are willing to develop a front-and backend capable of gathering and displaying the data as described in the data model.
7 References

<table>
<thead>
<tr>
<th>No.</th>
<th>Version</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>2.0</td>
<td>Seamless Roaming</td>
</tr>
<tr>
<td>[2]</td>
<td>1.0</td>
<td>Development of a new common port database concept and structure</td>
</tr>
<tr>
<td>[3]</td>
<td>1.0</td>
<td>Draft 5-100 product specification</td>
</tr>
</tbody>
</table>
## 8 Acronyms

### 8.1 Acronyms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>APR</td>
<td>Automatic Port Reporting Demonstrator</td>
</tr>
<tr>
<td>CMDS</td>
<td>Common Maritime Data Structure</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>JSON</td>
<td>JavaScript Object Notation</td>
</tr>
<tr>
<td>MCP</td>
<td>Maritime Connectivity Platform</td>
</tr>
<tr>
<td>MRN</td>
<td>Maritime Resource Name</td>
</tr>
<tr>
<td>REST</td>
<td>Representational State Transfer</td>
</tr>
<tr>
<td>SOA</td>
<td>Service Oriented Architecture</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>XML</td>
<td>Extendible Mark-up Language</td>
</tr>
<tr>
<td>XSD</td>
<td>XML Schema Definition</td>
</tr>
</tbody>
</table>
## Appendix A  List of data elements ID used in the online test

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Type</th>
<th>Mandatory (Yes/No)</th>
<th>Subcategory</th>
<th>ID</th>
<th>Recommended (Yes/No)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

“*This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 636329*.”
<table>
<thead>
<tr>
<th>Group element name</th>
<th>Definition</th>
<th>Type</th>
<th>Document (fileName)</th>
<th>Mandatory information (server)</th>
<th>Submission schedule (before actual)</th>
<th>Data (FIPs relevant)</th>
<th>Business roles</th>
<th>Draft proposed data element ID (subject to change)</th>
<th>(FIPs-relevant)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N° of identity document</td>
<td>The type of document (e.g. national, passport or other type), identity card with a number of renewal or a statement otherwise indicated (e.g. card, identity card, etc.)</td>
<td>String</td>
<td>see &quot;Reference data&quot;, country of issue (if Country of issue of identity document)</td>
<td>e</td>
<td>32</td>
<td>(Date of end of validity between ADD620, invalid)</td>
<td>Person</td>
<td>Person/Name/Profile/Entity</td>
<td></td>
</tr>
<tr>
<td>N° of identity document</td>
<td>Preceding number of the specified document</td>
<td>String</td>
<td>see &quot;Reference data&quot;, country of issue (if Country of issue of identity document)</td>
<td>e</td>
<td>32</td>
<td>9999-xx-xx</td>
<td>Person</td>
<td>Person/Create/Document</td>
<td></td>
</tr>
<tr>
<td>Date of issue of identity document</td>
<td></td>
<td>String</td>
<td>see &quot;Reference data&quot;, country of issue (if Country of issue of identity document)</td>
<td>e</td>
<td>32</td>
<td>9999-xx-xx</td>
<td>Person</td>
<td>Person/Create/Document</td>
<td></td>
</tr>
<tr>
<td>Country of issue of identity document</td>
<td></td>
<td>String</td>
<td>see &quot;Reference data&quot;, country of issue (if Country of issue of identity document)</td>
<td>e</td>
<td>32</td>
<td>9999-xx-xx</td>
<td>Person</td>
<td>Person/Create/Document</td>
<td></td>
</tr>
<tr>
<td>Name of issuer entity</td>
<td></td>
<td>String</td>
<td>see &quot;Reference data&quot;, country of issue (if Country of issue of identity document)</td>
<td>e</td>
<td>32</td>
<td>9999-xx-xx</td>
<td>Person</td>
<td>Person/Create/Document</td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td></td>
<td>String</td>
<td>see &quot;Reference data&quot;, country of issue (if Country of issue of identity document)</td>
<td>e</td>
<td>32</td>
<td>9999-xx-xx</td>
<td>Person</td>
<td>Person/Create/Document</td>
<td></td>
</tr>
<tr>
<td>Visual identification feature</td>
<td>Visual feature or -Visual identification feature, as applicable</td>
<td>String</td>
<td>see &quot;Reference data&quot;, country of issue (if Country of issue of identity document)</td>
<td>e</td>
<td>32</td>
<td>9999-xx-xx</td>
<td>Person</td>
<td>Person/Create/Document</td>
<td></td>
</tr>
<tr>
<td>Partial photograph</td>
<td></td>
<td>String</td>
<td>see &quot;Reference data&quot;, country of issue (if Country of issue of identity document)</td>
<td>e</td>
<td>32</td>
<td>9999-xx-xx</td>
<td>Person</td>
<td>Person/Create/Document</td>
<td></td>
</tr>
<tr>
<td>Date of expiration</td>
<td></td>
<td>String</td>
<td>see &quot;Reference data&quot;, country of issue (if Country of issue of identity document)</td>
<td>e</td>
<td>32</td>
<td>9999-xx-xx</td>
<td>Person</td>
<td>Person/Create/Document</td>
<td></td>
</tr>
<tr>
<td>Partial encryption</td>
<td></td>
<td>String</td>
<td>see &quot;Reference data&quot;, country of issue (if Country of issue of identity document)</td>
<td>e</td>
<td>32</td>
<td>9999-xx-xx</td>
<td>Person</td>
<td>Person/Create/Document</td>
<td></td>
</tr>
<tr>
<td>Date of birth/issue</td>
<td></td>
<td>String</td>
<td>see &quot;Reference data&quot;, country of issue (if Country of issue of identity document)</td>
<td>e</td>
<td>32</td>
<td>9999-xx-xx</td>
<td>Person</td>
<td>Person/Create/Document</td>
<td></td>
</tr>
<tr>
<td>License to be issued</td>
<td></td>
<td>String</td>
<td>see &quot;Reference data&quot;, country of issue (if Country of issue of identity document)</td>
<td>e</td>
<td>32</td>
<td>9999-xx-xx</td>
<td>Person</td>
<td>Person/Create/Document</td>
<td></td>
</tr>
</tbody>
</table>

**EU logo:** European Union’s Horizon 2020 research and innovation programme, under grant agreement No 636329.