Service Description: Maritime Cloud

Issue: 1

Issue Status: Approved

Issue Date: 18/05/2015

Lead Author	Reviewer	Approved for Release
Name: Ole Bakman Borup	**Name:** Transnational Project Co-ordination Group	**Name: Project Steering Committee**
Job Title: WP6 Contributor	**Job Title:** N/A	**Job Title:** N/A
Partner: DMA	**Partner:** All	**Partner:** All
Signature: pp Alwyn I. Williams	**Signature: pp Alwyn I. Williams**	**Signature: pp Alwyn I. Williams**

Executive Summary

This document introduces The Maritime Cloud, a proposed technical framework enabling efficient, secure, reliable and 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. The framework has been introduced into the NSR as a common framework for the ACCSEAS project, supporting the ACCSEAS testbed, and possibly the future e-navigation implementation in the NSR.

Contents

Document Disclaimer

Document is uncontrolled when removed from iManage (either electronic or printed)

Document Information

Project Title	ACCSEAS
Work Package No.	6
Document Title	Service Description: Maritime Cloud
Description	This document describes the results of the efforts in developing the Maritime Cloud.
Date	18/05/2015
Lead Author	Ole Bakman Borup
Lead Author's Contact Information	c/o Mads Bentzen Billesø Søfartsstyrelsen / Danish Maritime Authority Maritime Analysis, Technology and Business Development (MAF), e-Navigation Telephone: +45 9137 6329 E-mail: MCB@dma.dk
Contributing Author(s)	WP6 Contributors
iManage Location	29922
Circulation	1. Client 2. Project Files (i-manage) 3. Transnational Project Co-ordination Group 4. Project Steering Committee
NSRP Secretariat Approval	~~Yes~~ / No

1 Introduction

This document introduces The Maritime Cloud, a proposed technical framework enabling efficient, secure, reliable and 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. The framework has been introduced into the NSR as a common framework for the ACCSEAS project, supporting the ACCSEAS testbed, and possibly the future e-navigation implementation in the NSR.

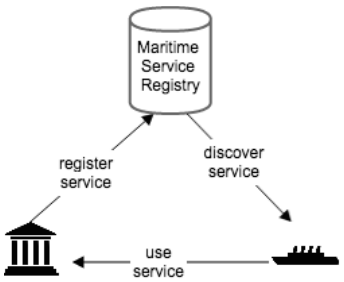
It may further provide a common reference framework for the adjacent Baltic Sea Region (BSR), thus allowing precise exchange of concepts between different EU projects like ACCSEAS, MONALISA 2 and their successors, and other European regions may benefit from its wider applicability.

1.1 Overview

The Maritime Cloud is a digital Information Technology (IT) framework consisting of standards, infrastructure and governance that facilitates secure interoperable information exchange between stakeholders in the maritime community by the principles of Service Oriented Architectures (SOA). The core of the Maritime Cloud consists of three key infrastructural components providing central framework services:

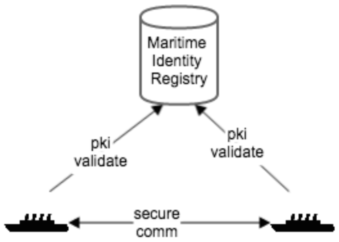
Maritime Service Portfolio Registry

Encounter point for those that consume, provide or specify services in the maritime domain. It enables service standardization, and automatic service provision and discovery.



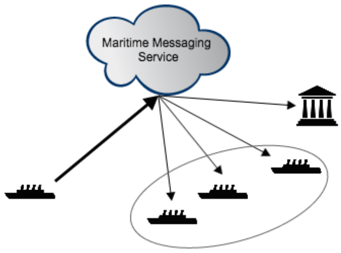
Maritime Identity Registry

Provides all maritime stakeholders with a basic *Maritime Identity* and basic methods for authentication, integrity and confidentiality in information transfer through the use of digital certificates in a Public-Key Infrastructure (PKI).



Maritime Messaging Service

Geo-aware *messaging service* taking into account the needs of ships in terms of achieving interoperability across varying data links with varying availability, technical characteristics and limited bandwidth. Allows *geo-casting*, a broadcasting method addressing receivers within a certain geographical area.



An important concept in the Maritime Cloud is the **Almanac**. It is an offline digital version of the public parts of Maritime Identity Registry and Maritime Service Portfolio Registry. It will function as a 'white pages/yellow pages phonebook' of registered maritime stakeholders and services, and allow offline use of central framework services like service discovery and secure communication.

1.2 Background

At the very core of the definition of e-navigation,

> *The harmonized collection, integration, exchange, presentation and analysis of marine information onboard and ashore by electronic means to enhance berth to berth navigation and related services for safety and security at sea and protection of the marine environment,*

lies the fundamental ability to ensure seamless transfer of information. The strategy for e-navigation in the report of IMO MSC85 (MSC 85-26-Add.1) describes the need for: *A communication infrastructure providing authorized seamless information transfer on board ships, between ships, between ship and shore and between shore authorities and other parties with many related benefits*.

The development of the Maritime Cloud was motivated by this e-navigation need and testbed experience from the EU funded EfficienSea project. In the project potential e-navigation solutions were implemented and tested, and a need for a common technical framework to facilitate service management, security and additional carrier agnostic communication means was confirmed.

The Maritime Cloud is intended as a refinement of the agreed overarching e-navigation architecture, shown in **Error! Reference source not found.**. The architecture dwells on:

1. **A Shipboard technical infrastructure -** Shipboard communication, navigation and display equipment is integrated to exchange information seamlessly, using harmonized data formats.
2. **A Shore based technical infrastructure -** Shore based information is made available through harmonized data/information services.
3. **Communications -** A concept of generic communication links providing the logical connections that allow data/information flow between the shipboard and the shore based systems - or at a higher logical level: The people operating/using these systems.

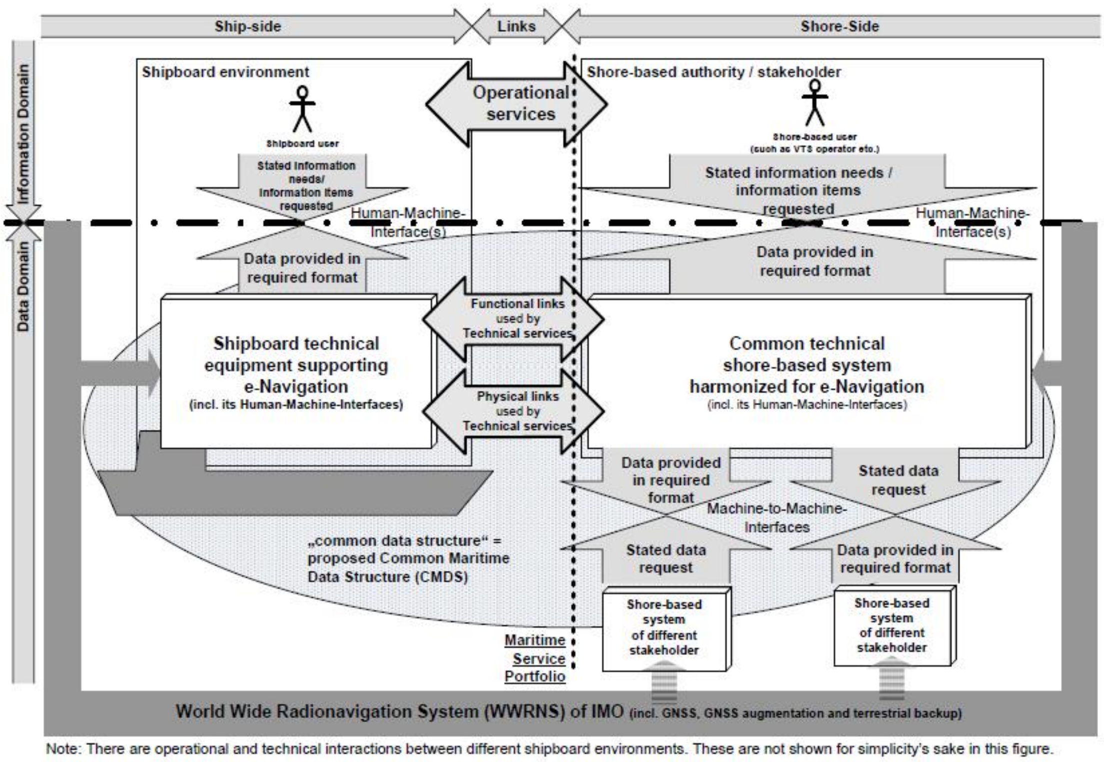


Figure 1: *IMO overarching e-navigation Architecture (IMO NAV57, WP6)*

To provide efficient and secure delivery of a data/information service from one stakeholder to another in this architecture, an added level of detail was needed. The Maritime Cloud intends to fill this gap.

Early on in the development of the Maritime Cloud a number of high-level requirements was identified:

1. Provide additional communication means, initially utilizing Internet connectivity
2. Service consumers must easily be able to discover provisioned services
3. Service providers must easily be able to advertise their provisioned services
4. All maritime actors must have a unique maritime ID with attached attributes as role, nationality, etc.
5. Means for secure communication, that is
    a. Authenticity – Guarantee of who I am talking to – allowing authorization (access control) to be enforced by service providers
    b. Integrity – Guarantee that data is unaltered
    c. Confidentiality – Guarantee that data is not accessible by a third party

The development of the Maritime Cloud is based on a number of guiding principles. These were influenced by the *System Wide Information Management* (SWIN) concept, a concept managed by the Federal Aviation Administration intended for greater sharing of Air Traffic Management system information within aviation.

Re-use not re-invent

Utilize existing and proven Information and Communication Technology (ICT) concepts and practices. E.g. from

- Distributed systems

- Service-oriented architectures
- Software design patterns
- IT security

Separation of information provision and consumption

- Actors are often both providers and consumers of information
- Not ideal to decide in advance who will need what information, obtained from whom and when
- Decoupling providers of information from the possible consumers allows the number and nature of providers and consumers to evolve through time

Loose system coupling

Use a modular design with loose coupling and high cohesion where components of systems have little or no knowledge of the definitions of other separate components. By doing this barriers between systems and applications are removed, and interfaces are compatible. It allows for independent acquisition and composability of system components.

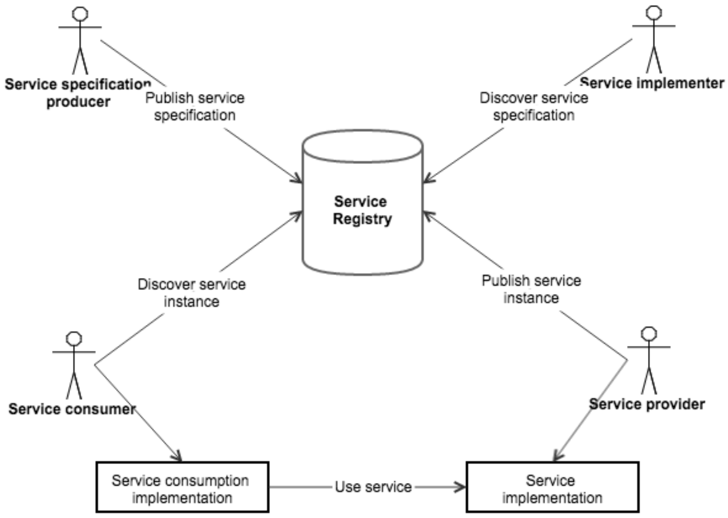
Build on open standards

Open standards means widely accepted and supported standards set by recognized standards organizations or the marketplace. These standards support interoperability, portability, and scalability and are equally available to the general public at no cost or with a moderate license fee.

Facilitate Service Oriented Architectures (SOA)

Driven by analysis of user needs, functionality is developed, packaged and implemented as a suite of interoperable services that can be used in a flexible way within multiple separate systems from several domains within the maritime world.

2 Maritime Service Portfolio Registry



The Maritime Service Portfolio Registry contains **service specifications** according to an envisioned Service Specification Standard and provisioned **service instances** implemented according to a service specification. The service registry aims at improving the visibility and accessibility of available maritime information and services. This enables service providers, consumers, and regulatory authorities to share a common view on service standards and provisioned services. The service registry does not provide maritime information but a specification of services and the information they carry, and the technical means to obtain it. The service registry provides the mechanisms to manage the life cycle of service specifications and service instances. As depicted above, the service registry enables the "provider" to "publish" information related to its service instances so that the "consumer" is able to "discover" them and obtain everything (e.g. interface information) required to ultimately use those services.

The service registry supports some of the cornerstones of SOA: Service loose coupling, abstraction, reusability, autonomy, composability, discoverability and standardized service contracts.

The service registry is intended to facilitate, or implement, the **Maritime Service Portfolio** (MSP) concept by providing a repository for the specification of operational and technical services and provisioned service instances. The service registry is intended to span all maritime services, not only digital services, thereby making it a single reference point for provision and discovery. It is anticipated that the envisioned Service Specification Standard will be in the form of **S-100 Product Specifications** according to a revised version of the S-100 data framework standard accommodating service orientation. Currently a S-100 Product Specification is very data centric, limited to specifying complete datasets with no means to specify the interoperable services transferring data (e.g. continuous and real-time delivery services).

2.1 Maritime Identity Registry

Identity of a ship is often addressed in terms of a ships name and IMO number. On communication systems, the identity of a ship may be a callsign, 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 callsign or MMSI number corresponds correctly to a unique ship. None of these identity systems or registers takes into account the need for dealing with actors who are not ships and don't necessarily have their own radio station, such as ship owners or service providers. The Maritime Cloud will provide a Maritime Identity in the Maritime Identity Registry, enabling access to:

- Certificates in a public key-infrastructure that enable secure data communication with other maritime stakeholders over any communication channel
- The Maritime Service Portfolio Registry
- The Almanac
- The Maritime Messaging Service

All actors may maintain their own contact information (such as VHF working channel, e-mail address, Phone or FAX nr., etc.), while other attributes may origin from Authoritative Registers (such as IMO / MMSI number). This way the Identity Registry will provide updated 'white pages' contact information readily available to SAR and VTS authorities, or to other maritime professionals if marked as 'public', as part of the downloadable and dynamically upgradable publication **The Almanac**.

Adding options for advanced features such as a public-key infrastructure providing digital certificates and authentication capabilities for certain situations, well known from for instance the financial sector, will enable trusted information and facilitate encrypted data transfer between maritime actors, and even digital signing of documents.

2.2 Maritime Messaging Service

The Maritime Messaging Service (MMS) within the Maritime Cloud are intended to ensure seamless information transfer across different communication links in a carrier agnostic manner.

The MMS within the Maritime Cloud will be based on Internet connectivity, yet any number of alternative communication services may be connected to and utilized by the Maritime Messaging Service via dedicated gateways. This way, a message sent by one specific ship using INMARSAT access to the MMS, may be received via a VSAT terminal on another ship, a HF data connection on yet another ship, or a VTS operator on a DSL landline Internet connection.

Each communication service will impose technology and situation specific limitations in terms of restrictions to capabilities, bandwidth availability, size of transferrable data packages, latencies, etc. – but basic transfer of text or structured data (e.g. XML) will be possible.

Thus, when a maritime actor wishes to transfer information to another maritime actor not within range of a compatible communication link, or in need of multicasting information to a group of actors not within range of one single communication link, the MMS can ensure delivery across which ever communication link is currently active at each relevant actor. In case a ship temporarily has no active communication link, the MMS will function as a prioritized store-and-forward queue of messages where the validity period can be defined on messages. Through mechanisms of protocol level acknowledgements, the delivery of information via the MMS can be quality assured.

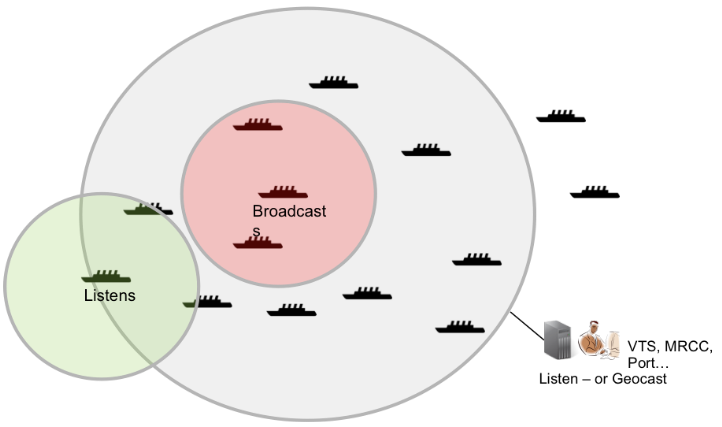
The MMS mechanism requires each actor in the Maritime Cloud to maintain a persistent connection or regularly establish a connection to the MMS, maintaining knowledge of which data links are open towards each mobile actor. At each connect, or regularly, mobile actors provide a position update at protocol level to the MMS, enabling a geographical awareness of the position of each actor at the MMS. The geographical awareness may be strengthened through the supplement of (satellite) AIS, providing high resolution but requiring no additional communication. The geographic awareness enables 'geo-casting' – i.e. actors may logically 'broadcast to' or 'listen to' an area around their own position, regardless of which communication link is used for broadcasting or listening in to the broadcast.

Priority information such as MSI may be queued for quality assured delivery (requiring an automatic acknowledge of reception). Shore entities (or military or law enforcement units) may 'listen' to an area of interest without specifying their updated position.

Geo-messaging service

Digital communication means are essential for a communication framework. Currently we have only one general-purpose digital communication mean universally available: AIS ASM. AIS ASM will not be sufficient for the envisioned e-navigation solutions. New communication systems (like NAVDAT and VDES) need to be developed and demonstrated – i.e. not available in the short term. To solve this an Internet based messaging protocol is introduced.

- Geo-messaging is a messaging protocol implemented on top of TCP/IP
- The protocol allows to send messages to actors based on their maritime id, but as the protocol is geo-aware, it also allows sending messages to recipients within a specific geographical area (geo-casting)
- Actors can listen to a specified area
- Geo-cast is an implicit feature of many radio based communication systems. The area will be defined by the physical capabilities of the communication system
- The protocol allows to emulate existing communication systems and simulate future communication systems



2.3 Maritime Cloud Almanac

An important concept in the Maritime Cloud is the **Almanac**. It is an offline digital version of the public parts of Maritime Identity Registry and Maritime Service Registry. It will function as a 'white pages/yellow pages phonebook' of registered maritime actors and services and allow offline use of central framework services like service discovery and secure communication. The Almanac will limit the need for especially mobile actors to search online for contact information, but rather to update the publication upon request, or at regular intervals, when communication links are available at low cost.

3 Ship and shore side integration

The services of the Maritime Cloud will be provided to ship and shore side applications by a Maritime Cloud service component. The component makes it possible to keep the Maritime Cloud services abstracted from the physical components and encapsulates the complexities of communication roaming. The component will function as a local information hub, connected to relevant sensors, navigation displays and communication equipment. The component API will provide services for

- Security through online use of the Maritime Identity Registry or offline use provided by the Almanac
- Service discovery through online use of the Maritime Service Portfolio Registry or offline use provided by the Almanac
- Service provision of dynamic services. E.g. a vessel providing own position and navigational data
- Communication through generic communication primitives seamlessly roamed to appropriate available communication systems based on a user defined rule base.

The component will handle update of and access to the Almanac.

3.1 Governance and operations

The possible global governance and operation of the Maritime Cloud is under ongoing consideration. The concept will be able to facilitate a number of different governance structures. Below some initial thoughts are given.

It is generally expected that registering stakeholders to participate in the Maritime Cloud will be a simple process, which may easily be integrated with existing work procedures, such as issuing call signs and MMSIs for ships or shore stations, but including a more advanced digital certificate where needed (IMO NAV 59/6, annex 2, page 4). Once registered, each actor will be given access to maintain most parts of own contact information and decide whether access to it is public or restricted, such as the ship's e-mail address, a VTS center's VHF working channel, or how to access local port information. The components included in Maritime Cloud Data Centers should be operated based on international standards for cyber security. There are several different options for implementing the data centers that host the core components of the Maritime Cloud, noting that these are not intended to include large scale storage of all information, but only components that facilitate authenticated information exchange and automatic discovery of information services. This document describes three scenarios, and their associated advantages and disadvantages.

One international data center

The simplest scenario would be one single company or organization operating a global data center. Each Flag State will have responsibility for the logical content of their own national part of the registries, and all maritime parties will be able to register through their National Competent Authority, enabling them to interact as authorized parties to the Maritime Cloud.

Advantages: This is a very simple solution with low technical complexity. There will be no complexities associated with maintenance of one coherent core system.

Disadvantages: The responsible operator will have full control of the system, and all stakeholders must agree to trust one single global organization. The data center must apply methods for assuring redundancy in all aspects of its operation and prevent the physical data center from becoming a single point of failure.

One international organization – three regional data centers

In this scenario, one international organization governs three regional data centers divided evenly by time zones, for instance one in the American time zone (UTC – 8 hours), one in the European/African time zone (UTC) and one in the Asian/Pacific time zone (UTC + 8 hours).

These regional data centers should constantly synchronize public data on a peer-to-peer level, enabling functional transfer to another data center, in case the connection to one data center fails.

Each Flag State will have responsibility for the logical content of their own national part of the registries, and all maritime parties will be able to register through their National Competent Authority, enabling them to interact as authorized parties to the Maritime Cloud. Ships and other entities may connect via the nearest data center, or any of the other data centers.

Advantages: This solution is technically relatively simple and provides a high degree of resilience through the distributed network of redundant data centers. The time zone separation will ensure that operational personnel is available during normal working hours with at least one of the major physical data centers at any point in time. This model could provide a path whereby developing countries may achieve exceptionally low entry barriers for participation in the Maritime Cloud.

Disadvantages: None identified.

National data centers + an international data exchange

This scenario fully resembles the LRIT regime. Each Flag State will either have its own data center, or join a regional data center, and each data center will exchange data through the International Data Exchange. Ships will connect through the data center they are registered with.

Advantages: This scenario allows the reuse of the organizational and governance structures developed for the LRIT, with only modifications to the technical services provided through the data centers.

Disadvantages: The technical complexities of many different data centers will be significant. Design will have to be based on a large set of internationally agreed technical standards. As a result, establishment will be time consuming, and development and operation will come at a relatively high cost. As the technologies evolve and require updates, coordination between the many different data centers will require significant resources. Coordinated updates across many different data centers could be a high-risk operation.