 Input paper: ENAV17-9.15

Input paper for the following Committee(s): check as appropriate Purpose of paper:

**□** ARM **□** ENG **□** PAP **□** Input

**x** ENAV **□** VTS x Information

Author(s) / Submitter(s)

Kwangil Lee, Electronics and Telecommunications and Research Institute

Jin Hyoung Park, Korea Research Institute of Ships and Ocean Engineering

Han Jin Lee, Korea Research Institute of Ships and Ocean Engineering

Kasper Nielsen, Danish Maritime Authority

Jens Kristian Jensen, Danish Maritime Authority

Thomas Steen Christensen, Danish Maritime Authority

An Identification and messaging scheme for Maritime Cloud

# Introduction

E-navigation is defined as the harmonized collection, integration, exchange, presentation and analysis of maritime 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. For the realization of the e-navigation, one of the key elements is the information and communication infrastructure which exchange and collect the maritime information both in onboard and ashore.

The Maritime Cloud was introduced as a communication infrastructure for e-navigation. It is defined as a communication framework enabling efficient, secure, reliable and seamless electronic information exchange between all authorized maritime stakeholders across available communication system. It also needs identification and authentication of maritime resources. The structure would be a base framework for the e-navigation.

This paper describes a structure for the MC for the identification and authentication of maritime entities. Maritime Messaging Service (MMS) of the Maritime Cloud is also explained for a seamless messaging services.

The scope of this document explains

* Maritime Cloud Architecture as an e-navigation infra-structure
* Identification of maritime entity and maritime resources
* Addressing for seamless roaming
* Authentication scheme for each maritime entities

# Design Considerations

The followings are considered for the design of identification and authentication scheme for the Maritime Cloud as an e-navigation communication infrastructure.

* Heterogeneity: Maritime objects are ranged from small sensors to all users and application data. It is not possible to describe all information regarding every kinds of maritime objects in one way since each maritime object has its own attributes and characteristics. Therefore, the objects shall be defined so as to accommodate the difference among maritime resource objects.
* Flexibility: Each stakeholder has different usage of the information and resources. Since it is not possible to specify all usage of the information and its attributes, it needs to allow to define and use it for their own purpose.
* Scalability: The Maritime Cloud shall be scalable to accommodate future extension of all maritime resources and information. The Maritime Cloud should be able to be extended easily when new requirement and request arises.
* Open platform: The Maritime Cloud shall support open platform which is need to be exchanged and integrated in standard manner. This means that the interface shall be available to all users.

# E-navigation Infrastructure

A maritime cloud is a communication infrastructure for e-navigation. The structure of e-navigation shall be described as illustrated in Figure 1.

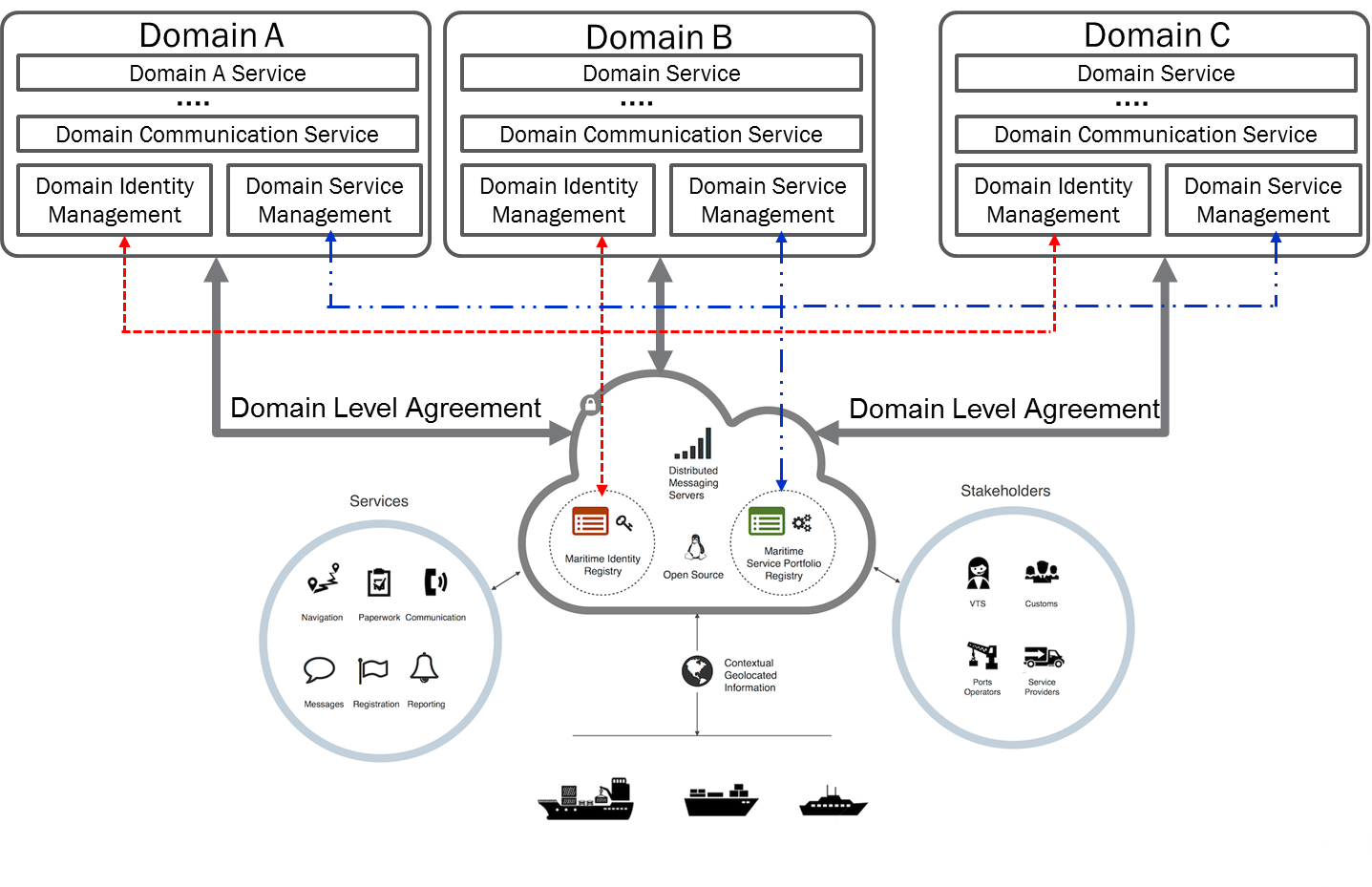


Figure 1. e-navigation structure for maritime domain

The e-navigation infrastructure would consist of multiple numbers of domains. Each domain is connected through the Maritime Cloud which plays a role as hub. The Maritime Cloud connects each domain with standard open interfaces for communication, authentication and authorization. These interfaces would be shared and used for all maritime stakeholders and information. Each domain may have its own way to communicate, authenticate and authorize with other domains by providing proprietary interfaces. These interfaces may meet its own purpose but cannot be commonly used by all maritime stakeholders. This may requires to define interfaces whenever it needs to collaborate with other domains. However, each domain needs to define an interface once with the maritime cloud, then it doesn’t need to define another interface to collaborate with other domains.

Each domain has a responsibility to maintain all maritime objects in its domain. This means that all objects are identified and information on objects is exchanged by the domain-specific scheme. However, any information in other domains shall be exchanged through the Maritime Cloud. This means that any objects in a domain shall be identified and registered by the Maritime Cloud. However, the credit and level of information reliability, and service shall be provided are various from domain to domain. Based on the Domain Leave Agreement, the level and type of services will be defined. When an authentication and authorization is delegated to each domain, the Maritime Cloud domain will play a role of the highest level of authentication and authorization entity for the entire maritime identities and services.

## Key elements for domain management

Each domain has its own responsibility for domain-specific information and resources. Some domain may provide its own communication infrastructure among local entities while some makes use of components in the maritime cloud domain. These are basic functions are required for the maritime digital infrastructure.

* Identity management

Enrollment and update the resources which are owned by the domain. It is possible to define domain-specific type. If some identities are necessary to communicate with other domains, it shall be registered in the Maritime Cloud domain.

* Service Management

All services provided by the domain shall be managed by the service management function. It includes discovery, advertisement and update the service information. When the services are required to communicate with services in other domain, it also shall be registered in the service management in Maritime Cloud.

* Authentication, Authorization and Access right management

All identities in a domain shall be identified and authenticated. Each domain has its own responsibility for the authentication and access rights for the maritime resources.

* Communication infrastructure

The communication interface and services are also available. For this purpose, other available communication middleware can be used such as UPnP(Universal Plug and Play) or other well-known communication protocols are used for this purpose such as http and REST. The Maritime Messaging Service in the Maritime Cloud is one of the communication infra-structure.

* Message Gateway (MGW)

When a domain has its own communication services, a domain shall provide a message gateway with the Maritime Cloud so as to interconnect with other domains. The identity and service shall comply with the requirement of the Maritime Cloud.

* Each domain shall provide means to connect the Maritime Cloud so as to communicate with other domains including the Maritime Cloud itself. All entities and stakeholders to be communicated with other domains shall be registered to Maritime Identity Registry in the Maritime Cloud. Same rules are applied to the services in the domain.

## Maritime Cloud Domain Management

The Maritime Cloud domain is a domain which provides communication services for GMDSS and IMO MSP services. The Maritime Cloud has its own responsibility for the service within the Maritime Cloud domain. It also covers the authentication of the services defined in the Maritime Cloud.

In addition, the Maritime Cloud has the responsibility for interconnection management among domains. All identities and services are registered and authenticated by the Maritime Cloud.

### Maritime Identity Registry (MIR)

Maritime Identity Registry records all identity information of maritime device and users. The identity information is defined as <type, instance, affiliation>. It also maintains a list of <type, authentication methods, authentication authority, access rights> for the authentication and authorization. The maritime identity which is used for maritime cloud shall be explained in the next clause. Even though it is defined for maritime cloud, it may be used for all maritime resources in e-navigation.

### Maritime Service Registry (MSR)

A Service Registry contains provisioned service instances as defined by service specifications, and will enable service providers, consumers, and regulatory authorities to share a marketplace for services. The service registry does not provide maritime information itself, but a specification of services and the type of information they carry, plus the technical interface to obtain it. When each service is provided and requested, it is verified by its source and its compliance to the service description. The service registry enables the “provider” to “publish” its service instances so that “consumers” are able to “discover” them and obtain interface information required to use a service. It also provides access right information for the services.

### Maritime Cloud Services

A set of services are defined for maritime cloud domain. These services are maintained and managed within the maritime cloud domain. All services in maritime cloud shall be maintained by MIR and MSR as specified in 3.3.1 and 3.3.2.

### Maritime Messaging Service

The Maritime Messaging Service (MMS) is a basic service of the Maritime Cloud service which is the communication infrastructure in the Maritime Cloud. It provides a seamless roaming among Maritime Cloud entities. This means that MMS shall be registered as a service at MSR in the Maritime Cloud.

The all users for MMS shall be also registered in MIR which is used for user authentication and for access right.

# Maritime Identity

A maritime entity is an object in maritime digital infrastructure. A maritime entity can be duplicated and multiple copies in the maritime domain. A maritime resource is a maritime entity which is identified uniquely in the maritime domain. A maritime resource identifier is an identifier that is uniquely assigned to each maritime entity. A maritime resource may have some additional information such as location information in addition to maritime entity. Maritime resource identifier is used for identification of the maritime resource and is also used for the authentication and location retrieval for the resource.

## Maritime Resource Identifier

Each maritime resource has six different identification elements: domain, location, device, service, user and application data. With the combination of these elements, each maritime resources are identified uniquely. The definition of each resource classes can be summarized as following:

* Domain: Application domain. Each application domain has a responsibility of the management of other identity classes.
* Locator: Logical location where the resource is used or possessed such as company, organizations or ship. For ship identification, IMO number or other identifier may be used.
* Device: device is to identify some specific equipment and system or server. The device can be identified by the IP address including DNS or MMSI identifier.
* Service: Service is a class to identify some specific service application. It can be identified by service name such as text messaging service, notice to mariner service, and weather routing service.
* User: an identifier for user at system or some specific services. It can be an email address, passport number or social security number.
* Application data: a resource object to identify data which is used by some specific users or applications. For example, route ID can be an application data used by a company, a user or a ship.

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Description | Example | etc |
| Domain | Application domain. | Maritime Cloud  Sea Traffic Management  VTS |  |
| Locator | Logical location where maritime identity presents | Ship, company, nations,…, etc. |  |
| Device | An identifier for some specific equipment and system. | MMSI, DNS, IPADDR |  |
| Service | An application service, | TXTService, MSI |  |
| User | A user registered to a service | Email, SSN  (social security number), |  |
| Application Data | Data type which is used by user or by services. | RouteID, MSI ID, Chart ID |  |

* Each maritime object is identified uniquely by the combination of the above information. When some of information is omitted, the identifier may indicate a group of maritime resources rather than a single maritime resource.

## Maritime Resource Name

Each element of maritime identity can be represented by maritime resource name.

### Uniform Resource Name (URN)

A Uniform Resource Name (URN) is a Uniform Resource Identifier (URI) that uses the URN scheme, and does not imply availability of the identified resource. Both URNs (names) and URLs (locators) are URIs, and a particular URI may be both a name and a locator at the same time. Perhaps an example can best clarify this: the ISBN number used for books is in fact a URN, it is an unambiguous identifier for a given book. But a ISBN number is not a URL as it does not define where the book can be found.

### Maritime Resource Name (MRN)

Maritime Resource Name is similar to Uniform Resource Name (URN) which is an identifier that uses the URN scheme and does not imply availability of the identified resource. Same as URN, it does not specify the availability of each resource and not tell if it is duplicated or not. The exact format and expression is explained in the document of *Maritime Resource Name*.

# Maritime Messaging Service (MMS)

The maritime resource identifier is used as a source/destination address for the communication through maritime digital infrastructure. In MMS, maritime resource identifier is used to find the location of the maritime resources and to deliver the message to the exact maritime resource for seamless roaming. MMS is the communication service only for the Maritime Cloud domain but not limited to.

MRI is used as the basis for the address for MMS. Since the length of the MRN may be too long, it shall be shorten by only using type and type-specific information. The other information shall be handled by MMS internally.

MMS in Maritime Cloud shall support various types of communication services as following

* Point-to-point: This is a communication service to deliver a message to a single destination.
* Geo-casting: The geo-casting is a communication service to deliver all maritime resources within a geo-graphic region.
* Group-casting: The group-casting a communication service to deliver messages a group of destination. This enables to deliver messages to multiple maritime resources.
* Any-casting: This service is a single message delivery service to one of group. The group can be a same maritime entity or any maritime resource in a group.

# Seamless Roaming with MMS for Maritime Cloud.

## Requirements

The seamless roaming is to guarantee the message delivery to the destination even though the sender has no knowledge of the current location of the receiver or the receiver changes its location. The current location information of each identity shall be maintained with its identity information. This means that the identity information shall maintain the exact current location information or has the reference to the location.

The each maritime entity shall report its current location information periodically to the location server. This enables the location server to maintain up-to-date location information of all maritime entities. The location server can be maintained in the centralized (physically or virtually) server or distributed server. The location server can be implemented as separate server or as a part of MIR. Here we assume that the location server is a part of MIR.

The seamless roaming process is very similar to hand-over procedures of Mobile IP.

## Structure

The following figure illustrates the procedures providing message service with authentication in the Maritime Cloud.

Each maritime entity is connected to MMS server. It is also connected with MIR and MSR. In the maritime domain, it may have multiple MMS servers and so MIR and MSR do. MMS server directly connected with the maritime resources by using Internet.

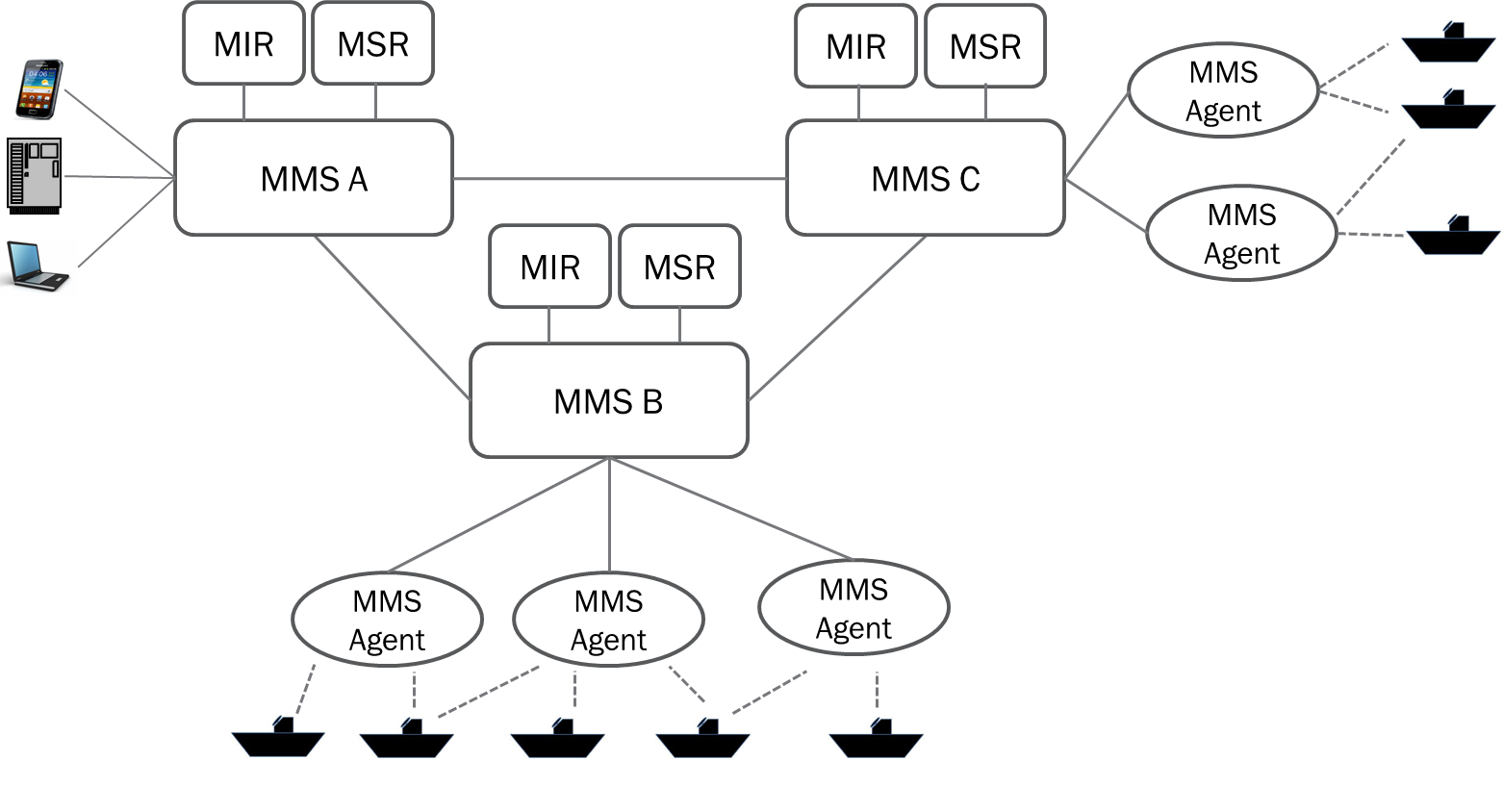


Figure 2. Maritime Cloud Structure

All maritime resources cannot be connected to MMS server directly when communicate with GMDSS equipment. In this case, maritime resources should be connected through MMS agent. It connects to MMS server and a maritime resource. Since the bandwidth of GMDSS is limited, it may perform some additional processing for the message delivery to the receiver rather than sends the whole message. This may requires some data and protocol conversion of the original message.

The followings are illustrated as a possible communication procedures for the Maritime Cloud. As shown in the figure, the messaging service consists of four steps as follows:

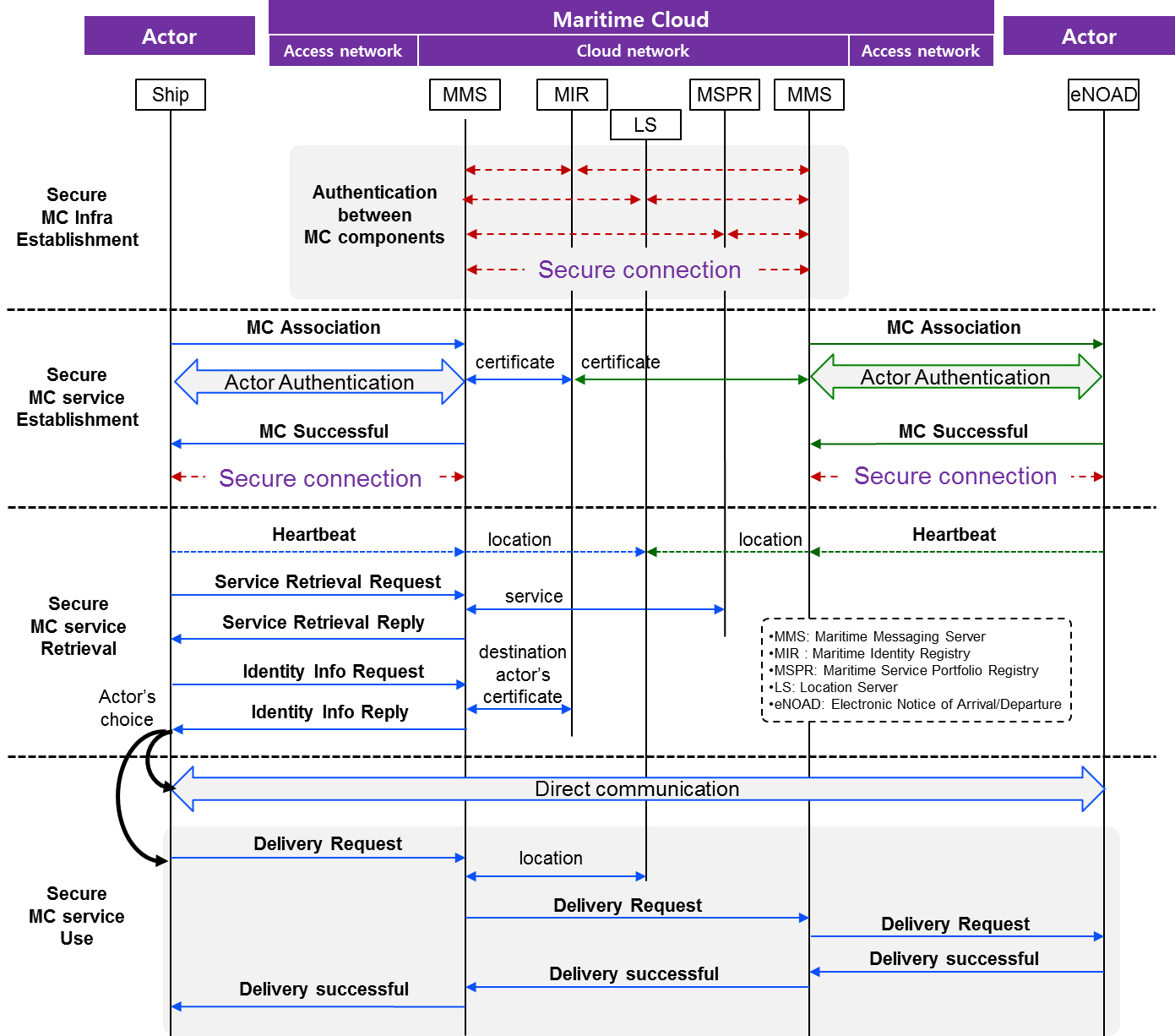


Figure 3. Maritime Message Service Sequence

The communication procedures for the Maritime Cloud service consist of four steps as follows:

Infrastructure establishment: Initially, all MC components such as MMS, MIR, MSPR, and LS should be connected with each other and setup secure connection before they work for the service if necessary. The public key for the authentication may be pre-established in the system or acquired from Maritime Identity Registry on-line for the secure communication services for maritime cloud.

Secure Maritime Cloud service establishment: If MMS server receive a request from an actor with its identity information, it first of all authenticates the actor. If the actor is legitimate maritime entity, its request is allowed. The public key to be used when authenticating the maritime entity is acquired from MIR on-line. A Maritime Identity may want to authenticate a MMS. For this, the authentication process supports mutual authentication between the maritime entity and the MMS.

Service Retrieval: To make use of useful maritime services, an actor may retrieve service list from MSR. Consecutively, it may retrieve information on a destination server to connect from MIR.

Communication Service: When a session setups with MMS, the requestor communicate with the counterparty. MMS shall provide seamless roaming for the service, so each entity is not necessary to aware of the current location of the communication party. There are two types of communication can be established: Direct communication through Internet or MMS service. Direct communication implies the Internet communication through satellite or 4G/LTE communication.

## Procedures

### Registration

Each maritime resource needs to be registered to its home identity server. When MIR is implemented in distributed or hierarchical, the identity registry is not always the same when the maritime resource moves. When there are multiple identity registries are available, then it is called home registry server where the maritime resource is registered. The maritime identity registry which is used but not “home identity registry” by the maritime resource is called “visiting registry”.

For example, each person P-A, P-B, P-C and each ship S-A, S-B, S-C is registered to MMS/MIR A, B, and C accordingly. Then MMS/MIR A has (P-A, S-A), MMS/MIR B does (P-B, S-B) and MMS/MIR C does (P-C, S-C).

### Advertisement

Each device and maritime resource shall advertise its location to others using available communication equipment and systems. The location of each resource can be collected by location server which may be implemented within MIR.

When a maritime resource is connected to the Internet, the location information is collected by its location server. When its location information is listened by a MMS Agent, i.e. one of GMDSS receivers(AIS, VDES, NAVDAT), it records the current location information of the maritime resources locally and request to update the location information to the location server. It also provides messaging service for the resource until it moves to other region.

### Position Update

When a MMS agent detects the location change of the maritime resource, it sends a position update message to the location server of the maritime resource. When a position is updated, it may require multiple location updates when multiple maritime resources are related.

The following figure illustrates an example. The person C-P is registered to C-S. C-S and C-P is now connected to new MMS server B through MMS Agent B-2. The MMS server B detects the new resources for C-S and C-P and its home registry is MMS/MIR server C. Then it sends the position update message to MIR C for those resources. The MIR C now has the current location information of it.

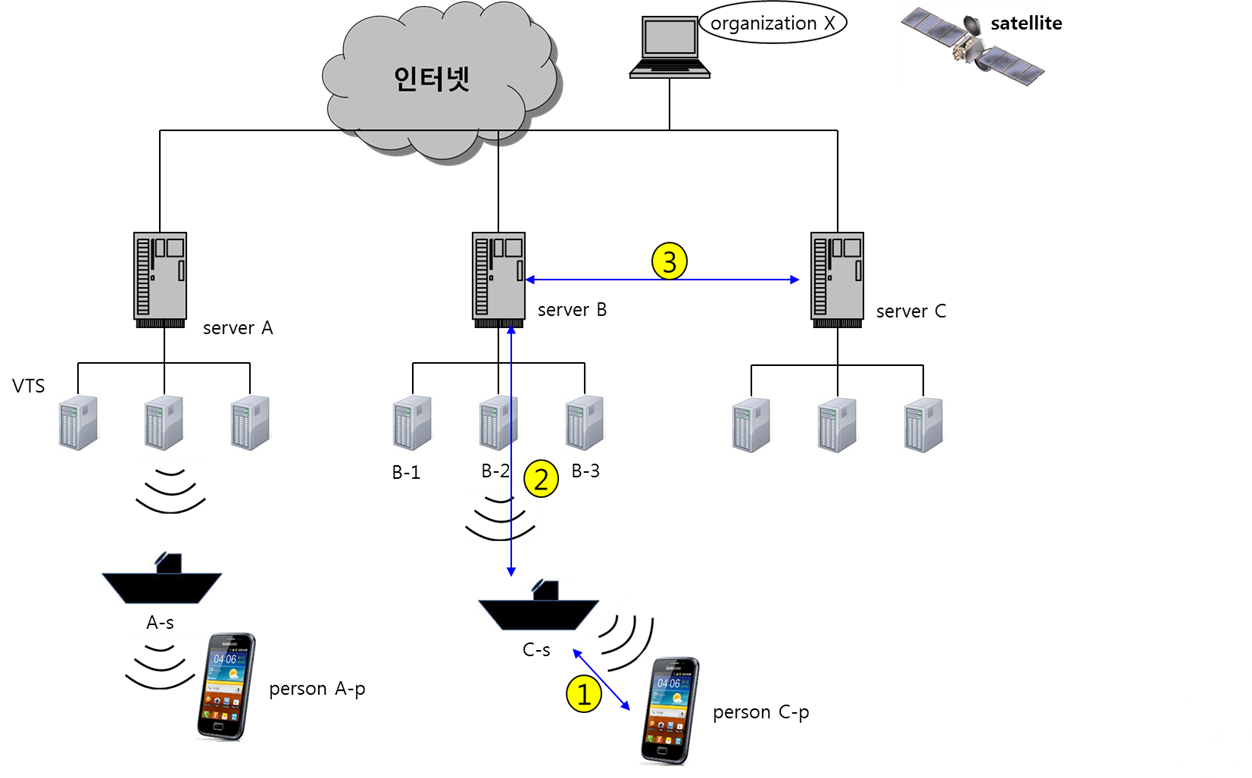


Figure 4. MMS Registration and Position Update Procedure

### Messaging services

There are two possible scenarios for the message delivery. When a resource is connected to the Internet or public networks, a maritime resource connects to its MMS server and sends messages to it. Then the MMS server forwards the messages to the target MMS server so as to reach the destination.

When a maritime resources needs to send a message through a MMS agent, then it to the based on the destination address. The current location of the destination address is provided by MIR, the location server. Based on the information from the MIR, the MMS server forwards the message to the target MMS server where a destination is currently located. The target MMS server forwards the messages to the destination through the proper communication channel.

For example, when a person A-P sends a message to a person C-P. Person A sends a message to MMS A through the available communication equipment in a ship A. The MMS A forwards the message to the home server of C-P, MMS C. MMS C queries the current location of MIR C and gets the current location of P-C, MMS/MIR B. Then MMS C forwards the message to MMS B. Since the MMS B knows the exact location information of C-P, it delivers the message to C-P along with MMS Agent B-2 and C-S. The following figure illustrates the procedures.

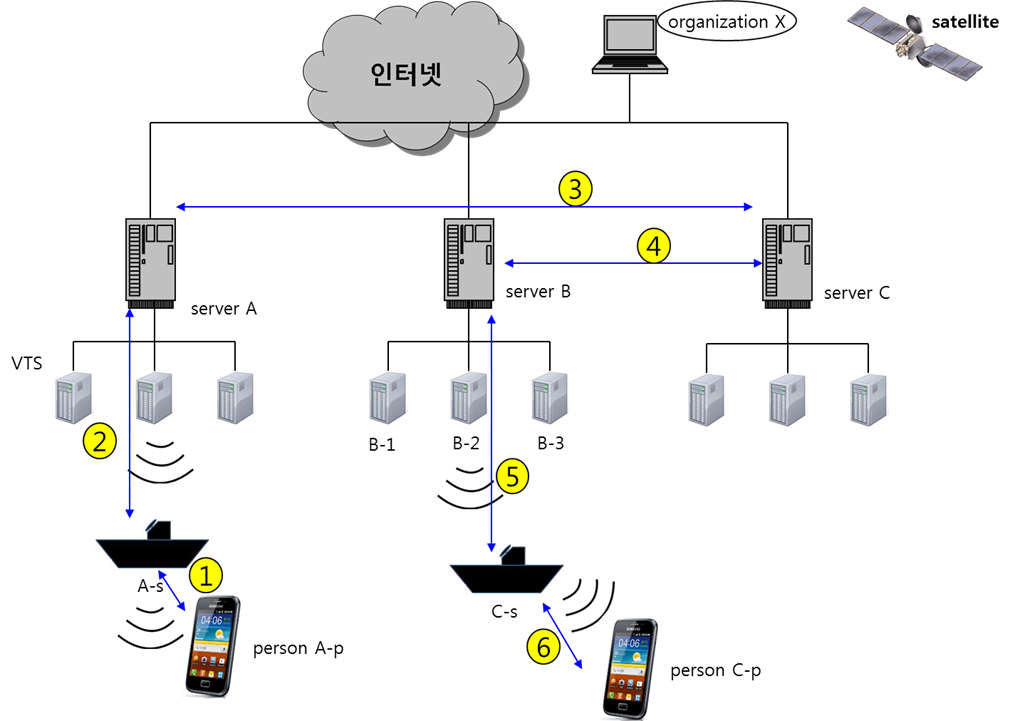


Figure 5. MMS Seamless Roaming Procedure

# Authentication for Maritime Cloud

## Overview

All maritime resource shall be authenticated before it uses by any services in maritime cloud. The authentication can be classified as device authentication and user authentication.

Based on identity information, the authentication procedures shall be performed. When the multiple authentications are related, then each authentication procedure is performed in cascade.

The following figure illustrates an example architecture for the authentication structure in the maritime cloud. It shows some core functions for the implementation of PKI based authentication scheme. The authentication is classified as device and user authentication. Each authentication mechanism is managed by different Registration Authority (RA). Each regional authority shall be connected to the central Certification Authority (CA).

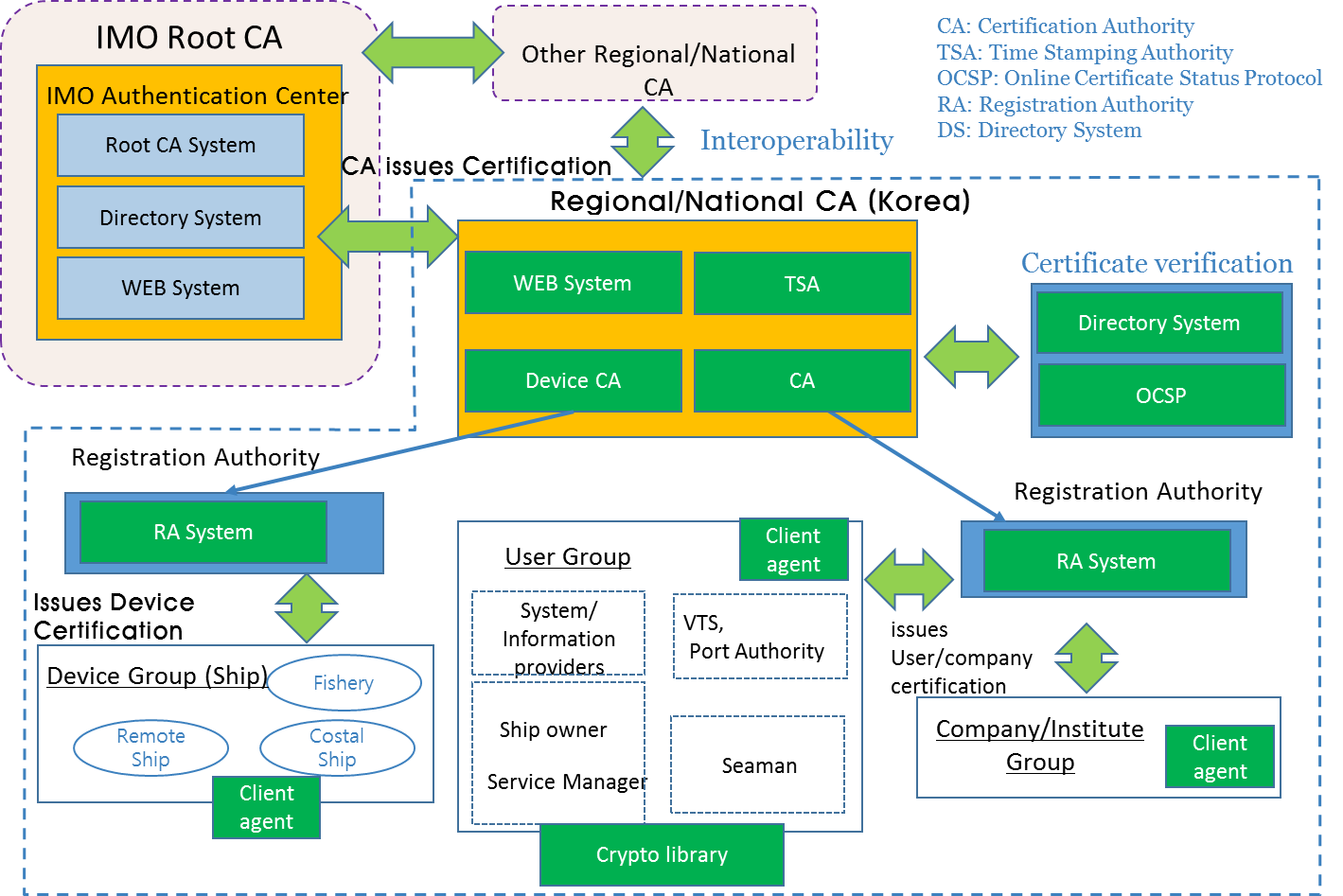


Figure 6. Maritime Cloud Authentication Scheme

## Authentication method

The authentication methods are different based on the type of maritime element. The following table summarizes the authentication method for each resource element. Some elements can be authenticated by automatically with manager inspection and verification. Some may be authenticated by systematically making use of authentication protocols.

|  |  |  |
| --- | --- | --- |
| Type | ID | Verification Method |
| Domain | Domain ID or name | Domain Level Agreement or contract |
| Locator | Location/organization identifier or Domain name | Manager or Face to Face verification |
| Equipment | MAC address or Serial number | Administrator or protocol verification |
| Service | Domain name or IP address | Service manager or protocol verification |
| User | Social security number or user ID | Face to Face verification or similar way |
| Application Data | Application id or name | Controlled by Access right |

## Maritime PKI Hierarchy

The structure can be extended to additional level of hierarchical authentication scheme based on PKI. The figure illustrated the MIR hierarchy within a maritime cloud domain. The hierarchy can be extended to connect other certification authority in other domains.

In a domain, the MIR takes a role of the registration authority. Its role may be delegated to the other identification management services. When it is delegated, the registration authority has proper responsibility for each RA. When a maritime cloud is divided into sub-domain such as a sub-domain can be implemented per a region or per country, it is required to have a root CA. This requires the inter-operability among multiple CAs. For the e-navigation infrastructure, an international organization such as IMO or IALA takes a responsibility for the management of CAs.

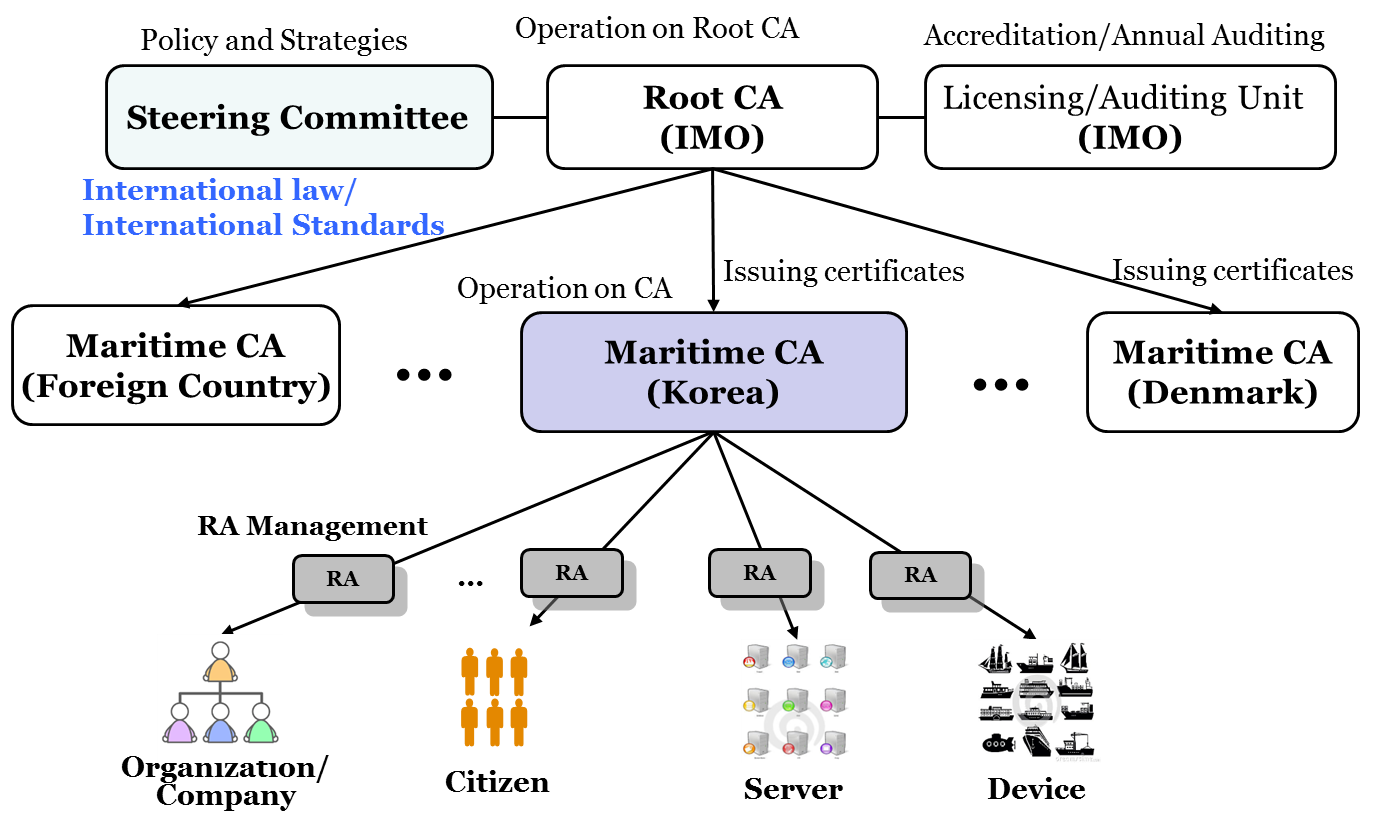


Figure 7. Maritime PKI Structure

# Conclusion

In this paper we consider the basic structure and functions of the maritime cloud. We believe that maritime cloud will be a central part of the e-navigation digital infrastructure. Also, the elements of the maritime resource identification are defined. The maritime identifier shall be used to identity each maritime resources uniquely regardless of where it is located and what type of resource is. Finally, we consider an authentication scheme for maritime cloud. It may also be used for an authentication infrastructure for e-navigation digital infrastructure.