Input paper: [[1]](#footnote-1) DTEC1-5.1.1.1

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

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

**x** DTEC **□** VTS **□** Information

Agenda item [[2]](#footnote-2) 5.1

Technical Domain / Task Number 2 …………………………………

Author(s) / Submitter(s) DLR, Germany  
 KRISO, Republic of Korea  
 Fintraffic, Finland  
 GRAD, UK & Ireland  
 AMSA, Australia  
 Navelink  
 UCPH, Denmark  
 AIVeNautics, Republic of Korea

Introducing MCP (Maritime Connectivity Platform)  
specifications to IALA

# Summary

IALA guideline G1161 'Evaluation of platforms for the provision of maritime services in the context of e-navigation', describes the need for harmonised decentralised platforms to facilitate the authentication and discoverability of technical services (associated with Maritime Services in the context of e-navigation). This document introduces the Maritime Connectivity Platform (MCP) as a possible platform for these purposes.

With contributions from multiple IALA members, various initiatives worked out a bundle of specifications that have been implemented in demonstrators and explored in field trials. These are now in a mature state ready for submission to the DTEC committee WG 1 as input for IALA guidelines or standards on digital platforms. It is proposed to establish an ongoing activity to extend this family of documents and provide further input for the DTEC committee. This will contribute to IALAs role in the digital transition of navigation and shipping.

# Background

In the early days of e-navigation, a number of organisations engaged in the realisation of this novel concept, partially through a number of international projects (including EfficienSea, Monalisa I + II, ACCSEAS and later EfficienSea 2, STM validation project and the SMART navigation project). Through these efforts, the need for authentication and the discoverability of technical services became evident. Consequently, work on the MCP started, both as a concept and as a prototype. In 2019, the MCP Consortium was established, and an actual specification was beginning to be developed, and in 2021 the MCP Consortium (MCC) endorsed the first operational MCP identity service provider (Navelink).

The MCP is based on technical specifications that harmonise:

* Maritime cyber security and specifically the establishment of infrastructure for digital identity management. These specifications currently are the “go to" solution to implement maritime services that use bi-directional message authentication and/or encryption.
* The application of the Maritime Resource Name (MRN) scheme for the harmonisation of digital resource identifiers for maritime services, vessels, user identities and other entities (e.g. virtual AtoN) in combination with MCP digital identities.
* A service for the reliable message exchange as an abstraction layer of IP-based services and the VHF data exchange system (VDES).
* Ways to publish and manage next-generation maritime services, making them available to the mariner.

Over the years, the different components of the MCP have reached different levels of maturity. This is summarised in the table below:

|  |  |
| --- | --- |
| MCP component | Maturity |
| **MCP Identity Registry** Facilitates authentication of parties exchanging data | Specifications have been made - and an operational instance has been run by Navelink for several years. |
| **MCP Service Registry** Facilitates service discoverability | Concept defined and prototype developed. This will be tested through the Open Digital Incubator initiative. |
| **MCP Maritime Messaging Service** Facilitates secure, reliable and seamless data exchange | Is in the process of being specified in parallel with prototype implementation. Specification is being made in an RTCM working group in collaboration with the MCP Consortium. |
| **MCP Trust System** Facilitates decentralised trust management among stakeholders | Concept exists and a prototype is being deployed by the MCP Consortium. |

Given the work already done in MCC and the maturity reached, various international organizations and initiatives are considering MCP as a technical concept for data exchange and to solve some of the issues to be addressed when implementing digitalization and data sharing. These are for example the IMO Maritime Services and the discussions for ISO 28005 Ships and marine technology — Electronic port clearance (EPC).

# Discussion

The intention is that the technical specification for the MCP be adopted as an IALA guideline, while the MCP Consortium (MCC) will maintain the operational governance of the MCP. Thus, the MCC will undertake the following tasks:

* Maintain procedures for endorsing MCP service providers using the IALA guideline containing MCP specifications.
* Endorse MCP identity service providers and maintain a signed list of their root certificates.
* Control access to the distributed ledger, which will hold globally discoverable information from all endorsed MCP service registry service providers (facilitating global service discoverability).
* Develop open-source reference implementations of the different MCP components.
* Operate a free (non-operational) public MCP demonstrator that all stakeholders can use for assessment and testing purposes.

Currently the MCP identity registry is well defined by the MCP Consortium - and it is the hope that these specifications can be adopted without any modifications. After all, these are the product of years of development and testing - and even years of operational use. Any modifications would cause severe difficulties with existing operational systems and compatibility.

Other areas of the MCP that are less developed, should be further matured within the IALA by the designated task group - in collaboration with the MCP Consortium.

## Appendices

The following appendices are provided with this document:

|  |  |
| --- | --- |
| Appendix | Description / purpose |
| A: The MCP concept document | The document gives a high-level description of the MCP. |
| B: Identity Management and Security; General Approach and Basic Requirements | The document introduces the MCP Identity Registry. It is the intention that this document will become the main part of a new IALA Guideline describing the Maritime Identity Registry. |
| C: Identity Management and Security; Identity Management | This defines how identities are handled in MCP using MRN (Maritime Resource Names). It is the intention that this becomes an appendix to above mentioned IALA guideline. |
| D: [Identity Management and Security; Public Key Infrastructure (PKI)](https://maritimeconnectivity.github.io/maritimeconnectivity.net/docs/MCP%20IDsec3%20MCC%20Identity%20Management%20and%20Security;%20Public%20Key%20Infrastructure.pdf) | This gives detailed description of the PKI part of the identity registry. It is the intention that this becomes another appendix in above mentioned IALA guideline. |
| E: Identity Management and Security; Authentication and Authorization for Web Services | This gives detailed description of web service authentication using tokens. It is the intention that this also becomes an appendix in above mentioned IALA guideline. |

# Action requested of the Committee

To take note of the information, and for interested parties to join the work in the dedicated task group.

Annex A

The Maritime Connectivity Platform (MCP)

Conceptual Overview

# Need for The Maritime Connectivity Platform

Digitalisation will change the way of navigation, shipping and maritime transportation. The driving motivation for digitalisation encapsulates everything from improving the safety of navigation, to improving efficiency and protecting the marine environment. In recent years reducing carbon emissions has become of even higher priority– and here also, secure digitalisation of the maritime domain is part of the solution.

Major initiatives have been started - with the International Maritime Organisations (IMO) e-navigation initiative and International Hydrographic Organisations (IHO) development of the S-100 concept as important examples. The overall focus has however, been on data harmonisation with S-100 being a prime example. Other initiatives include the IMO Compendium on Facilitation and Electronic Business and the availability of new physical communication channels provided by improved satellite coverage and development of the VHF Data Exchange System (VDES). Recently initiatives focusing on harmonising the means of data exchange (beyond the physical links) have also emerged, though these are still somewhat immature.

Digitalised services will provide necessary information, functionality and are the basis for a safe cooperation ship to ship and shore to shore. The most important enablers for this intention are:

1) A way for users and machines to **securely authenticate and authorise** themselves to each other.

2) An option to increase the **discoverability of services** to facilitate offering and finding them.

3) An efficient way to **provide services for information exchange and new functionalities** digitally.

The Maritime Connectivity Platform (MCP) aims to provide exactly these core features, and more widely, provide a foundation for the development of digital maritime services. It is a decentralised framework for enabling an efficient, secure, reliable and seamless digital service provision and information exchange between all authorised maritime stakeholders across all available communication systems (for instance VDES, LEO, 4G/5G). It enables maritime actors to use digital services to exchange both public and private information. Both commercial and non-commercial institutions can become part of the global MCP framework using their own installation (that is to say, their own independent ‘incidence’) of the MCP, thereby making them MCP service providers.

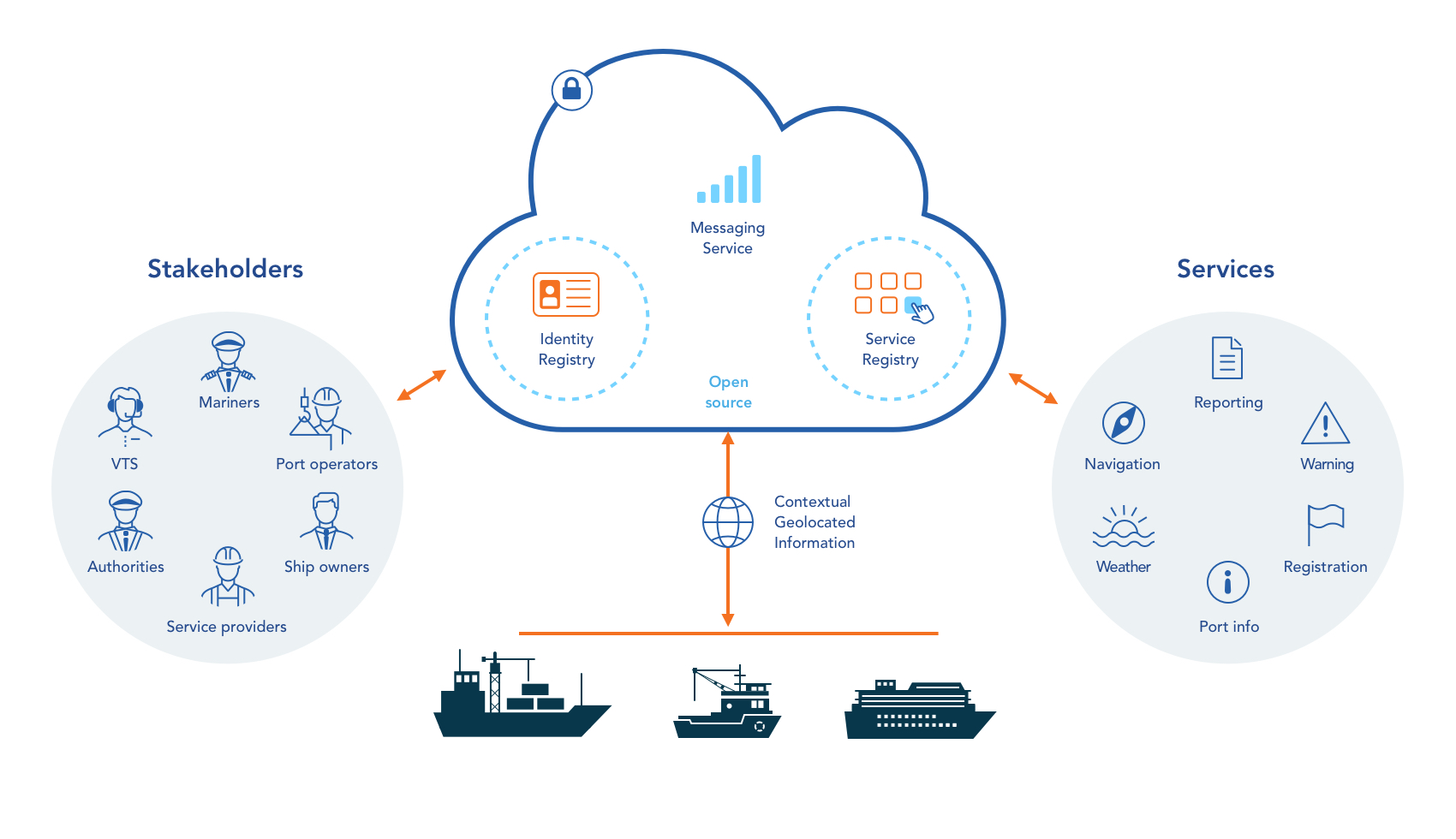


Figure 1 - Overall Concept of the Maritime Connectivity Platform

The MCP brings proven internet standards to maritime navigation and transportation systems by applying open, standardised and powerful vendor-neutral technologies. The MCP was initially created to address the goals of the IMO e-navigation initiative. However, the MCP has the potential to support digitalisation across a much wider maritime domain because it is an open-source solution that relies on the concept of Web Services for identity management and service management and, as such, can support much more than just the IMO’s Maritime Services in the context of e-navigation. The approach is based on digital services[[3]](#footnote-3) to access information (like maritime safety information) and functionality (like traffic management).

Overall, the MCP consists of three components, each addressing one of the three core features (c.f. Figure 1):

1. **Maritime Identity Registry** (MIR) - for secure and reliable exchange of information, it supports safe authentication and usage to all services, using identity information provided by trusted stakeholders. It facilitates confidentiality, integrity and authenticity in information exchange between users and between machines. The MIR uses existing standards such as MRN (Maritime Resource Names), OpenID Connect and X.509 certificates.

* **Maritime Service Registry** (MSR) - for registering, and discovering all relevant e-navigation and e-Maritime services, commercial and non-commercial, authorised and non-authorised, for free and against payment. The MSR can be seen as a sophisticated ‘yellow pages’ phone book of maritime services that can be searched for using a number of different criteria.
* **Maritime Messaging Service** (MMS) – for allowing authorised maritime stakeholders to send and receive messages in an efficient, reliable and seamless manner within the MCP. The MMS aims to mitigate limitations with regard to limited connectivity at sea and the use of various communication technologies.

The need for each component is described in more detail in the following subsections.

## Maritime Identity Registry - Need for Authentication

## The prerequisite for the digitisation of the maritime domain is a trustworthy provision of digital services for information exchange. For example, when a vessel approaches a port or waters controlled by a Vessel Traffic Services (VTS) centre it is dependent on receiving some information from them. However, it is not only important to receive the respective information, but also to verify from whom the respective information was sent and who the service is provided by. Otherwise, arbitrary participants could, for example, deliberately send out false information in order to disrupt the processes. In this case the recipient, would not be able to differentiate which information is the original and which is the falsified information. To solve this problem, the respective participants need be able to authenticate each other securely. In the paper world, authentication is done by a handwritten signature of the authorised person. In the digital world this is done by using digital certificates.

The MCP features - as one of its core components - an identity registry, where all entities that wish to exchange information are registered and have a digital certificate issued to them. Thus, a vessel registered with the MCP identity registry and having a digital certificate issued from it, can authenticate itself (prove its identity) to the VTS centre, and thus provide data to the VTS centre which the VTS centre can trust the origin of. The principle of authentication is a cornerstone in contemporary digital solutions.

## Maritime Service Registry - Need for Service Discoverability

Exchange of information in the maritime world has traditionally been based on radio communication - where "discovery" of the service was simply a matter of being within range of the radio station and tuning into the right frequency. New digital solutions are however, predominately using the internet to facilitate information exchange and this presents a new challenge with regard to service discoverability. The internet is global, and a service on the internet can in principle be located anywhere in the world and accessible from anywhere in the world. Thus, a mechanism for discovering internet-based services is needed; for instance when a ship wishes to receive information from a VTS centre.

For this purpose, the MCP features a maritime service registry, where maritime stakeholders can register services for others to discover. It is possible to search for services in a flexible manner, including but not limited to, searching for services from a specific provider(s), services providing specific information and services covering specific geographical areas.

## Maritime Messaging Service - Need for a Messaging Service

The maritime domain has certain specific challenges when it comes to data exchange between different entities in addition to authentication and service discoverability. These include the use of both IP (Internet Protocol) and non-IP based communication and the fact that some entities (primarily vessels) are mobile and often have poor and/or intermittent connectivity.

In order to facilitate efficient and reliable information exchange in the maritime domain, the MCP features a messaging service that supports seamless and carrier agnostic data exchange across IP and non-IP networks. The MMS also provides message queuing for use when connectivity is poor or unstable.

The MMS supports the use of VDES, including both terrestrial and satellite components.

# General PrincIples, relations to other standards and Governance

## General Design Principles

The development of the MCP concept has been guided by the following principles:

**Decentralisation:** With an ambition that the MCP should be used for all kinds of data by all types of organisations globally, the MCP needs to be fully decentralised both for technical and political reasons. Thus, all components (MIR, MSR and MMS) will exist in multiple instances operated by different organisations around the world. In simple terms, this means there is no ‘one’ MCP. Rather any organisation may run their own incidence of the MCP as they see fit, yet the architecture of the MCP allows authentication, service discoverability and messaging to function across different MCP service providers.

**Vendor independence**: It must be possible to implement, run and maintain the MCP on various technical infrastructures without relying on any vendor specific or proprietary features.

**Openness**: The MCP must be open for all stakeholders and other interested parties in the maritime industry and beyond. It is a call to join forces and together take the industry into the digital era.

**Non-profit governance**: While MCP instances could and should be run by both private and public interests, based on different business models and incentives, it is of great importance that governance of the MCP concept itself maintains its not-for-profit character.

**Service-oriented architecture**: In the context of service-oriented architecture, a service usually refers to a set of related software functionalities that can be re-used for different purposes together with policies that govern and control its usage. The MCP embrace this definition but also envisage a much broader scope that includes services which do not rely solely on machine-to-machine communication, such as services delivered over telephone calls (voice or fax), email, websites, NAVTEX and other “primitive” solutions.

**Proven technologies**: The MCP concept relies on well-proven industry standard technologies, such as web-services, OpenID Connect, X.509 certificates, and the like, but will remain open for, and follow the development of, new and emerging technologies.

## Relations to other maritime standards

The MCP is well aligned with other existing maritime standards - some of which have actually been derived from work done in relation with the MCP. Primary maritime standards / guidelines relating to the MCP include;

* G1128 The Specification of e-navigation technical services

This IALA guideline describes how to create technical service specifications and these are aligned with the format of services registered in the MCP service registry

G1128 was derived from work done on the MCP

* G1157 Web Service Based S-100 Data Exchange

Describes how to create technical services following G1128 that uses web services (internet based)

* G1143 Unique identifiers for maritime resources (MRN)

An IALA guideline that describes MRN unique identifiers which are used throughout MCP

Like G1128, MRN was a "by-product" of the MCP development

* IEC 63173-2 SECOM – Secure exchange and communication of S-100 based products

A standard that describes how to develop services that can deliver S-100 date to a vessel

SECOM requires the existence of an identity registry and a service registry, i.e. MCP

This standard is aligned with both G1128 and G1157

* IALA G1161 – Evaluation-of-Platforms-for-the-Provision-of-Maritime-Services

An IALA guideline that explains the need for all the components of the MCP; identity registry, service registry and messaging service

* G1117 VHF Data Exchange System (VDES) overview

Provides an overview of VDES which extends the Automatic Identification System (AIS) adding new technology. The use of MCP MMS in relation with VDES is described.

## Governance - The MCP Consortium (MCC)

In order to govern the MCP, an international consortium – the Maritime Connectivity Platform Consortium (MCC) – has been established. The MCC is a neutral and independent entity that operates in a strictly not‑for‑profit and transparent way. The consortium has been structured in a similar way to the World Wide Web Consortium, and thus has a small number of host members and a larger number of regular members. All members form the General Assembly – the highest authority of the MCC – in which the host members have a right of veto. All host members are (and must be) not-for-profit organisations.

The MCC was established in 2019 by the following not-for-profit organisations (host members): The *General Lighthouse Authorities of UK and Ireland (GLA)*, the *Korea Research Institute of Ships and Ocean Engineering (KRISO)*, the *German Aerospace Centre (DLR) (former OFFIS),* *Research Institutes of Sweden (RISE)* and the *University of Copenhagen*. The *Danish Maritime Authority (DMA), Swedish Maritime Administration (SMA)* and the *Ministry of Ocean and Fisheries of the Republic of Korea (MOF)* joined the MCC as governmental observers.

In addition to this, an *Advisory Board* for the consortium has been established, which has representatives from relevant international organisations and associations.

The MCC undertakes the following activities:

1. Developing and maintaining all standards associated with the MCP
2. Defining criteria for being MCP service providers
3. Endorsing organisations to be MCP service providers
4. Facilitating root certification for the endorsed MCP identity service providers
5. Developing and maintaining an open source MCP reference implementation
6. Provides a public (free) MCP demonstrator, not for operational usage

The consortium encourages all relevant stakeholders (commercial and non-commercial) to join the Consortium and participate in the development, governance and promotion of the MCP.

# Further information

The MCP consortium operates and maintains a webpage for the MCP, on which all information about the consortium itself and general MCP information including standards and information about MCP instance providers can be found. The webpage can be found at the URL: [www.maritimeconnectivity.net](http://www.maritimeconnectivity.net/)

Annex B

MCC Identity Management and Security:  
General Approach and Basic Requirements

The goal of this document is twofold. The first goal is to define the general approach of the Maritime Connectivity Platform (MCP) with respect to identity management and security. The second goal is to define a set of basic requirements for governing and operating MCP identity services. The intended readers of this document are both technical personnel that are configuring and developing an MCP identity service, and the security head of the running an MCP identity service.

In the remainder of this section, we describe structure, functionality, and governance of the MCP with respect to identity management and security. This is to take into account that the MCP is currently adapting to include governing, integrating and harmonizing several operational MCP services in addition to providing reference implementations and a testbed. The remainder of this document is then structured as follows. In Section 1 with discuss the structure and functionality with references to the related documents [MCC:ID] where we address Identity Management, in [MCC:PKI] we focus on Public Key Infrastructure (PKI), and [MCC:AUTH] is about Authentication and Authorization for Web Services. Section 2 discuss the governance structure and, altogether, we derive a first set of requirements for MCP instances, which we collect into a profile in Section 3.

The outlined approach and requirements, build on the analysis, design choices, and experience with the testbed implementations during the EU projects *EfficienSea2* and *STM Validation Project* and the *SMART Navigation* Project funded by the Republic of Korea. The record of this can be found in the previous white paper "Identity Management and Cyber Security" of the MCP [1]. The current state of the testbed can be taken from the MCP Developer's Guide [2].

# Structure and Functionality

MCP – Maritime Connectivity Platform with MIR – Maritime Identity Registry

MCP Governance (MCC Consortium)

MCP Instance A

MCP Instance B

MCP Instance C

Identity Service B

Identity Service A

Identity Service C

MIR Governance

1. Figure : Structure of MIR within MCP.

The MCP specifies three core components and their interoperability: the Maritime Identity Registry (MIR), the Maritime Service Registry, and the Maritime Messaging Service. The MIR is responsible for identity management and providing security functionality to the other components. As shown in Fig. 1 the MIR consists of MIR governance and several MIR services. In summary, MIR governance and services together typically provide the following functionality:

1. **Identity Management:** The MIR enables that each maritime entity (such as a device, human, organization, service, or ship) can be registered as a participant of the MCP and be equipped with a unique identity. The identity is given in terms of a MRN (Maritime Resource Name). While MIR governance harmonizes the MRN namespace governed by the MCC and sets out criteria for the registration process it is up to the MIR services to implement and have certified concrete identity registries. We use the following terminology:

* MCP entity: An entity registered at some MIR services.
* MCP namespace: The subspace of the MRN namespace that is governed by the MCC.

See [MCC:ID] for details.

1. **Public Key Infrastructure (PKI):** The MIR enables that each MCP entity holds a cryptographic identity in terms of a public/private key pair and a certificate bound to their ID within the MCP. While the cryptographic identity of a MCP entity can change over time (due to updates of key material) the MIR ensures that each MCP entity holds only one *valid* cryptographic identity at any point in time bound to their ID within the MCP. MIR governance provides criteria as to the use and management of cryptographic identities but, similarly to above, it is up to the MIR services to implement and have certified concrete PKIs.   
   See [MCC:PKI] for details.
2. **Authentication and Authorization for Web Services:** The MIR enables that MCP entities benefit from login, single sign-on, and authorization for API access of web services, as well as secure integration of web services based on the widely used standards OAUTH 2.0 and OpenID Connect. To this end MIR governance provides criteria as to interoperability and configurations while the MIR services deliver concrete OAUTH 2.0/OpenID Connect platforms.   
   See [MCC:AUTH] for details.

# Governance and Profiles

The main purpose of the MCP is provide the governance structure for a system with several decentralised operational MCP services and ensuring their interoperability. At the time of writing the number of operational services is expanding. Additionally, these are organised in several ways (governmental, nation and commercial). Hence, the MCP must strike a balance between laying down criteria according to which the emerging deployments can be endorsed as MCP services while remaining open to both, ongoing refinements of the first set of requirements (e.g., with respect to security) as well as new developments and technologies the MCP might wish to utilize (e.g., with respect to distributed PKI). Therefore, the MIR adopts the following approach of profiles.

The MCP will not develop a single set of criteria that every MIR service has to comply with but rather allow several *MIR* *profiles* to coexist. Each MIR profile contains a set of requirements that define what MIR services must guarantee to be compliant with the profile. In addition, a profile will typically contain requirements that define what MIR governance is supposed to guarantee (e.g., to maintain operability and overall security). Each MCP service can choose which of the current MIR profiles it aims to fulfil. While the MCC is not able to carry out assessments as to whether a MIR service adheres to a profile itself (with respect to security) it will endorse organizations that can provide this.

Two distinct MIR profiles can either be compatible in that one is a refinement of the other, or they can be non-compatible. To allow non-compatible profiles ensures that the MCP can evolve into different branches. This is to enable that an MCP service or a cluster of MCP services may adopt new developments without having to ensure downwards compatibility. As usual downwards compatibility entails the risk of being forced to carry over security vulnerabilities or simply being bogged down by obsolete technology. Therefore, the approach of coexisting profiles is also meant to ensure that the MCP can evolve as a whole. The MCC Board will formulate requirements that will pin down how the profiles are managed and harmonized to be approved by the MCC GA.

# Profile "Basic RequirementS"

The profile "Basic Requirements" V1.01 consists of the following requirements:

1. Identity Management as detailed in [MCC:ID]:
   1. MCP MRN syntax as specified in Section 1 of [MCC:ID],
   2. ID1, ID1.1 - ID1.3: Decentral Management of MCP MRNs,
   3. ID2: Transparency of Syntax, and
   4. ID3, ID3.1 - ID3.2: Strong Notion of MCP Entity.
2. PKI as detailed in [MCC:PKI]:
   1. PKI1.1 - PKI1.7: Decentral PKI Concept,
   2. The cryptographic requirements as specified in Section 2 of [MCC:PKI], and
   3. The certificate format as specified in Section 3 of [MCC:PKI].
3. Authentication and Authorization as detailed in [MCC:AUTH]:
   1. OpenID connect as specified in Section 1 of [MCC:AUTH].

The above basic requirements are defined such that fundamental security and interoperability between the services is given. Many details of certificate practice and policy are organisation specific and the MCC will not govern these.

All organisations offering an MCP identity service, must therefore publish the

* Certificate Policy, and
* Certification Practice Statement.

detailing the actual operation of the MCP identity service. The Certificate Policy and Certification Practice Statement must follow best practice and include the Basic Requirement with implementation details where relevant.

References

[1] Identity Management and Cyber Security: White Paper of Maritime Cloud Development Forum, Input Paper to ENAV19

[2] MCP Developers' Guideline. <https://developers.maritimeconnectivity.net/identity/index.html>

[[MCC:ID] Identity Management and Security: Identity Management](https://www.iana.org/assignments/urn-formal/mrn)

[MCC:PKI] MCC Identity Management and Security: Public Key Infrastructure (PKI)

[MCC:AUTH] MCC Identity Management and Security: Authentication and Authorization for Web Services

Annex C

MCC Identity Management and Security:   
Identity Management

The MCP namespace is a subspace of the *Maritime Resource Name (MRN)* space [1], which is an official URN namespace. The syntax definitions below use the Augmented Backus-Naur Form as specified in [RFC5234].

# The MCP Namespace

The syntax for an MRN is as follows [1]:

<MRN> ::= "urn" ":" "mrn" ":" <OID> ":" <OSS>

[ rq-components ]

[ "#" f-component ]

<OID> ::= (alphanum) 0\*20(alphanum / "-") (alphanum)

<OSS> ::= <OSNID> ":" <OSNS>

<OSNID> ::= (alphanum) 0\*32(alphanum / "-") (alphanum)

<OSNS> ::= pchar \*(pchar / "/")

The rules for alphanum and pchar are defined in [RFC3986].

The optional rq-components and f-component are specified in [RFC8141].

"mrn" specifies that the URN is within the MRN namespace. The *Organization ID (OID)* refers to an organization that is assigned a subspace of MRNs such as IMO, IALA, or the MCP. Syntactically, it is a string that must be unique across the "mrn" scheme. The *Organization Specific String (OSS)* is specified and managed by the governing organization in a consistent way conform to the definitions of the MRN namespace. In particular, each organization must structure the OSS into two parts: the *Organization Specific Namespace ID (OSNID),* and the *Organization Specific Namespace String (OSNS)*. The OSNID identifies a particular type of resource (uniquely within the governing organization), while the OSNS identifies the particular resource (uniquely for its type within the governing organization). Altogether, this ensures that the resulting URN is globally unique.

For a MRN governed by the MCC the OID reads "mcp", and the OSNID specifies one of the following types used within the MCP: device, organization, user, vessel, service, mir, mms, and msr. The latter three types are to be used for entities of the three MCP components MIR, Maritime Messaging Service, and Maritime Service Registry respectively. Moreover, the definition of the OSNS takes into account the distributed structure of the MCP: identities can be provided and managed by several identity providers. In detail, the syntax of a *MRN governed by the MCC* (short: *MCP MRN* or *MCP name*) is as follows:

<MCP-MRN> ::= "urn" ":" "mrn" ":" "mcp" ":" <MCP-TYPE> ":" <IPID> ":" <IPSS>

<MCP-TYPE> ::= "device" | "org" | "user" | "vessel" | "service" |

"mir" | "mms" | "msr"

<IPID> ::= <CountryCode> | (alphanum) 0\*20(alphanum / "-") (alphanum)

<IPSS> ::= pchar \*(pchar / "/")

"mcp" specifies that the governing organization is the MCC. The next element is *MCP-TYPE.* As explained above this pins down one of the types currently used within the MCP. The *Identity Provider ID (IPID)* refers to a national authority or other kind of organization that acts as an identity provider within the MCP. If the identity provider is a national authority then the IPID must be a country code as defined by ISO 3166-1 alpha-2. Otherwise it will be a string of the same syntax as that for OIDs. The IPID must be unique across the urn:mrn:mcp namespace. The *Identity Provider Specific String (IPSS)* can be defined and managed by the respective identity provider in a way that is consistent and conforms to the definitions of the MRN namespace and requirements laid down by the MCC. In particular, the identity provider must ensure that the IPSS identifies a particular resource uniquely for its type within the domain of the identity provider. Altogether, this will ensure that the resulting URN is globally unique.

Examples:

* urn:mrn:mcp:user:dma:alice - valid MCP MRN for a user, where dma specifies the ID Provider, and the subsequent IPSS string is defined to give the username.
* urn:mrn:iala:aton:gb:sco:6789-1 - valid MRN for a marine aid to navigation (AtoN), where gb stands for United Kingdom, sco for Scotland, and the number is the scottish asset identifier. The example is from [4]. This is *not* a MCP MRN.
* urn:mrn:mcp:device:mirX:aton:gb:sco:6789-1 - valid MCP MRN for the same AtoN, where mirX specifies the ID Provider, and the subsequent IPSS string is defined to first specify the type of the device, and then to follow the country-specific convention of the IALA scheme.

The following requirements pin down that and how the MCP namespace can be managed decentrally.

**ID1 The MCC can delegate the assignment of part of the MCP namespace to other organizations that act as identity providers. More concretely, this means that the organization, say X, must hold an IPID, say string "nameofx", and is then responsible for the namespace with the prefix "urn:mrn:mcp:<MCP-TYPE>:nameofx".**

**ID1.1 The MCC must ensure that each IPID refers to at most one identity provider.**

**ID1.2 Each Identity Provider must ensure to respect all syntax prescribed in the MRN specification. Moreover, each Identity Provider must ensure that each IPSS of their name space refers to at most one entity of their domain.**

**ID1.3 The MCC can give recommendations on how to structure the IPSS, e.g. to harmonize the syntax for particular types of entities. These recommendations will not be binding. However, the MCC reserves the right that a particular syntax can be binding with respect to conformance to certain profiles.**

Note that ID1.1 and the second part of ID1.2 together ensure uniqueness: one MCP MRN is assigned to at most one entity. This is a general requirement for any URN. ID1.3 allows us to harmonize the IP specific strings while not principally restricting the governance of an IP provider over its namespace.

Example:

Say there are two ID providers, MIR X and MIR Y. Assume the MCC assigns the IPID "mirx" to MIR X, and "miry" to MIR Y respectively. The MCC must ensure that the strings "mirx" and "miry" are not assigned to any other MIR. MIR X is responsible for the namespace "urn:mrn:mcp:<MCP-TYPE>:mirx:\*", and MIR Y is responsible for the namespace "urn:mrn:mcp:<MCP-TYPE>:miry:\*" respectively. They might decide to employ the same syntax for the IP specific string, and make this part of a profile they both adhere to. Other ID providers are not bound to use the same syntax. However, if they do not comply to it they cannot be compliant to that profile.

Finally, the following is to ensure a good practice of transparency and interoperability:

**ID2 Every Identity Provider shall publish the syntax that describes their name space as well as provide a reference implementation that recognizes the strings of their namespace.**

### Further Requirements for a Strong Notion of Maritime Identity

The vision of the MCP is to enable a strong concept of digital maritime identity. Hence, we put down requirements that go beyond what is commonly required of URNs. Firstly, we require that every MCP entity must have a name within the MCP namespace. This gives a clear concept of MCP entity: those entities that are registered under an MCP MRN name. Secondly, we require that one MCP entity cannot have several MCP MRNs. For example, this supports law enforcement: When a maritime entity gets discovered and blacklisted for "bad behaviour" (e.g. fake emergency signalling) then it cannot simply revert to another MCP identity and participate as usual.

**ID3 Every entity of the MCP shall hold exactly one MCP MRN (i.e. MRN governed by the MCP). This does not exclude that a MCP entity can hold other MRNs, but these must be within namespaces governed by other organizations (e.g. IMO). Also, we will formulate exceptions concerning legacy MRNs within the MCP namespace.**

Hence, the AtoN in the example above can be identified by its IALA MRN, or its MCP MRN respectively. However, Requirement ID3 rules out that the AtoN can be referred to by a second MCP MRN. The following requirements implement ID3 in a decentral manner.

**ID3.1 Each Identity Provider shall ensure that each entity they register holds at most one MCP MRN within their namespace.**

**ID3.2 Each holder of a maritime entity shall ensure that this entity is registered with at most one MCP identity provider.**

Note that practically it won't be possible to avoid that a "bad player" will seek to register their entity at several different Identity Providers and thereby obtain several MCP identities for it. However, ID3.1 ensures that they can obtain at most as many identities as there exist Identity Providers. And ID3.2 ensures that when it is discovered that an entity holds several MCP MRNs of different providers then it is clear that they have violated a rule (and action can be tied to this).

References

[1] MRN Specification: <https://www.iana.org/assignments/urn-formal/mrn>

Appendix A.A SpeCIFICATION of SMART MRN SyntaX

KOR MRN namespace and its conversion to MCP MRN which is used in SMART-Navigation Project are given as an example of how an identity provider can utilize their own MRN namespace in the context of MCP. The string “KOR” states *Republic of Korea*, the governance body of KOR MRN and the *IPID* of MCP MRN. The KOR MRN is expected to govern the digital identity of maritime resources and related entities in a national level, enabling the use MCP services developed by the SMART-Navigation Project. In the context of MCP, the Republic of Korea will be an organization entity that provides identities through KOR and MCP MRNs. In conformance to this document, the SMART-Navigation Project uses the MCP MRN for every interaction with MIR by using the “mrn" attribute in the certificate profile and the KOR MRN for national identity management which is stored to the “mrnSubsidiary*”* attribute, where one-to-one mapping between two namespaces provides. The following description will more focus on the one-to-one mapping of two MRN namespaces rather than explaining the details of each types of entities. The syntax definitions below use the Augmented Backus-Naur Form (ABNF) as specified in [RFC5234].

The syntax for a KOR-MRN used in SMART-Navigation Project is as follows:

<KOR-MRN> ::= "urn" ":" "mrn" ":" "kor" ":" <KOR-TYPE> ":" <ISID> ":" <ISSS>

<KOR-TYPE> ::= "vessel" | "device" | "user" | "service" ":" <SST> | "system" | "mcp"  
<SST> ::= “instance" [ ":" <SIT> ] | "specification" | "design"

<SIT> ::= "web" | "app"  
<ISID> ::= (alphanum) 0\*20(alphanum / "-") (alphanum)  
<ISSS> ::= pchar \*(pchar / "/")

The *OID* of KOR-MRN is "kor"and the *OSNID* starts from one of the eight types, *KOR-TYPE,* currently used within the KOR context: “vessel", “device", “user”, “service", “system", and “mcp". Note that the absence of the type "*org*" compared to the *MCP-TYPE* indicates the organization is the one and only, Republic of Korea, in the context of SMART Navigation Project. The “service” type has *Service SubType (SST)* as following sub-element which corresponds to the documentation types of the IALA's G1128 e-Navigation technical service specification guideline. The KOR MRN defines *Service Instance Type (SIT)* for the “instance” subtype to specify the target terminal of the service and locates it to the end of the “instance” *SST* as a hierarchy.

The *Identification System ID (ISID)* refers to an external or internal identification system that governs a unique identifier of an entity for its own purpose. The SMART Navigation Project governs and restricts the *ISID* for each type. The *Identification System Specific String (ISSS)* is specified and managed by the governing identification system in a consistent way. Taking both into account an example of a vessel is given as “imo:8814276”, where “imo” and the actual imo number of the vessel “8814276” are represented in *ISID* and *ISSS* respectively, so as to make the vessel’s full KOR MRN to “urn:mrn:kor:vessel:imo:8814276”. The “mcp” type utilizes the *ISID* to indicate the MCP components where the “mms” is only one used in the project for the time of writing.

In order to establish the interoperability SMART Navigation Project uses the *IPSS* of the MCP MRN to build the mapping between the KOR MRN and the MCP MRN. In detail, the syntax of a MCP MRN of the SMART Navigation project, *KOR-MCP-MRN*, is as follows:

<KOR-MCP-MRN> ::= "urn" ":" "mrn" ":" "mcp" ":" <MCP-TYPE> ":" "kor" ":" <KOR-IPSS>

<KOR-IPSS> ::= [ <SST> ":" | <DST> ":" ] <ISID> ":" <ISSS> | <ISSS>  
<SST> ::= "instance" [ ":" <SIT> ] | "specification" | "design"

<SIT> ::= "web" | "app"

<DST> ::= “system"

<ISID> ::= (alphanum) 0\*20(alphanum / "-") (alphanum)  
<ISSS> ::= pchar \*(pchar / "/")

Note that "kor" represents both the *IPID* and an *organization* entity in the MCP type for the sake of reducing the redundancy, i.e., “kor:kor”. Thus the MIR implementation will have the ability to interpret this context as a configurable option. For the KOR MRN types which corresponds to those are in MCP MRN in terms of name, definition, and purpose in use, the *ISID* and the *ISSS* afterward take the place of *IPSS*, namely *KOR-IPSS*. The *KOR-IPSS* can optionally take *Service SubType (SST)* or *Device SubType (DST)* from beginning to represent the same subtypes of the KOR MRN, where a “instance” subtype can have *Service Instance Type (SIT)* at the end in the same manner with the KOR MRN. The *DST* is employed to embrace the “system” of the KOR MRNas the subtype of “device” of the MCP MRN. Please note that the actual use of the *SST* and the *DST* should be constrained to specific MCP types, i.e., the *SST* for services and the *DST* for device, but is formulated here in a simple manner. The identity provider, by restricting the identification systems, should guarantee that the *ISID* does not conflict to the value of either *SST*, *DST*, or *SIT*. The “mcp” type in the KOR MRN is converted by locating the “mcp” to the *OID* of the MCP MRN, the “mms” to the *MCP-TYPE* by meaning of the *ISID*, and *ISSS* at the end which is from the *ISSS* of the KOR MRN for the MMS, e.g., “urn:mrn:mcp:mms:kor:smart001”. As the SMART-Navigation Project proceeds and elaborates the use of MRNs in reality, the presented MRN syntax and its mapping can be changed.

Annex D

MCC Identity Management and Security:  
Public Key Infrastructure (PKI)

In addition to a unique ID in the form of an MCP MRN each MCP entity is provided with a cryptographic identity. This consists of a public/private key pair and a certificate for the public key bound to their ID. In the following, we describe the concept of the PKI that enables this, and a first set of requirements for it. We also identify issues that need to be addressed and refined in the future.

We proceed as follows. In Section 1 we explain the MCP core concepts of cryptographic identity. Section 2 details the decentral PKI. In Section 3 we specify the requirements on cryptographic keys and mechanisms. In Section 4 the format of MCP certificates is described. Moreover, in Section 5 we show how a service can use an intermediary level of service certificates. For example, this is necessary if a service comes with cryptographic requirements that do not allow the direct use of the MCP ID credentials. Finally, in Section 6 we identify further aspects to be considered.

# Cryptographic Identity

The cryptographic ID of an MCP entity consists of a public/private key pair and a certificate bound to their MRN. The certificate must be issued by the identity provider responsible for the entity. The latter is clearly defined by the IPID string within the MRN of the entity.

Given an entity with MRN A (short: entity A), and its identity provider P, we use the following notation:

* + pkA is the public key of A, and prA is the private key of A respectively.
  + certP(A, pkA, V) is the certificate of A signed by its identity provider P. The certificate contains the MRN A, the public key of A, and the validity period V of the certificate. (The precise format is provided in Section 3.3.)

The key pair is for use with a digital signature scheme. Hence, each MCP entity A can be verified by another party B to be the originator of a message or other data. As usual this involves the following steps:

1. Entity A signs the message, say M, using its private key prA. The result is a cyphertext C.
2. Entity A makes available its certificate certP(A, pkA, V), and transmits the signed message M||C.
3. Entity B obtains the certificate and receives the signed message.
4. Entity B validates the certificate. As a result, B trusts that pkA is the valid public key of the MCP entity with MRN A. (Necessary requirements on certificate validation will be specified.).
5. Entity B uses pkA to verify whether the ciphertext C is indeed the digital signature of M. If the verification is successful, then B has assurance that M indeed originates from A. (Note that without the fourth step B only has assurance that M originates from the holder of the private key counterpart of pkA.)

Note that B does not necessarily need to be an MCP entity.

At the time of writing the MCC does not prescribe a policy on how to use ID credentials. They could be used as long-term credentials to obtain short-term credentials for use for a service, or they could be directly used as working credentials.

# Decentral PKI

One of the principles of the MCP is to make do without a global notion of trust: in the international context of the MCP we cannot expect that all parties trust each other and each other's security management uniformly. Rather the goal of the MCP is to provide the transparency that enables organizations to decide on whom to trust in which context, and to provide the technical framework to translate such decisions into executable policies. For the PKI we put forward the following three principles:

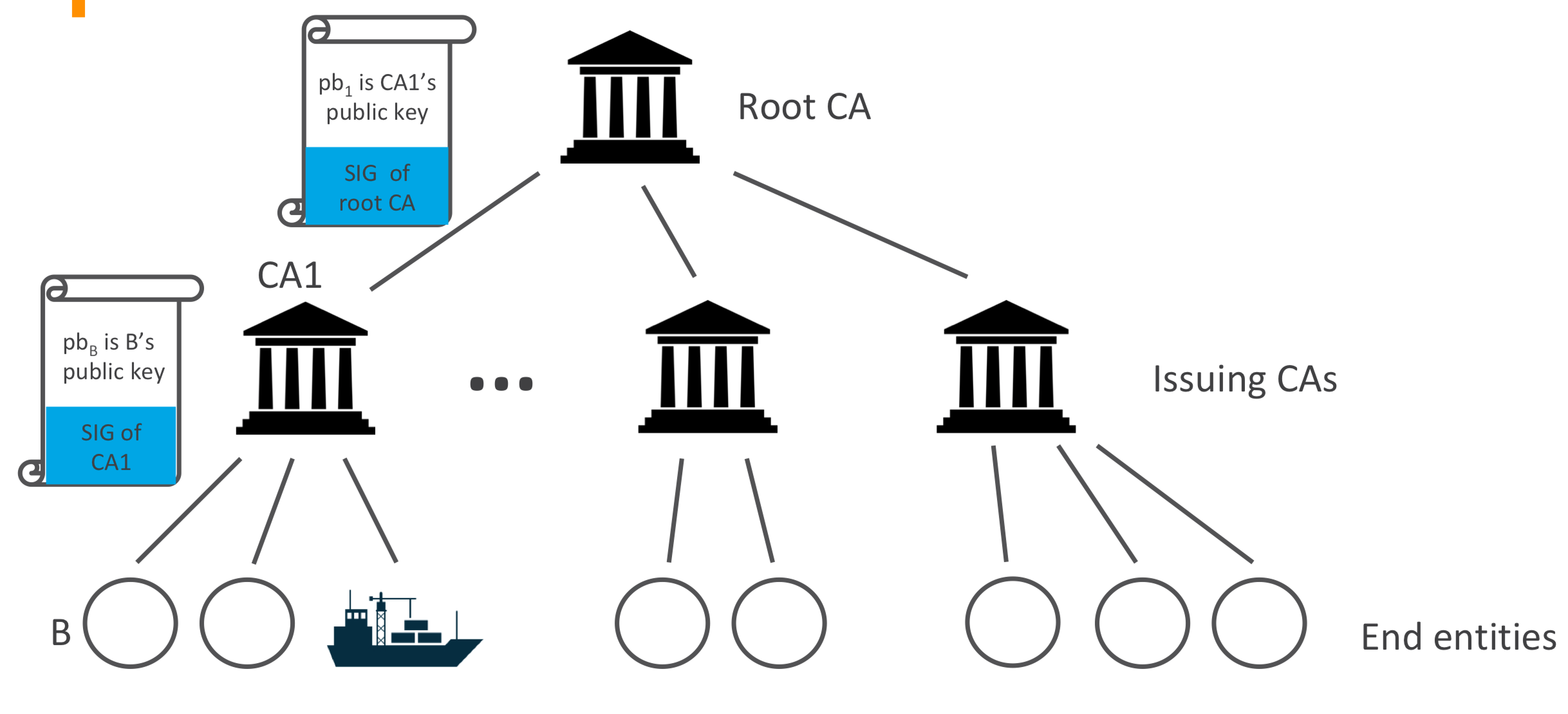
1. A security breach within the realm of one identity provider's PKI instance shall not enable an attacker to impersonate an entity within the realm (i.e. namespace) of another identity provider;
2. A security breach within an organization or set of organizations predefined by the MCC to carry out some tasks shall not enable an attacker to impersonate any MCP entity unless the identity provider of the entity coincides with (one of) the organization(s). In short this means identity providers' PKI instances can always remain secure independently from any central or distributed management by the MCC;
3. It is possible for everyone to obtain assurance as to the security level of any identity provider's PKI instance.
4. 

Figure 2: Hierarchical X.509 PKI Structure

The first two principles immediately imply that a classical hierarchical PKI with a root CA hosted by the MCC won't do. We illustrate this by giving examples of impersonation attacks. Assume a hierarchical PKI structure with MCC root CA as shown in Fig. 2. To verify a MCP certificate certP(A, pkA, V) a receiving party has to verify the signature of the identity provider P with the public key of P provided in an intermediary certificate certMCC(P, pkP, V) issued by the MCC root CA. Further, to verify the intermediary certificate the receiving party has to verify the signature of the MCC with the public key provided in the MCC root certificate certMCC(MCC, pkMCC, V). The latter provides the trust anchor accepted by the receiving party.

*Examples:*

1. *Single point of attack:* Assume the MCC root key prMCC is compromised. This will allow an attacker to impersonate any MCP entity A. Say P is the identity provider responsible for A. First, the attacker generates a key pair pkI(P), prI(P) and generates a fake certificate for P with his own key pkI(P): certMCC(P, pkI(P), V). This is possible since the attacker knows prMCC. Second, the attacker generates a key pair pkI(A), prI(A) and generates a fake certificate for A and his own key pkI(A): certI(P)(P, pkI(A), V). This is possible since he knows prI(P). Altogether, the attacker can now present a valid certificate chain that establishes pkI(A) to be the public key of A while he knows the private counterpart prI(A). Hence, he can impersonate A. Altogether this violates principle 2 above.
2. *Weakest Link I:* Say the attacker wishes to impersonate entity A of identity provider P. Note that in classic X.509 certificate validation it is only verified that there is a certificate chain up to a trusted root certificate. Say the attacker can easily obtain fake certificates signed by another identity provider P', perhaps, because the attacker is a state actor and P' is under his governance. Then, analogously to above, he only needs to generate his own key pair pbI(A), prI(A) and generate a fake certificate for A and pbI(A) signed by P': certP'(A, pbI(A), V). Since there is no check whether P' is indeed the identity provider of A this gives the attacker a valid certificate chain and corresponding private key, with which he can impersonate A. This violates principle 1 above.
3. *Weakest Link II:* Assume P is an identity provider of low security level, e.g., with a vetting procedure that can easily be undermined. Assume an attacker aims to join the MCP under a false identity so that he is able to inject fake messages without the risk of being traced. The attacker will simply choose P as the identity provider from whom to obtain his false identity. Without principle 3 in place a receiving party has no way to consider the low security level of P when processing the information within the message.

This motivates the following requirements:

**PKI1.1 (PKI Structure) There shall be no root CA at the top level of the MCC. Every identity provider that hosts a PKI instance is to provide their own root CA.**

**PKI1.2 (Validation of IPID) When a receiving party verifies a MCP certificate, say certP(A, pkA, V), it must verify that the certificate is indeed signed by the identity provider responsible for A. The identity provider responsible for A can be read by the receiving party from the IDIP string within the MRN A.**

The following requirements ensure that information on root certificates and security levels are made publicly available.

**PKI1.3 Every identity provider is to publish their currently valid root certificate in a suitable fashion. For example, this can be made accessible via their web page, or they can commission a generally accepted authority or assurer to do so.**

**PKI1.4 Every identity provider must publish the Certificate Policy, and Certification Practice Statement detailing the actual operation of the MIR service. The Certificate Policy and Certification Practice Statement must follow best practice and include the Basic Requirement with implementation details where relevant.**

**PKI1.5 Every identity provider is to generate and publish a root certificate revocation list (CRL) containing any revoked issuing CA’s. All active issuing CA’s must include an endpoint to the root CRL.**

**PKI1.6 Every identity provider is to generate and publish CRL’s containing any revoked MCP ID certificates for each of its issuing CA’s.**

**PKI1.7 Every identity provider is to support and provide an endpoint for an online certificate status protocol (OCSP) responder.**

From this the MCC will provide a secure way to automatically find and give basic trust in the authenticity of the MCP identity providers.

**PKI1.8 The MCC will publish one current and valid root certificate that is used to authenticate (sign) each identity provider certificate.**

**PKI1.9 The MCC will provide a list of identity providers, links to obtain their root certificates, security levels, and signatures of certificates signed with the given root certificate. Including a revocation list.**

The MCC board will manage this root certificate, and detail guidelines and rules for its operation; this includes the Certificate Policy and Certification Practice Statement. These rules should follow best practice and will be published on the MCC website. This will also include location of valid certificates, signed certificates, and revocation lists. There will also be example code on how to interact with this. The management can be delegated by the board to a specific host member.

Note, that this does not break with the above claim that the MCC will not work as a root CA. This certificate is intended to only give a basic trust, meaning that the authenticated MCP instances are endorsed by the MCC and, to the best of MCCs knowledge, are operating within rules and guidelines as defined by the MCC. As stated earlier, full trust can only be established between each organisation and if deeper trust is needed, we must refer to other PKI systems or external certification organisations. Details of this is ongoing work and will be addressed at a future point in time.

## Application programming interface and implementation

The details of the implementation can be found in [1]. This gives the API for MCP Root Certificates Storage Service. It also provides coding examples of how the API can be used.

## Security Requirements and Profiles

Security requirements to be defined will fall into the following categories:

1. Requirements on vetting. This can be specified similarly to classes such as EV (extended validation).
2. Requirements on certificate revocation.
3. Requirements on the validity period of certificates.
4. Requirements on security of keys and origin of signing - CA side (including requirements on HSMs).
5. Requirements on security of keys and origin of signing - MCP entity side (including requirements on HSMs).

The requirements will be dependent on the currently emerging profiles:

MCP entities generate their ID key pair themselves and in own responsibility and provide this to the responsible CA for certification.

The CA (perhaps together with a manufacturer) provisions the initial ID key pair and certificate securely within HSMs (for/within endpoints) to be distributed to the MCP entities.

# Cryptographic Requirements

The cryptographic mechanism approved for ID digital signatures is the Elliptic Curve Digital Signature Algorithm (ECDSA) [FIPS 186-3] with the appropriate hash algorithm from the SHA-2 family [FIPS 180-3]. The approved elliptic curve domain parameters are specified by reference to standardized curves. Currently the following combinations are approved:

|  |  |  |
| --- | --- | --- |
| ECDSA Key Size (bits) | Hash Algorithm | Elliptic Curve Domain Parameters |
| 384 | SHA-384 | P-384 [FIPS 186-3] (= secp384r1) |
| 256 | SHA-256 | P-256 [FIPS 186-3] (= secp256r1) |

**Future extensions:**

* Requirements on key pair generation and checks for key pair validity will be given by reference to standards. Also, we will check whether there are relevant recommendations in the last version [FIPS 186-5].
* Currently the only approved curve parameters are the NIST recommended curves. It will be checked whether this needs to be extended with regards to cryptographic recommendations of member states' security agencies (e.g., BSI and brainpool curves). Also, if a curve is found to be weak in the future it will be good to have an alternative curve per key size already approved.
* We will also consider matters of crypto agility.

# Certificate Format

We now specify the format of the MCP ID certificates. The format is based on the X.509 standard [2]. The standard information present in an X.509 certificate includes:

* **Version** – which X.509 version applies to the certificate (which indicates what data the certificate must include).
* **Serial number** – A unique assigned serial number that distinguishes it from other certificates.
* **Algorithm information** – the algorithm used to sign the certificate.
* **Issuer distinguished name** – the name of the entity issuing the certificate (MCP).
* **Validity period of the certificate** – start/end date and time. The length of the validity period of a certificate depends on the type of the entity that the certificate has been issued to. If the certificate has been issued to a user or an organization the length of the validity period MUST not be more than 2 years. For other entity types, such as devices or vessels, the validity period of a certificate should be in relation to the length of the period between maintenances of the equipment that the certificate has been issued to.
* **Subject distinguished name** – the name of the identity the certificate is issued to.
* **Subject public key information** – the public key associated with the identity.

The Subject distinguished name field consists of the following items:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Field** | **User** | **Vessel** | **Device** | **Service** | **MMS** | **Organization** |
| CN (CommonName) | Full name | Vessel name | Device name | Service Domain Name | MMS name | Organization Name |
| O (Organization) | Organization MRN | | | | | |
| OU (Organizational Unit) | "user" | "vessel" | "device" | "service" | "mms" | "organization" |
| E (Email) | User email |  |  |  |  | Organization email |
| C (Country) | Organization country code | | | | | |
| UID | Entity MRN | | | | | Organization MRN |

*Example:* The following gives an example of the Subject distinguished name field for a vessel with identity provider idp1:

C=DK, O=urn:mrn:mcp:org:idp1:dma, OU=vessel, CN=JENS SØRENSEN, UID=urn:mrn:mcp:vessel:idp1:dma:jens-soerensen

In addition to the information stored in the standard X.509 attributes listed above, the X509v3 extension SubjectAlternativeName (SAN) extension is used to store extra information. There already exists some predefined fields for the SAN extension, but they do not match the need we have for maritime related fields. Therefore the “otherName” field is used, which allows for using an Object Identifier (OID) to define custom fields. The OIDs currently used are not registered at ITU, but are randomly generated using a tool provided by ITU (see <http://www.itu.int/en/ITU-T/asn1/Pages/UUID/uuids.aspx>). See the table below for the fields defined, the OIDs of the fields and which kind of entities that use the fields.

|  |  |  |
| --- | --- | --- |
| **Field** | **OID** | **Used by** |
| Flagstate | 2.25.323100633285601570573910217875371967771 | Vessels, Services |
| Callsign | 2.25.208070283325144527098121348946972755227 | Vessels, Services |
| IMO number | 2.25.291283622413876360871493815653100799259 | Vessels, Services |
| MMSI number | 2.25.328433707816814908768060331477217690907 | Vessels, Services |
| AIS shiptype | 2.25.107857171638679641902842130101018412315 | Vessels, Services |
| Port of register | 2.25.285632790821948647314354670918887798603 | Vessels, Services |
| Ship MRN | 2.25.268095117363717005222833833642941669792 | Services |
| MRN | 2.25.271477598449775373676560215839310464283 | Vessels, Users, Devices, Services, MMS |
| Permissions | 2.25.174437629172304915481663724171734402331 | Vessels, Users, Devices, Services, MMS |
| Subsidiary MRN | 2.25.133833610339604538603087183843785923701 | Vessels, Users, Devices, Services, MMS |
| Home MMS URL | 2.25.171344478791913547554566856023141401757 | Vessels, Users, Devices, Services, MMS |
| URL | 2.25.245076023612240385163414144226581328607 | MMS |

Encoding of string values in certificates must follow the specifications defined in RFC 5280, and where possible it is highly recommended to use UTF-8.

To be able to check the revocation status of a given certificate all MCP ID certificates must include an endpoint to an up-to-date certificate revocation list that is signed by the issuing CA that has signed the certificate in question according to RFC 5280[2].

Additionally, all MCP ID certificates must also include an endpoint to an OCSP responder that is able to return the revocation status of the certificate in question according to RFC 6960[3].

# Service Certificates

Several maritime services come with requirements concerning cryptography and/or certificate formats that might make it impossible to employ MCP ID credentials directly. For example, if an identity provider issues certificates for ECDSA with 384 bits key size this will not meet the real-time requirements and low bandwidth conditions of AIS and VDES [TODO: ref Gareth's paper]. While the service must then provide its own CA the service CA can automatically issue its service certificates based on MCP ID credentials. We provide an example of how this can be done based on the concept of *certificate signing requests (CSRs)*, also known as *certification requests*. The most common format for CSRs is defined by the PKCS#10 standard [RFC 2986].

*Example:* In the following we show the steps carried out by an MCP entity to request a service certificate, and the steps performed by the service CA to issue the certificate respectively. The example follows the implementation of the Haptik CA from the project Haptik[4]. This functionality will also be embedded in a web service and secured by the MCP OpenID Connect/OAuth 2.0 framework.

The MCP entity

1. generates a fresh key pair for use with the service,
2. builds a X.500 name for use in the service certificate,
3. builds a corresponding PKCS#10 CSR,
4. signs the CSR with their private MCP ID key, and
5. sends the CSR together with their MCP ID certificate to the service CA.

On receipt the service CA

1. checks whether the CSR is valid,
2. builds a X.509v3 certificate according to the CSR and additional information provided by the CA such as issuer, serial number, and validity period,
3. signs this with their CA private key, and
4. sends the new certificate to the requesting MCP party.

**Note:** This pattern is also applicable when the MCP ID keys are mainly used as enrolment keys to obtain shorter lived "working keys".

# Integration of Other PKI Systems

In the spirit of decentralisation the PKI shall remain open for PKI systems other than X.509, and be agile for updates of certificate formats. Care will be taken to accommodate the necessary flexibility when defining usage of certificates. More to this point is provided by example of the P3KI approach.

References

1. MCP Root Certificates Storage Service; Oliver Steensen-Bech Haagh
2. RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile; Internet Engineering Taskforce
3. RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP; Internet Engineering Taskforce
4. https://haptik.io

Annex E

MCC Identity Management and Security:  
Authentication and Authorization for Web Services

In some situations, it is inconvenient or impossible for an entity to authenticate with its MIR-issued certificate to a relying party. As an alternative the relying party can request a MIR to authenticate the entity online using the OpenID Connect () token-based authentication protocol. Therefore, each MIR must support (see ).

Section 1 of this document specifies how OIDC should be used in the context of authentication by a MIR, while in Section 2 we will discuss how external organisations can be federated.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in https://openid.net/specs/openid-connect-core-1\_0.html [4].

# MCP usage of OpenID Connect

A relying party, for example a web service provider, can choose to authenticate service consumers by delegating the authentication to a MIR. In practice this works like “Login with LinkedIn” and similar solutions: the service consumer (a user, an app) is directed to the MIR which will (if needed re-)authenticate the consumer and then direct the consumer back to the relying party with (a reference to) a token. The token can only be processed by the relying party and contains information about the authenticated service consumer. The relying party can now decide to which degree it will serve the consumer.

The token is an OIDC *Identity Token* and can be thought of as a very short-lived certificate issued by the MIR. The fields of a MIR issued certificate correspond to OIDC *claims* in the OIDC Identity Token. A relying party could offer authentication both by means of a certificate as well as by means of an OIDC Identity Token. In both cases, after some processing, the relying party ends up with information on the identity of the authenticated consumer, including the MRN, as asserted by the MIR.

**AUTH1.1 Any Identity Token issued by a MIR MUST contain both the claims required by OIDC (*iss*, *aud*, *exp*, *iat*, and *sub*) as well as the relevant claims from the table below, according to the type of the authenticated party (as defined in MCP-IDSEC3). Such Identity Token MAY contain other, additional, claims as allowed by OIDC.**

| **X509 Field Name** | **Open ID Connect Claim** | **Used for entity type** |
| --- | --- | --- |
| Subject Name | uid | Vessel, User, Device, Service, MMS |
| Flagstate | flagstate | Vessel, Service |
| Callsign | callsign | Vessel, Service |
| IMO number | imo\_number | Vessel, Service |
| MMSI number | mmsi | Vessel, Service |
| AIS shiptype | ais\_type | Vessel, Service |
| Port of register | registered\_port | Vessel, Service |
| Ship MRN | ship\_mrn | Service |
| MRN | mrn | Vessel, User, Device, Service, MMS |
| Permissions | permissions | Vessel, User, Device, Service, MMS |
| Subsidiary MRN | subsidiary\_mrn | Vessel, User, Device, Service, MMS |
| Home MMS URL | mms\_url | Vessel, User, Device, Service, MMS |
| URL | url | MMS |

Note that the certificate Subject is represented as an *uid* claim. This as most OIDC implementations are geared to using the *sub* claim to convey a *pairwise Subject Identifier* (a persistent pseudonym).

# Identity Provider Proxying

A MIR that is requested by a relying party to authenticate a service consumer using the OIDC protocol can in turn delegate the authentication request to a 3rd party, using OIDC or other means. Such MIR acts as a *proxy* between the relying party and the next identity provider.

**AUTH2.1 Whenever a MIR does rely on another *legal entity* for the actual authentication it SHOULD include relevant OIDC claims to reflect this in the issued *Identity Token*.**

**AUTH2.2 A MIR SHOULD NOT rely on another legal entity for actual authentication, unless that entity is a MIR in *good status* as defined in .**

References

1. MCP-IDSEC3: MCC Identity Management and Security: Public Key Infrastructure (PKI) 1.0, MCP Consortium 2021.
2. MCP-GEN4: Requirements for MCP identity service providers 1.0, MCP Consortium 2021.
3. [OIDC](https://openid.net/specs/openid-connect-core-1_0.html): OpenID Connect Core 1.0, N.Sakimura et al. https://openid.net/specs/openid-connect-core-1\_0.html
4. [RFC2119](https://www.rfc-editor.org/rfc/rfc2119.txt): Key words for use in RFCs to Indicate Requirement Levels, S. Bradner. The Internet Society, March 1997. https://www.rfc-editor.org/rfc/rfc2119.txt

1. Input document number, to be assigned by the Committee Secretary [↑](#footnote-ref-1)
2. Leave open if uncertain [↑](#footnote-ref-2)
3. The digital services implement the technical services as described by the IMO concept for implementing maritime services. [↑](#footnote-ref-3)