Input paper for the following Committee(s):	check as appropriate	Purpose of paper:
x ARM □ ENG	□ PAP	□ Input
x ENAV □ VTS		**x** Information

Agenda item [2]	n.n
Technical Domain / Task Number [2]	…………………………………
Author(s) / Submitter(s)	OFFIS, Germany
	Sitronics KT JSC, Russia
	KRISO, Republic of Korea
	Sternula, Denmark
	GLA, UK & Ireland
	Fintraffic, Finland

Status on MCP and its role in e-Navigation

1   SUMMARY

The Maritime Connectivity Platform (MCP) has recently reached a major milestone. This paper therefore provides a status update on the development and realisation of the MCP, as well as describing its intended place in the overall e-Navigation concept and the digitalisation process of the maritime domain at large.

As will probably be known to many, the MCP consists of three main components - the Maritime Identity Registry (MIR), the Maritime Service Registry (MSR) and the Maritime Messaging Service (MMS). When the MCP has been presented, the word was always that this is work in progress. Now a major milestone has been reached by the fact that the MIR component of the MCP has finally been defined. This means that there is now a description of what exactly MIR is and what it means to be an MCP identity service provider.

This document describes from the highest level, the different building blocks (standards and guidelines) that have been written in order to facilitate the realisation of e-navigation (exchange of data in the maritime domain), and it describes MCP with its different core components and how it fits into this context.

It is the vision that the MCP will be used as the platform for providing secure and reliable digital (e-navigation) services to the maritime domain from both IALA members and other relevant organisations.

2   BACKGROUND

The e-Navigation process has been underway since around 2006, and many documents, standards and guidelines have been developed during this period. In this context we would like to highlight some of the most important documents;

1. Strategy for the development and implementation of e-navigation (IMO MSC85/26/Add.1, annex 20)

---

1 Input document number, to be assigned by the Committee Secretary
2 Leave open if uncertain

2. Initial description of maritime services in the context of e-navigation (IMO MSC.1/Circ. 1610)

3. The specification of e-navigation technical services (IALA G1128)

4. Unique identifiers for maritime resources (IALA G1143)

5. IHO Universal Hydrographic Data Model (IHO S-100)

6. Guidance on the definition and harmonization of the format and structure of maritime services in the context of e-navigation (IMO Resolution MSC.467(101))

7. Web Service Based S-100 Data Exchange (IALA G1157)

8. Secure exchange and communication of S-100 based products (SECOM) (IEC 63173-2)

9. Evaluation of platforms for the provision of maritime services in the context of e-navigation (IALA G1161)

All these components together facilitate the definition, implementation and provision of **technical** services, i.e. digital services offered by an electronic devices to another electronic devices, that enable the digital exchange of information. In this way, technical services implement one or more maritime services, which are the core of e-Navigation.

The following paragraph briefly summarizes the content of the referenced documents and explains how these "building blocks" fit together:

Ad. 1. IMO MSC85/26/Add.1, annex 20 defines the overall aim of e-navigation, but does not provide any practical guideline on how to realise actual information exchange.

Ad. 2. IMO MSC.1/Circ. 1610 defines a number of high-level maritime services, for instance VTS service and service for providing maritime safety information. Again, these services are high-level and non-technical descriptions that do not provide direct guidance for digitalisation. It does however define areas for which technical services needs to be developed.

Ad. 3. IALA Guideline 1128 defines a harmonised way to describe technical services that are actually capable of exchanging information (G1128 provides a concrete template to defining technical services). The guideline is technically agnostic, so any information exchange using any specific technology can be described using this template. Technical services that are made using this guideline can be implemented by different stakeholders, enabling them to exchange information defined by the service specification, and thus realising the goals of e-navigation.

Ad. 4. When information is exchanged, elements within this information needs to be able to be identified. An AtoN, a navigational warning message, a container or anything else needs to be able to be assigned a unique identifier (similar to barcodes on products or social security numbers for people). IALA G1143 defines a mechanism to give unique identifiers to anything within the maritime domain.

Ad 5. IHO S-100 describes how to define product specifications. A product specification describes certain "products", such as navigational charts (S-101), bathymetry data (S-102), navigational warnings (S-124) and many other relevant "products" within the maritime domain. The most important part (in this context) of a product specification is the data model. So, a product specification for, i.e. a navigational warning, will contain a data model describing the exact digital representation of a navigational warning. Thus these product specification provides harmonised data, which is required to define technical services.

Ad 6. IMO Resolution MSC.467(101)) describes the relationship (which is also briefly described above) between Maritime Services (ad. 2), Technical Services (ad. 3) and product specifications (ad. 5). It also mentions Maritime Resource Names (MRNs) (Ad. 4).

Ad 7. IALA G1157 describes how to create technical services specifications (using G1128, ad. 3) that uses standard internet technology - i.e. web-services.

Ad 8. This guideline describes how to define web-services that exchange data according to an S-100 product specification. This guideline is aligned with both G1128 (ad. 3) and G1157 (ad. 7).

Ad. 9. IALA G1161 describes how to select a platform providing additional features in order to support e-navigation information exchange in the maritime domain. The main key features are authentication of entities (so entities that exchange information can be sure of their respective identities) and service discoverability.

In summary, the referenced guidelines and standards broadly describe how specifications can be created for technical services. These technical services can then be implemented by maritime stakeholders, e.g. pilots, so that they are able to exchange information with each other. However, guideline IALA G1161 mentions a platform to enable digital authentication and services discoverability for facilitating the provision of Maritime Services. This is where the MCP comes into the picture as it is exactly such a platform. The following chapter describes how the MCP sets out to accomplish the provision of maritime services.

3   THE MARITIME CONNECTIVITY PLATFORM (MCP)

The MCP is a decentralised platform that facilitates secure and reliable information exchange within the maritime domain and beyond. Beyond – because the maritime world is not isolated, but needs to exchange information with other domains, including other transport domains.

The exchanged information can be almost of any nature, ranging from private confidential information between a vessel and the shore office of the shipowner, to public information provided by authorities, such as the provision of navigational warnings.

The MCC defines specifications and procedures for three core services;

- The Maritime Identity Registry (MIR): Facilitating authentication of entities exchanging information

- The Maritime Service Registry (MSR): Facilitating service discoverability

- The Maritime Messaging Service (MMS): Facilitating secure, reliable and technology agnostic information exchange

As a decentralised platform, there is no single entity operating this. Several organisations can be MCP service providers, and collectively they form "the Maritime Connectivity Platform".

The MCP is governed by the Maritime Connectivity platform Consortium (MCC), which serves two overall purposes:

- Defining both the (technical) standards that MCP parties must adhere to, as well as additonal criteria for being an (endorsed) MCP service provider. The MCC strives to provide open-source, free, reference implementations of those standards.

- Endorsing organisations to be MCP service providers

3.1   The Maritime Identity Registry (MIR)

A MIR instance is responsible for identity management and authentication of (some) entities in the MCP. In particular, the MIR will provide the following functionality:

- Firstly, Identity Management: A MIR enables that a maritime entity (such as a device, human, organization, service, or ship) can be registered as an entity of the MCP and be issued a unique identity (by assigning a MRN).

- Secondly, Public Key Infrastructure (PKI): A MIR ensures that each MCP entity holds a corresponding cryptographic identity, i.e. a public/private key pair and a certificate with the public key bound to their identity.

- Thirdly, a MIR provides infrastructure for federated authentication for situations where PKI-based authentication is not practical, based on established internet standards (OAUTH 2.0/OpenID Connect). This makes it easier for relying parties to integrate with the MCP. For example, a service provider in Denmark can request that a user from a Korean vessel authenticates at the Korean MIR where she is registered (similar to some other service is asking you to "Login with Facebook", where "Facebook" is in the same role as the Korean MIR).

While different organisations can be MCP identity service providers (operate a MIR), a basic level of trust is ensured for the relying parties by the fact that the MCC will endorse such organisations and by that assessing basic features of their operation - mainly with regard to ensuring interoperability. It is envisioned that other organisations will endorse MCP identity providers for specific purposes using a more thorough vetting procedure.

3.2   The Maritime Service Registry (MSR)

A MSR does not provide actual maritime information but rather metadata about maritime information service providers. Like e.g. the information that they carry, and the technical means to obtain it. An MSR instance contains service specifications according to a Service Specification Standard (which is identical to IALA Guideline 1128) and provisioned service instances implemented according to these service specifications.

The functionality of the MSR is twofold: service discovery and service management. It enables service providers to register their services in the MCP and allows an end-user to discover those services. Services and service instances can be searched via different criteria such as keywords, organizations, locations, or combinations, and more. The management of a service encapsulates the functions to publish a service specification and register and publish a service instance.

As with the MIR, the MSR is decentralised, so many different entities can be MSR service providers. The MCP MSR concept provides mechanisms through the means of a block chain to facilitate global service discoverability across all MSR's.

3.3   The Maritime Messaging (MMS)

A MMS is a messaging service intended to offer transparent seamless information transfer across different communication links in a carrier agnostic and geolocation-context sensitive manner.

The MMS can establish ship-shore and ship-ship communication based on internet connectivity, and utilize a number of alternative communication services via dedicated gateways, such as VDE-TER and VDE-SAT.

For example, a message, sent by one specific ship using INMARSAT access to a MMS, may be received via a VDES terminal on another ship, a HF data connection on yet another ship, or a VTS operator on a DSL landline internet connection. The MMS uses the MRN to identify entities as end-point addresses.

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

3.4   The Maritime Connectivity Platform Consortium (MCC)

The MCC has been structured in a way inspired by the World Wide Web consortium (W3C). As with W3C, the MCC has a few host members, which are all non-profit organisations. An addition to these, there are regular members, which can also be for-profit-organisations. The host members form the board, which decides on new members and endorses MCP service providers.
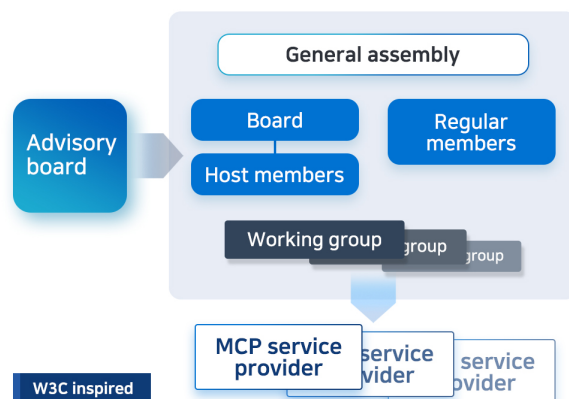
Figure 1: Organisation of the Maritime Connectivity Platform Consortium

Documents defining the criteria for being MCP services providers must be adopted by the General Assembly, in which all members are represented, with veto possibility for the host members. Furthermore, the MCC has an advisory board and a few governmental observers that are represented at the board, but without voting rights.

4   CURRENT STATUS AND RECENT DEVELOPMENT

The MCP has been under development for quite a number of years. The basic concept emerged around 2012, and through the effort of several different organisations and several international projects (the most notable of which were Monalisa, ACCEAS, EfficienSea2 and the STM validation project, all co-funded by the EU and the SMART Navigation project funded by Korea) a prototype testbed was established in 2015. In 2019 a governing body for the MCP was established, namely the MCP consortium (MCC). Moreover, most recently, documents specifying the Maritime Identity Registry and defining the requirements for being MCP identity service providers were released by the MCC.

MMS guidelines are currently under development.

The documents in question are attached in the annexes:

[1]   Annex A. Requirements for MCP identity service providers (MCP Gen4)

[2]   Annex B. MCC Identity Management and Security; General Approach and Basic Requirements (MCP IDsec1)

[3]   Annex C. MCC Identity Management and Security; Identity Management (MCP IDsec2)

[4]   Annex D. MCC Identity Management and Security; Public Key Infrastructure (PKI) (MCP IDsec3)

[5]   Annex E. MCC Identity Management and Security; Authentication and Authorization for Web Services (MCP IDsec4)

This means that for the purpose of authentication of entities (one of the basic requirements described in G1161 (ad. 9 in the above)), the MCP is ready to be used operationally, either for e-navigation services or digitalisation in general. Anyone can establish a MIR; some organisations have done this, and others are in the process of doing so. The Korean government is running a national MIR service, and the Finnish government is planning to do so. Some major players in the maritime domain (SAAB, Wärtsilä and Kongsberg) have established a MIR service through their consortium Navelink, which anyone can purchase access to - on a non-profit basis. Other organisations are considering establishing MIR, or using an existing one.

Further information about the MCP and MCC including access to testbed, open source reference implementation and MCC membership application can be found at: maritimeconnectivity.net

5 ACTION REQUESTED OF THE COMMITTEE

The Committee is requested to take note of the information, considering to add work items to the next committee work period, such as adding a guideline on how to facilitate transport of e-navigation services over VDES by the use of the MCP

ANNEX A

Requirements for MCP identity service providers

1. INTRODUCTION

This document describes what it means to be an MCP (Maritime Connectivity Platform) identity service provider, and what the requirements are for being such. The document is high-level but other than this informative introduction is mostly normative.

The intended audience of this document includes:

Non-technical people in organisations that wish to be MCP identity service providers

Non-technical people in organisations that wish to rely on a MCP identity service provider for authentication

This document makes references to documents that are geared towards a technical audience.

The goal of the MCP specifications is to enable easier development and deployment of network-based services for the maritime domain. This is achieved by specification of:

o Maritime Resource Names, MRNs, that identify a vessel, service, person, etc.

o an MCP Maritime Identity Registry (MIR), which assigns MRN's to vessels, services, persons, etc., and service providers. A MIR can issue X509 certificates that binds the assigned MRN to the holder of the private key associated with the public key in the certificate. A MIR can also act as a federated authentication service, minting tokens for use at a particular service.

o an MCP Maritime Service Registry (MSR), that allows parties to search for services that meet certain criteria, for example those that offer up-to-date AtoN information in a particular geographic area.

o an MCP Maritime Messaging service (MMS) allowing authorized maritime stakeholders to send and receive messages in an efficient, reliable and seamless manner within the MCP to solve problems of the current maritime wireless data communication system.

Various services can then choose to rely on a MIR to authenticate users. Services that are specified by the MCP consortium, such as a MSR or MMS, will always rely on a MIR for authentication. Importantly, also services specified elsewhere can do so. For example, a local AtoN information service, when itself registered with a MIR, can now require that its users authenticate with their MIR issued certificate, or with a token minted by a MIR.

One or more MIRs can establish a "hierarchy of trust", where a root MIR has registered subordinate MIR providers. A "root" MIR in turn may be endorsed by the MCP consortium. This way a vessel registered with a shipping company MIR which in turn is registered with an endorsed MIR in e.g. Korea, might be able to use (might be trusted by) an agent service registered with a port MIR which in turn is registered with a Finnish endorsed MIR. Likewise, that same vessel might trust a Finnish service that provides up-to-date AtoN information about a fairway into Helsinki, because that service can proof that is registered (possibly indirectly) with an endorsed MIR. See The MIR hierarchy of trust
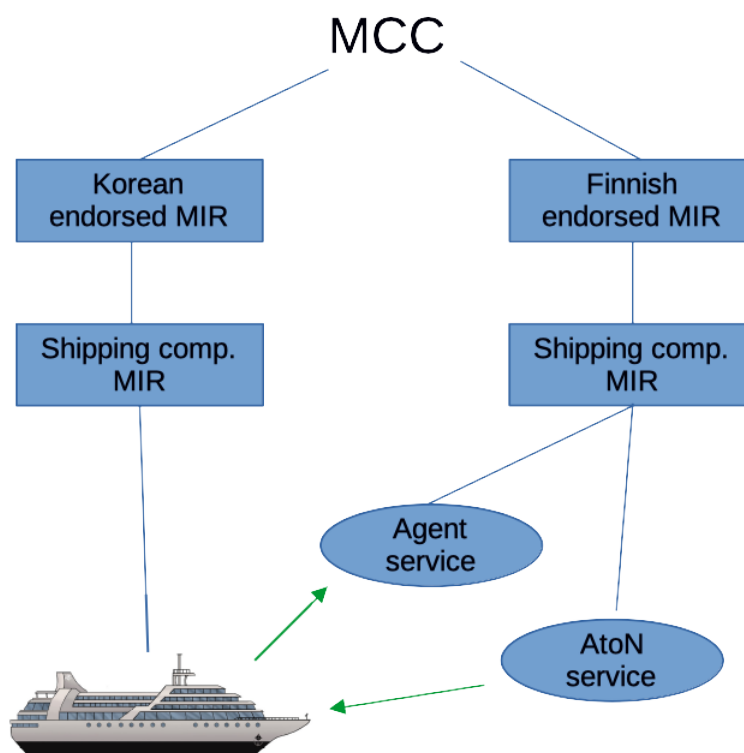
Figure 1: The MIR hierarchy of trust

The remainder of this document specifies what is required from a party that wishes to operate a MIR, MSR or MMS, such that the scenarios sketched out above are indeed possible.

2. DEFINITIONS

The *MCP consortium* (MCC) is the organization that authors the MCP specifications and endorses MIR services.

An *MRN* is a Maritime Resource Name.

An *MCP service* is one of: an MCP Maritime Identity Registry (MIR), an MCP Maritime Service Registry (MSR), or an MCP Maritime Messaging Service (MMS).

An *MCP service provider* is an organization that offers one or more MCP services.

A MIR can be *endorsed* by the MCC. This means that the MCC has deemed that the MIR service is operated according to the specifications and other requirements set forth in this document; and has issued an MRN to the MIR and signed the root certificate of the MIR.

A party is *registered* when it has been issued an MRN by a MIR that itself is registered.

A MCP service is deemed to be in *good status* if it is registered with a MIR that is currently in good status, or if it is currently endorsed by the MCC. Informatively, good status is achieved if the chain of trust is rooted in a currently endorsed MIR.

The key words *MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY,* and *OPTIONAL* in this document are to be interpreted as described in [RFC2119](#).

3. REQUIREMENTS FOR A MIR SERVICE

A MIR service assigns MRN's to maritime parties, and issues a X509 certificate to such parties, but only after appropriate vetting of each party.

This chapter describes the requirements a MIR service provider must meet, and processes it must adhere to, in order to operate a MIR service that can be registered with another MIR, or endorsed by the MCP consortium.

3.1. Compliance with MCP Specifications

A MIR service provider MUST ensure that each entity to which its MIR service assigns an MRN has been vetted according to the procedures specified in MCP Gen 5.

A MIR service MUST assign MRN's that are compliant with MCP IDSec 2. Before the MIR service is put into operation it MUST either register with a MIR in good status, or obtain endorsement from the MCC. This is to ensure that the IPID part of the MRN of the (new) MIR will be globally unique.

Digital certificates issued by a MIR service MUST be compliant with the requirements put forth in MCP IDSec 3.

A MIR service MUST also be able to act as an Open ID Connect Identity Provider as specified in MCP IDsec 4.

A MIR service provider MUST adhere to applicable data protection rules such as the EU General Data Protection Regulation (GDPR) and any other applicable laws.

3.2. Requirements for endorsement by the MCC

A MIR service provider that wishes for its MIR service to be endorsed:

- o MUST have a public certificate practice document compliant with RFC3647.
- o MUST follow the vetting procedures in MCP Gen 5, when enrolling organisations into their identity registry, and keep records of the results of applying vetting procedures for potential future assessment.

3.3. Physical operations

MCP identity service providers are encouraged to use renewable energy sources for their operations.

4. ENDORSEMENTS

Upon request the MCC secretariat, or a party appointed by the MCC secretariat, will assess the MCP service provider to verify compliance with the requirements of the relevant sections of this document. As part of this assessment the service provider will be subject to the vetting procedure specified in MCP Gen 5.

Having made this assessment, the secretariat makes a recommendation to the MCC board on whether or not to endorse the service, and the board makes the final decision on this.

Endorsed MCP services will be listed on the MCC web page, and root certificates of endorsed MIR services will be included in a list which will be digitally signed (as stated in MCP IDSec 3) by one of the MCC host members.

4.1. Revocation of endorsement

When it is evident that an endorsed MCP service no longer complies with the requirements of this document the MCC board can revoke the endorsement of that service.

In case there is reasonable doubt that an endorsed MCP service no longer complies with the requirements of this document the MCC board may request the service provider for clarification and can ask the MCC secretariat to re-assess the service provider. Having made this assessment, the secretariat makes a recommendation to the MCC board on whether or not to revoke the endorsement of the service, and the board makes the final decision on this.

5. UPDATES OF SPECIFICATIONS

When new versions of the MCP specifications are approved and published by the MCC the MCC will publish a date by which MCP services are expected to have adopted the new version(s). The MCC may revoke the endorsement of services that are not compliant with the new versions by that date.

6. REFERENCES

MCP Gen 5: Vetting procedure for MCP instance providers, version 1.0.

MCP IDSec 2: MCC Identity Management and Security: Identity Management, version 1.0.

MCP IDSec 3: MCC Identity Management and Security: Public Key Infrastructure (PKI), version 1.0.

MCP IDSec 4: MCC Identity Management and Security: Authentication and Authorization for Web Services, version 1.0.

RFC2119: Key words for use in RFCs to Indicate Requirement Levels. S. Bradner. The Internet Society, March 1997.

RFC3647: Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework. S. Chokani et al. The Internet Society, November 2003.

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].

1   STRUCTURE AND FUNCTIONALITY

MCP – Maritime Connectivity Platform with MIR – Maritime Identity Registry
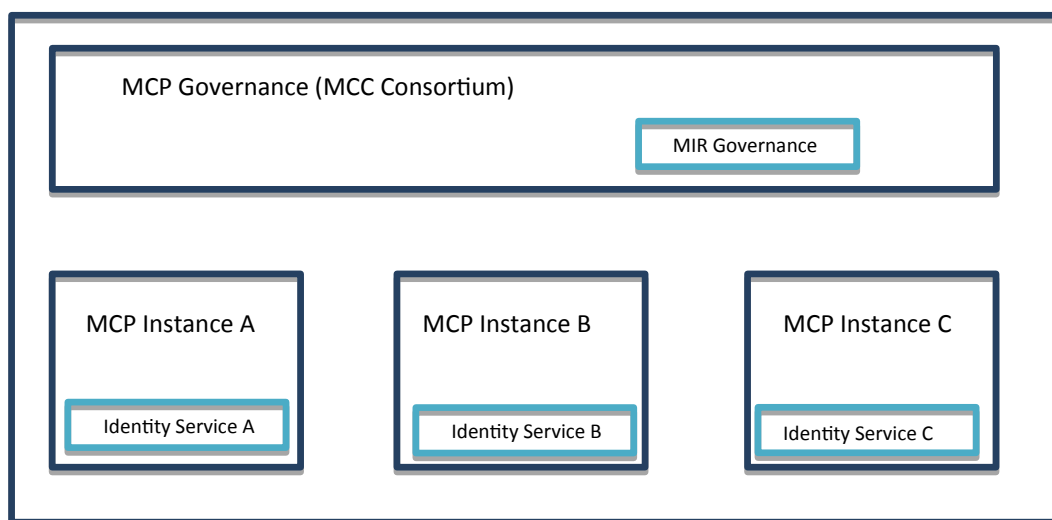

Figure 1: Structure of MIR within MCP.

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:

   o   MCP entity: An entity registered at some MIR services.

   o   MCP namespace: The subspace of the MRN namespace that is governed by the MCC.

   See [MCC:ID] for details.

2. **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.

3. **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.

2   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.

3   PROFILE "BASIC REQUIREMENTS"

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

1   Identity Management as detailed in [MCC:ID]:

    a.   MCP MRN syntax as specified in Section 1 of [MCC:ID],

    b.   ID1, ID1.1 - ID1.3: Decentral Management of MCP MRNs,

    c.   ID2: Transparency of Syntax, and

    d.   ID3, ID3.1 - ID3.2: Strong Notion of MCP Entity.

2   PKI as detailed in [MCC:PKI]:

    a.   PKI1.1 - PKI1.7: Decentral PKI Concept,

    b.   The cryptographic requirements as specified in Section 2 of [MCC:PKI], and

    c.   The certificate format as specified in Section 3 of [MCC:PKI].

3   Authentication and Authorization as detailed in [MCC:AUTH]:

    a.   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

    o   Certificate Policy, and

    o   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

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

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

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].

1 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:

- o 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.

- o 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.

- o 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.

  1.1.1   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 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 MRN as 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.

1   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:

- o pk_A is the public key of A, and pr_A is the private key of A respectively.

- o $cert_P(A, pk_A, V)$ 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 $pr_A.$ The result is a cyphertext C.

2.   Entity A makes available its certificate $cert_P(A, pk_A, V)$, 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 pk_A is the valid public key of the MCP entity with MRN A. (Necessary requirements on certificate validation will be specified.).

5.   Entity B uses pk_A 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 pk_A.)

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.

2   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.
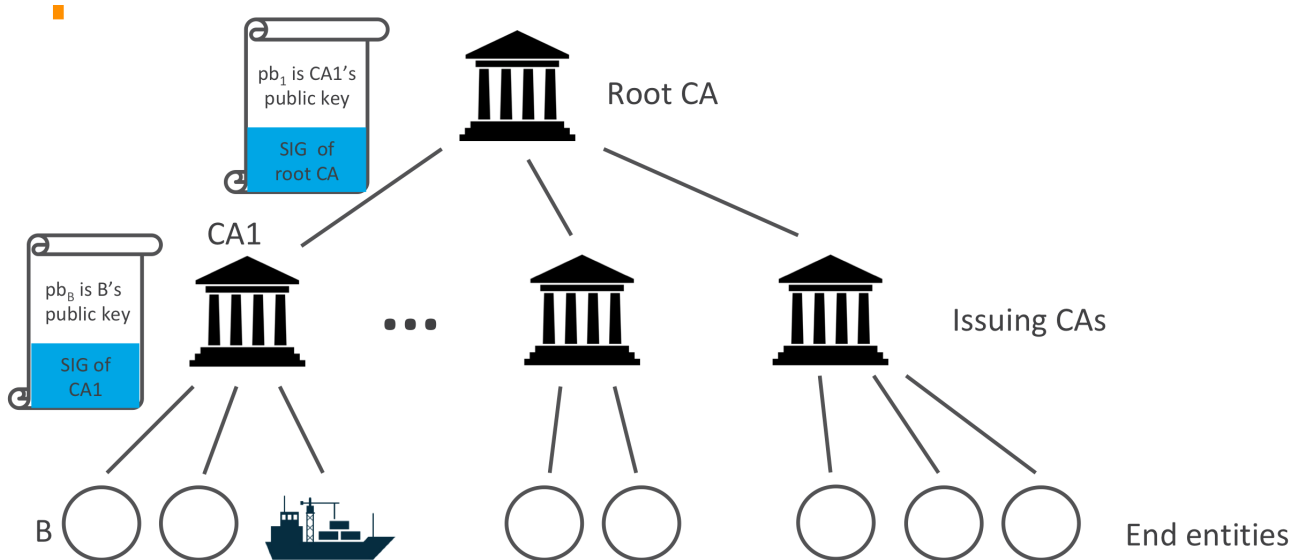

Figure 2: Hierarchical X.509 PKI Structure

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 $\text{cert}_P(A, pk_A, V)$ a receiving party has to verify the signature of the identity provider P with the public key of P provided in an intermediary certificate $\text{cert}_{MCC}(P, pk_P, V)$ 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 $\text{cert}_{MCC}(MCC, pk_{MCC}, V)$. The latter provides the trust anchor accepted by the receiving party.

Examples:

a. *Single point of attack:* Assume the MCC root key pr_{MCC} 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 $pk_{I(P)}, pr_{I(P)}$ and generates a fake certificate for P with his own key $pk_{I(P)}$: $\text{cert}_{MCC}(P, pk_{I(P)}, V)$. This is possible since the attacker knows pr_{MCC}. Second, the attacker generates a key pair $pk_{I(A)}, pr_{I(A)}$ and generates a fake certificate for A and his own key $pk_{I(A)}$: $\text{cert}_{I(P)}(P, pk_{I(A)}, V)$. This is possible since he knows $pr_{I(P)}$. Altogether, the attacker can now present a valid

certificate chain that establishes $pk_{I(A)}$ to be the public key of A while he knows the private counterpart $pr_{I(A)}$. Hence, he can impersonate A. Altogether this violates principle 2 above.

b. *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 $pb_{I(A)}$, $pr_{I(A)}$ and generate a fake certificate for A and $pb_{I(A)}$ signed by P': $cert_{P'}(A, pb_{I(A)}, V)$. 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.

c. *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 $cert_P(A, pk_A, V)$, 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.

2.1 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.

2.2 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:

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

2. 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.

3 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:

- o   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].

- o   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.

- o   We will also consider matters of crypto agility.

4   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:

- o   **Version** – which X.509 version applies to the certificate (which indicates what data the certificate must include).

- o   **Serial number** – A unique assigned serial number that distinguishes it from other certificates.

- o   **Algorithm information** – the algorithm used to sign the certificate.

- o   **Issuer distinguished name** – the name of the entity issuing the certificate (MCP).

- o   **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.

- o   **Subject distinguished name** – the name of the identity the certificate is issued to.

- o   **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].

5   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".

6   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

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].

1   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).

2   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: OpenID Connect Core 1.0, N.Sakimura et al. https://openid.net/specs/openid-connect-core-1_0.html

[4] RFC2119: 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