Version: 0.3

MCC Identity Management and Security: General Approach and Basic Requirements

1 GENERAL

1.1 Summary

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 instances of the MCP. Both, 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].

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 instances in addition to providing reference implementations and a testbed. The remainder of this document is then structured as follows. In Section 2 we address Identity Management, in Section 2 we focus on Public Key Infrastructure (PKI), and Section 3 is about Authentication and Authorization for Web Services. Altogether, we derive a first set of requirements for MCP instances, which we collect into a profile in Section 4.

1.2 Structure and Functionality

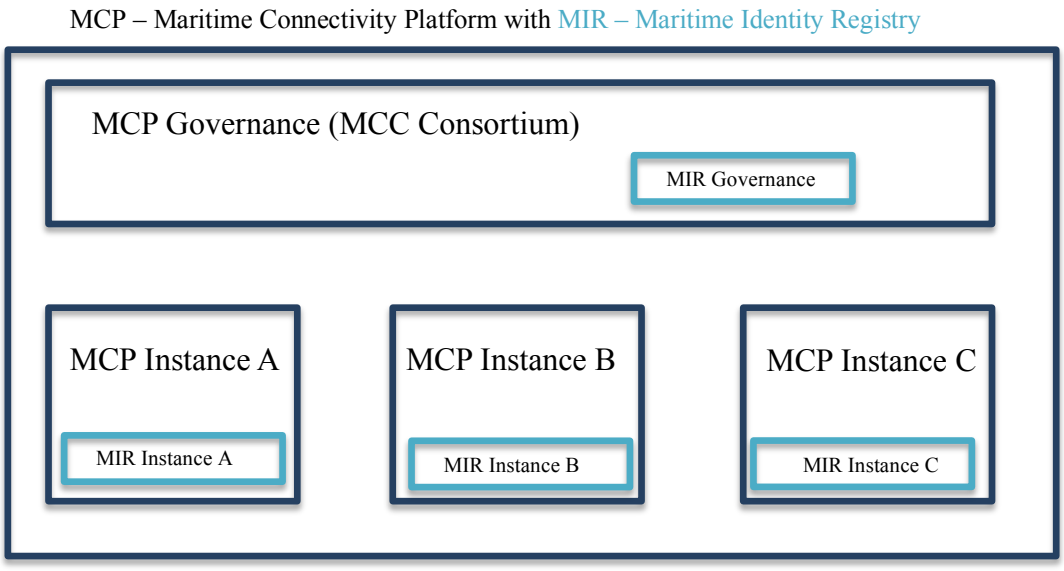

Figure 1: Structure of MIR within MCP

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 instances. In summary, MIR governance and instances 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 instances to implement and have certified concrete identity registries. We use the following terminology:
    - MCP entity: An entity registered at some MIR instance.
    - MCP namespace: The subspace of the MRN namespace that is governed by the MCC.
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 instances to implement and have certified concrete PKIs.
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 instances deliver concrete OAUTH 2.0/OpenID Connect platforms.

1.3 Governance and Profiles

The focus of the MCP is currently changing from only providing reference implementations and a testbed to including governing several operational MCP instances as well as ensuring their interoperability. At the time of writing there are two emerging operational instances: one is evolving from the STM project; the second is being deployed by the SMART project of the Republic of Korea. Hence, the MCP has to strike a balance between laying down criteria according to which the emerging deployments can be endorsed as MCP instances 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). This is why the MIR adopts the following approach of profiles.

The MCP will not develop a single set of criteria that every MIR instance has to comply with but rather allow several *MIR profiles* to coexist. Each MIR profile contains a set of requirements that define what MIR instances have to 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 instance can choose which of the current MIR profiles it aims to fulfill. While the MCC is not able to carry out assessments as to whether a MIR instance adheres to a profile itself (in particular 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 instance or a cluster of MCP instances 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 WG IDSec will formulate requirements that will pin down how the profiles are managed and harmonized.

2 IDENTITY MANAGEMENT

2.1 The MCP Namespace

We first describe the MCP namespace. As explained above it is a subspace of the *Maritime Resource Name (MRN)* space [3], which is an official URN namespace. The syntax definitions below use the Augmented Backus-Naur Form as specified in [RFC5234].

The syntax for a MRN is as follows [3]:

```
<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 five types currently used within the MCP: device, organization, user, vessel, and service. 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"
<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 five 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.

Important note: We expect that the definition of MCP-TYPE, i.e. the set of types, will be modified and possibly extended in the near future. In particular, "vessel" is likely to be replaced by "ship".

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.

ID2 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".

ID2.1 The MCC must ensure that each IPID refers to at most one identity provider.

ID2.2 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.

ID2.3 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 ID2.1 and the second part of ID2.2 together ensure uniqueness: one MCP MRN is assigned to at most one entity. This is a general requirement for any URN. ID2.3 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:

ID3 Every Identity Provider is encouraged to publish he syntax that describes their name space as well as provide a reference implementation that recognizes the strings of their namespace.

Important note: According to current discussions in the MCC WGs this recommendation is likely to become mandatory in the future. Also, it is foreseen that an automated service will be hosted from the MCP web page that makes such information and tools available.

1.3.1 Further Requirements for a Strong Notion of Maritime Identity

The vision of the MCP is to enable a strong concept of digitial maritime identity. Hence, we put down requirements that go beyond what is commonly required of URNs. The following ensures that one physical 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.

ID1 Every entity registered as a MCP participant shall hold at most 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.

Important note: According to current discussions in the MCC WGs this requirement is likely to be strengthened to "Every entity of the MCP shall hold *exactly one* MCP MRN (i.e. MRN governed by the MCP)" in the future. Similarly to the current formulation this does not exclude that an MCP entity can hold another MRN of another organization. But it will give a clear concept of MCP entity: those entities that are registered under an MCP MRN name.

Hence, the AtoN in the example above can be identified by its IALA MRN, or its MCP MRN respectively. However, Requirement ID1 rules out that the AtoN can be referred to by a second MCP MRN. The following requirements implement ID1 in a decentral manner.

ID1.1 Each Identity Provider shall ensure that each entity they register holds at most one MCP MRN within their namespace.

ID1.2 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, ID1.1 ensures that they can obtain at most as many identities as there exist Identity Providers. And ID1.2 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).

3 PUBLIC KEY INFRASTRUCTURE (PKI)

4 AUTHENTICATION AND AUTHORIZATION FOR WEB SERVICES

5 PROFILE "BASIC REQUIREMENTS

ANNEX A 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

[3] MRN Specification: **https://www.iana.org/assignments/urn-formal/mrn**

[4] G1143 Unique Identifiers for Maritime Resources, IALA Guideline C69-11.2.6, Edition 1.0, June 2019