ID: MCP IDsec 2

Version: 1.0

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:

- 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.

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.