ID: MCP IDsec 1

Version: 1.0

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 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 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.

1 STRUCTURE AND FUNCTIONALITY

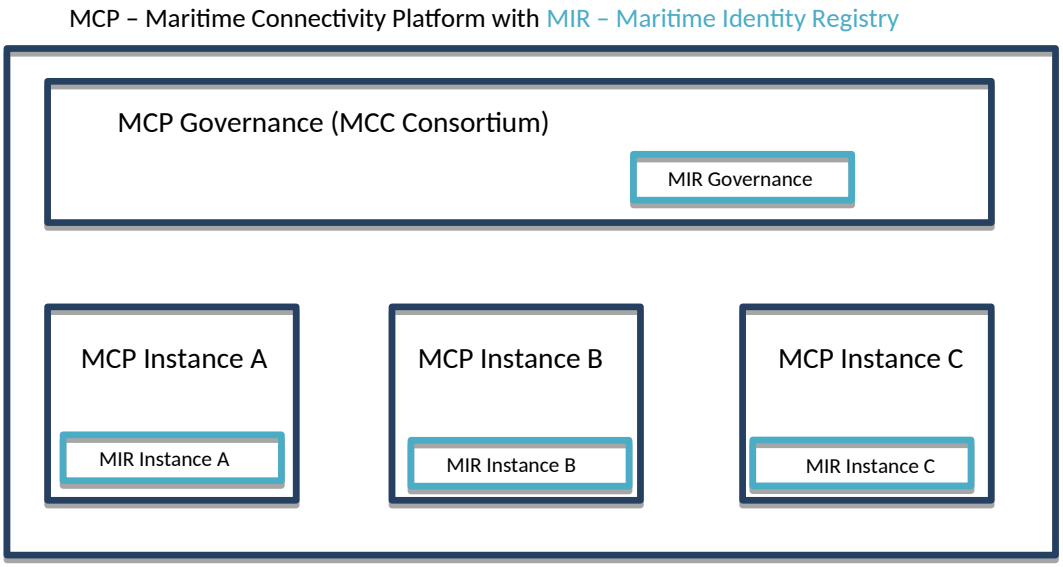

Figure 1: Structure of MIR within MCP

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.

    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 instances to implement and have certified concrete PKIs.
   See [MCC:PKI] for details.

   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.
   See [MCC:AUTH] for details.

2 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.

3 PROFILE "BASIC REQUIREMENTS"

The profile "Basic Requirements" V1.0 consists of the following requirements:

1. Identity Management:
    - MCP MRN syntax as specified in Section 2.1
    - ID1, ID1.1 - ID1.3: Decentral Management of MCP MRNs
    - ID2: Transparency of Syntax
    - ID3, ID3.1 - ID3.2: Strong Notion of MCP Entity
2. PKI:
    - PKI1.1 - PKI1.5: Decentral PKI Concept
    - The cryptographic requirements as specified in Section 3.2
    - The certificate format as specified in Section 3.3

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

[MCP IDsec 2] MCC Identity Management and Security: Identity Management

[MCP IDsec 3] MCC Identity Management and Security: Public Key Infrastructure (PKI)

[MCP IDsec 4] MCC Identity Management and Security: Authentication and Authorization for Web Services