ID: MCP IDsec 4

Version: 1.02

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

[1] 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 (

[2] OIDC) token-based authentication protocol. Therefore, each MIR must support

[3] OIDC (see

MCP-GEN4).

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.

[4] 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

RFC2119 [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*.

[5] **A MIR SHOULD NOT rely on another legal entity for actual authentication, unless that entity is a MIR in *good status* as defined in**

AUTH2.2 MCP-GEN4.

REFERENCES

[6] MCP-IDSEC3: MCC Identity Management and Security: Public Key Infrastructure (PKI) 1.0, MCP Consortium 2021.

[7] MCP-GEN4: Requirements for MCP identity service providers 1.0, MCP Consortium 2021.

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

[9] 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