ID: MCP IDsec 4

Version: 1.0

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

For authentication and authorization in web services the MCP offers users to be able to use OpenID Connect [1] (OIDC). OpenID Connect is a token based authentication protocol that is built as a layer on top of the OAuth 2.0[2] authorization protocol. In Section 1 we will detail our usage of OpenID Connect, while in Section 2 we will discuss how external organisations can be federated.

1 MCP USAGE OF OPENID CONNECT

A service provider can choose to use the MCP based OpenID Connect authentication for their web service. This means that when a user wants to use the service, they must first login with their MCP credentials and receive an OIDC token from MCP that contains information about the user and what organization they belong to. The user can then use this token to authenticate themselves with the web service. The service provider can also choose to implement authorization based on the information in the token.

The table below shows the claims that an MCP OpenID Connect token must contain:

Attribute	**Description**
preferred_username	The username of the user in the parent organization.
email	The email of the user.
given_name	First name of the user.
family_name	Last name of the user.
name	Full name of the user.
org	The Maritime Resource Name of the organization the user is a member of.
permissions	List of permissions for this user assigned by the organization the user is a member of.
mrn	The Maritime Resource Name of the user.
roles	List of roles that the user has in the role hierarchy.

1 https://openid.net/connect/

2 https://oauth.net/2/

To learn more about how to use MCP based OIDC we refer to the MCP developer's guideline[3].

Future Tasks:

- Formulate adequate risk containment principles analogously to those for the MCP PKI and translate them into requirements for MCP OIDC instances. For example, if it was up to a central entity to issue authorization tokens then this central entity constitutes a single point of attack for MCP web authorization (even when authentication itself is delegated to identity providers).
- Specify secure OIDC configurations recommended for use.

2 FEDERATION OF EXTERNAL ORGANISATIONS

It is possible for OIDC in a decentralised scenario and, thus, for external organisations to authenticate and authorise MCP IDs based on their MCP credentials. This follows the principle that not all MCP instance providers are trusted equally by individual organisations, so the original idea of "login with your global MCP login" is no longer valid. However, given that some organisations require this, we do provide the needed functionality.

Note that MCC does not provide an automatic system for this, though it could be possible in the future.
Federation of external organisations can only be performed on an individual level, between the MCC member organisation hosting the MCP instance and the external organisation via a written agreement.

AUTH1.1 All external organisations that are federated into an MCP instance must be an MCC member.

AUTH1.2 Any external organisations can be federated into multiple MCP instances, though separate agreements must be made for each.

After an agreement have been met, OIDC federation tokens can be exchanged between the organisations using a secure method. It is required to use relevant MCP certificates for this purpose to ensure the identity of both organisations.

AUTH1.3 The MCC member organisation hosting the MCP instance must keep a full log over all communication relevant to the federation.

The MCC board can at any time examine this information as part of the general auditing of MCP instance providers.

[3] https://developers.maritimeconnectivity.net/identity/index.html#brokered-user-federation