Document ID: MCP Gen 5

Version: 1.2

Vetting procedure for MCP identity service providers

ID: MCP Gen 5			
Version	**Author(s)**	**Nature of change**	**Date of adoption**
1.0	Thomas Christensen	Initial version	General assembly meeting #3 December 11, 2020
1.1	Thomas Christensen	• GDPR / data privacy moved to endorsement procedure document (MCP Gen 7) • Check on VAT removed • Terminology: 'MIR instance provider' changed to 'MCP identity service provider' • Scope extended to include vetting of MCP service providers to be endorsed by MCP consortium	
1.2	Thomas Christensen	Just updated the title of the document	

1 SUMMARY

This document described the minimal vetting procedures an MCP identity service provider needs to follow, when a new organisation is registered in their identity registry (MIR). The procedure is also used for vetting MCP service providers themselves - when being endorsed by the MCP consortium.

1 PROCEDURE

When an organisation applies to be registered in a MIR, the organisation needs to submit the following information:

- Certificate of Registration or corresponding certificate from a third party, i.e. an authorized authority or public register, issued within 6 months before application
- Organisation name

- Type of organization (e.g. company, authority, university or association)
- Registered address and country
- The organization's registration number (as provided by authorized authority or public register)
- The law under which the organization is incorporated
- The main (domain) URL of the organisation

In order for the MCP identity service provider to accept the organisation, the following must be checked:

Organizational information

- CHECK: That all of the information above has been received
- CHECK: The Certificate of Registration or corresponding certificate is issued within six (6) months before request form. Control that the certificate is issued by authorized authority or public register in registered country.
- CHECK: The organization name corresponds to the data in received certificate
- CHECK: Type of organization (e.g. company, authority, university or association) corresponds to the data in the certificate.
- CHECK: Registered address and country corresponds to the data in received certificate
- CHECK: The organization's registration number corresponds to the data in received certificate.
- CHECK: The law under which the organization is incorporated corresponds to the data in received certificate
- CHECK: There is a valid URL to the organization.
- Optional CHECK: There is a valid OV SSL (minimum requirement) or EV SSL certificate enclosed for the URL
- Optional CHECK: That the information (name, address) in the OV/EV SSL certificate matches the information received and the certificate of registration.
- Optional CHECK: GLN code and/or IMO code and/or other identifying item, if applicable.

The MCP identity service provider must store all information received from the organisations applying for registration, as well as documentation proving that the above checks have been carried out. This information may be subject to a subsequent audit by the MCP consortium secretariat.