Procedure for endorsing MCP identity service providers

Document Revision

ID: MCP Gen 7			
Version	**Author(s)**	**Nature of change**	**Date of adoption**
1.0	Thomas Christensen	Initial version	General assembly meeting #5 December 6, 2021
1.1	Thomas Christensen	• Step 7 – one or more IPID's instead of just one • Recurrence section added • Added step 4 regarding data privacy	

1 PROCEDURE

The process of endorsing MCP identity service providers consists of the following steps:

1. Validate the identity of the candidate organisation by following the vetting procedure in MCP Gen 5.
2. Obtain the vetting procedure the candidate organisation will use to vet organisation to be enrolled in their identity registry.
3. Check that their vetting procedure as a minimum follows the procedure in MCP Gen 5.
4. Check that the organisation declares that they follow applicable data privacy practices - for instance GDPR for the EU
5. Get the certificate policy and certificate practice statements
6. Check that these documents exist (are not empty)
7. Obtain their suggestion for one or more MCP MRN domains (IPID)
8. Get their root certificate
9. Obtain two example certificates for each MCP entity type (including whole certificate trust chain) issued by the MIR PKI, one active and one revoked
10. Check that the certificates comply with the MCP PKI specification (MCP IDsec 3)
11. Get endpoints for certificate revocation list and OCSP from certificate

12. Check that an up-to-date certificate revocation list is returned from the endpoint
13. Check that the example revoked certificates are in the revocation list and that the active certificates are not
14. Check using the OCSP endpoint that the correct revocation status is returned for all certificates
15. Obtain URL for OIDC Well-Known configuration information endpoint
16. Check that the information from the endpoint complies with the OIDC specification
17. Acquire token, and check that token complies with MCP standard
18. Make a suggestion to the MCC board
19. The board decides
20. The MRN domain(s) are issued to the organisation
21. Include their root certificate in the MCC list of root certificates of endorsed MCP identity service providers
22. List them on the website as endorsed MCP identity service providers

2 RECURRENCE

Once an organisation has been adopted as an endorsed MCP identity service provider – this endorsement is valid for a period of one year – measured from the date of the board meeting at which the endorsement was decided.

Thus – in order to continuously be endorsed – the endorsement procedure must be repeated within one year. This process is undertaken by the secretariat, and only if deviations from the endorsement criteria are detected, are the board notified. If no deviations are detected, the endorsement is extended for another year.