Document: MCP Gen 7
Version: 1.0

Procedure for endorsing MCP identity service providers

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. Get the certificate policy and certificate practice statements
5. Check that these documents exist (are not empty)
6. Obtain their suggestion for an MCP MRN domain (IPID)
7. Get their root certificate
8. Obtain two example certificates for each MCP entity type (including whole certificate trust chain) issued by the MIR PKI, one active and one revoked
9. Check that the certificates comply with the MCP PKI specification (MCP IDsec 3)
10. Get endpoints for certificate revocation list and OCSP from certificate
11. Check that an up-to-date certificate revocation list is returned from the endpoint
12. Check that the example revoked certificates are in the revocation list and that the active certificates are not
13. Check using the OCSP endpoint that the correct revocation status is returned for all certificates
14. Obtain URL for OIDC Well-Known configuration information endpoint
15. Check that the information from the endpoint complies with the OIDC specification
16. Acquire token, and check that token complies with MCP standard
17. Make a suggestion to the MCC board
18. The board decides
19. The MRN domain is issued to the organisation
20. Include their root certificate in the MCC list of root certificates of endorsed MCP identity service providers
21. List them on the website as endorsed MCP identity service providers