Document ID: DMC MCP 4

Version: 1.0

Publisher: Digital Maritime Consultancy (DMC)

Website: dmc.international

DMC Certification Practice Statement (CPS)

ID: DMC MCP 4			
Version	**Author(s)**	**Nature of change**	**Date of adoption**
1.0	Thomas Christensen & Oliver Haagh	Initial version	22/5 2025

1 INTRODUCTION

1.1 Overview

This CPS describes the operational practices and responsibilities of DMC as an MCP Identity Service Provider, in accordance with IALA Guideline G1183. It applies to all certificate lifecycle services provided by the DMC CA, including identity issuance, revocation, validation, and renewal for MCP entities.

1.2 Certificate Types

- Server Certificates: For secure communications (e.g., HTTPS) using SSL/TLS.
- Client Certificates: For authentication of users, vessels, and services in maritime applications.
- Service Certificates: When cryptographic or protocol-specific constraints exist (e.g., VDES, AIS).

1.3 Acceptable Subscriber Names

DMC only accepts identifiers compliant with the MCP MRN structure: urn:mrn:mcp:entity:dmc:<ipss>

1.4 Registration Procedures

DMC requires organisation identity verification and MRN compliance before certificate issuance. DMC as an Identity Provider is uniquely designated by the string "dmc" as the IPID in the MRN structure.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

DMC publishes:

- Valid certificates
- Certificate Revocation Lists (CRLs)
- Certification Practice Statement and Certificate Policy
- Root and intermediate CA certificates

Information is published on a public repository for validation purposes, conforming to G1183's decentral PKI model.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Initial Identity Validation

Organisations must submit verifiable documentation. Organisation validation is based DMC's vetting procedures (document ID) - which are compliant with the requirement defined by the MCP consortium.

3.2 Subscriber Registration

Every entity must hold exactly one MCP MRN within DMC's namespace. Each MRN uniquely identifies a single maritime entity.

4 CERTIFICATE LIFECYCLE OPERATIONS

4.1 Certificate Issuance

DMC verifies organisation identity and MRN conformity before issuing certificates signed by its intermediate CA. Certificates must be compliant with the X.509 standard.

4.2 Key Management

Key pairs can be generated by:

- The entity (e.g., ship, organization, service)
- DMC, with key provisioning using HSMs for secure deployment

4.3 Validity Periods

- Root Certificate: 10 years; renewed every 3 years
- Intermediate Certificate: 3 years; renewed annually
- Client Certificates: 6 months; renewed 2 months before expiry.

4.4 Renewal and Revocation

- Certificates are manually renewed according to the above rules and as defined in G1183.
- Revocation lists and OCSP responders are maintained and published.

5 CRYPTOGRAPHIC REQUIREMENTS

5.1 Algorithms

DMC supports the following:

- ECDSA P-384 with SHA-384
- ECDSA P-256 with SHA-256

5.2 Certificate Format

Each certificate includes:

- X.509v3 structure
- MCP MRN in the UID field
- Optional SAN fields for vessel/service info (e.g., IMO number, MMSI).

6 PHYSICAL, OPERATIONAL, AND PERSONNEL SECURITY

6.1 Facility and Device Security

- Secure, restricted access to certificate issuance facilities
- Use of HSMs for root key storage and signing
- Dual-control and separation-of-duty enforcement

6.2 Logging and Auditing

All certificate actions (issuance, revocation, renewal) are logged and stored for a minimum of 2 years.

7 COMPLIANCE AND ASSESSMENTS

DMC allows for:

- Independent compliance audits
- Public inspection of audit logs (non-sensitive)

8 LEGAL AND LIABILITY

- Limited Warranties: DMC provides assurance only for the organisation identity verification under its namespace.
- Confidentiality: Personal data is protected as per GDPR.
- Dispute Resolution: Disputes are managed via a formal internal process led by DMC's Dispute Committee.

9 DEFINITIONS AND ACRONYMS

All terms are defined as per IALA G1183, RFC 5280, and internal PKI standards. Key terms include:

- MCP: Maritime Connectivity Platform
- MRN: Maritime Resource Name
- IPID: Identity Provider Identifier
- IPSS: Identity Provider Specific String

10 DOCUMENT MANAGEMENT

- Policy Updates: Published on the DMC repository and effective 30 days post-publication.
- Version Control: Managed via integer and decimal versioning system.