Document ID: DMC MCP 3

Version: 1.0

DMC Certificate Policy (CP)

ID: DMC MCP 3			
Version	**Author(s)**	**Nature of change**	**Date of adoption**
1.0	Oliver Haagh & Thomas Christensen	Initial version	22/5 2025

1 INTRODUCTION

This Certificate Policy (CP) defines the requirements for issuing, managing, and using digital certificates by Digital Maritime Consultancy (DMC) as part of its role within the Maritime Connectivity Platform (MCP) ecosystem. It supports secure identity provision for ships, services, devices, and maritime authorities using MCP-compliant MRNs and X.509 certificates.

2 IDENTIFICATION

- Policy title: Digital Maritime Consultancy Certificate Policy
- OID: DMC MCP 3
- Policy Applicability: All certificates issued by DMC under its MCP namespace.

3 COMMUNITY AND APPLICABILITY

3.1 Certification Authorities

- Root CA: Operated by DMC; only used to sign intermediate certificates.
- Intermediate CAs: Used for entity certificate issuance (e.g., vessels, services).

3.2 Registration Authorities

- Internal or delegated RA under DMC's control, responsible for validation of MCP entities.

3.3 Subscribers

- Entities registered under DMC's MRN namespace, such as:
  - Ships
  - Maritime services
  - Authorities
  - Devices

3.4 Relying Parties

- Any party relying on DMC-issued certificates for authentication or secure communication within the MCP.

4 CERTIFICATE USAGE

4.1 Appropriate Usage

- Authentication of primarily, but not limited to, maritime entities
- Electronic signatures
- Encryption in communication protocols (e.g., HTTPS, VDES, SECOM)

4.2 Prohibited Usage

- Unauthorized signature creation on behalf of third parties
- Defence related applications

5 POLICY ADMINISTRATION

- Policy Authority: DMC Policy Management Authority

- Contact Info: policy@dmc.international
- CP Maintenance: Reviewed annually and updated as needed. Major changes require 30-day public notice.

6 PUBLICATION AND REPOSITORY

DMC maintains a publicly accessible repository that includes:

- This Certificate Policy
- CPS
- CRLs and OCSP access points
- Root and intermediate CA certificates

7 IDENTIFICATION AND AUTHENTICATION

- Initial identity verification for MRN-based subjects is required before issuance.
- Uniqueness of MCP MRNs is enforced within DMC's namespace.
- Certificates will include subject fields in accordance with [RFC 5280] and IALA G1183 guidelines.

8 CERTIFICATE LIFECYCLE OPERATIONAL REQUIREMENTS

8.1 Certificate Application

- Requires a Certificate Signing Request (CSR) and proof of MRN registration.

8.2 Issuance

- Performed after complete vetting and MRN compliance checks.

8.3 Renewal

- Certificates are renewed according to G1183..

8.4 Revocation and Suspension

- Revocation supported through CRLs and OCSP.

- Mandatory revocation conditions include compromise of private keys, inaccurate subject data, or policy violations.

9 TECHNICAL SECURITY CONTROLS

- Key Sizes: ECDSA P-256 and P-384 with SHA-2 hash algorithms.
- Key Protection: Hardware Security Module (HSM) for root CA key.
- Private Key Lifetime: Must match certificate validity and adhere to DMC archiving policy.

10 CERTIFICATE PROFILE

- Format: X.509 v3
- Extensions: SAN fields include MRN, IMO number, MMSI, etc. in accordance with G1183
- Distinguished Name: Must include UID field with full MRN (e.g., UID=urn:mrn:mcp:entity:dmc:org1:service123)

11 COMPLIANCE AUDIT AND ASSESSMENT

- Internal audits.
- Logs and records are maintained for 2+ years and are subject to periodic review.

12 LEGAL MATTERS

- Warranty: DMC warrants only the accuracy of organisation identity vetting and binding to MCP MRNs.
- Liability: Limited to direct use cases outlined in this CP.
- Dispute Resolution: Governed by DMC's internal dispute committee as per CPS.

13 REFERENCES

IALA Guideline for the provision of MCP identities, G1183.

RFC 5280