Network Working Group
Internet-Draft
Intended status: Informational
Expires: 30 August 2026

P.C. Luna
Independent Researcher
February 2026

Digital Identity Certification for Personal Media (DICPM)
draft-luna-dicpm-00

Abstract

This document specifies the Digital Identity Certification for Personal Media (DICPM), a protocol for cryptographic certification of personal media, binding media integrity to identity and consent while enabling verifiable licensing terms and revocation.

Status of This Memo

This Internet-Draft will expire on 5 August 2026.

Copyright Notice

Table of Contents

1. Introduction 2
2. Conventions and Requirements Language 2
3. Certificate Data Model 2
3.1. Canonical Serialization 2
3.2. Normative JSON Structure 2
4. Security Considerations 3
5. IANA Considerations 3
6. Normative References 3
Author's Address 4

1. Introduction

DICPM establishes a cryptographically verifiable certification layer binding media objects to identity and consent, with support for trust models, licensing constraints, and validation.

2. Conventions and Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] and [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Certificate Data Model

3.1. Canonical Serialization

All certificate payloads MUST be serialized using the JSON Canonicalization Scheme (RFC 8785) prior to signature generation.

3.2. Normative JSON Structure

```
{
  "cert_version": "1.0",
  "cert_id": "UUIDv4",
  "trust_model": "self | delegated | chained",
  "owner": {
    "global_id": "DID or UUIDv4",
    "public_key": "PEM-encoded SubjectPublicKeyInfo",
    "biometric_hash": "base64url salted irreversible hash"
  },
  "media": {
    "media_hash": "base64url SHA-256 or SHA-3 digest",
    "media_type": "registered media type",
    "created_at": "ISO8601 UTC timestamp"
  },
  "license": {
    "permitted_uses": ["commercial", "journalism", "educational", "artistic"],
    "project_reference": "string",
    "exclusive": true,
    "territory": "global or ISO country code",
    "expiration": "ISO8601 UTC timestamp",
    "revocation_policy": "URL or blockchain reference"
  },
  "extensions": {},
  "signature": {
    "algorithm": "Ed25519 | ECDSA-P256 | RSA-2048",
    "signed_at": "ISO8601 UTC timestamp",
    "value": "base64url signature"
  }
}
```


4. Security Considerations

Implementations SHOULD protect private keys using secure enclaves or HSMs where available. Biometric hashes MUST be salted and irreversible, and raw biometric templates MUST NOT be stored.

5. IANA Considerations

This document requests registration of the media type "application/dicpm+json".

6. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] IETF, "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", RFC 8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8785] IETF, "JSON Canonicalization Scheme (JCS)", RFC 8785, June 2020, <https://www.rfc-editor.org/rfc/rfc8785>.

Author’s Address

Paulo Cesar Pinto de Luna
Independent Researcher
Email: anjdric@gmail.com