

WritersLogic C2PA Certification Authority — Certificate Practice Statement (CPS)

Version 1.0 · 2026-07-09 Organization: WritersLogic Inc, 955 11th Ave Ste 3184, San Diego, CA 92101, USA (Delaware corporation) **Conforms to:** C2PA Certificate Policy (OID 1.3.6.1.4.1.62558.1.1, v0.1, 2025-06-02)

This Certificate Practice Statement (CPS) describes how WritersLogic Inc operates its Certification Authority (CA) to meet the requirements of the C2PA Certificate Policy (CP). WritersLogic executed the C2PA Certification Authority Agreement on 2026-05-15 (DocuSign Envelope ID 5180E49C-D2FC-8696-812A-29D9022E6C00).

Operational scale. WritersLogic is an early-stage company. At the current scale, David Condrey (Founder) is the sole responsible individual for CA operations — serving as CA Administrator, Registration Authority operator, Security/Incident Officer, and point of contact. Where the CP references separation of duties or dual control, WritersLogic operates as a single-operator CA and will introduce multi-person controls as the organization grows. This is reflected honestly throughout this CPS.

1. Introduction

- **CA operator / all roles:** David Condrey, Founder — david@writerslogic.com, +1 (619) 609-9959.
- **Scope:** issuance of C2PA Claim Signing Certificates to instances of WritersLogic Generator Products listed “conformant” on the C2PA Conforming Products List.
- **Incident contact (C2PA):** trust-list-admin@c2pa.org (per CA Agreement §6).
- **Public vulnerability reporting:** security@writerslogic.com (published in /.well-known/security.txt).

2. Publication & Repository

- Public CA artifacts are published at <https://writerslogic.com/.well-known/c2pa/>:
 - root-ca.crt, issuing-ca.crt, and [crl/issuing.crl](#) (DER, 30-day validity).
 - This CPS.
- The Root CA certificate is submitted to the C2PA Governing Authority for the C2PA Trust List.

3. Identification & Authentication

- **Subscribers** are WritersLogic Generator Products with conformant status on the C2PA Conforming Products List. Eligibility is confirmed against the C2PA program record before certificate issuance.

- Certificate Signing Requests are verified for proof of key possession and for a Distinguished Name that correctly identifies the Generator Product.

4. Certificate Life-Cycle

- **Issuance:** only to conformant Generator instances, at an assurance level not exceeding the product's Max Assurance Level, adjusted by any Dynamic Evidence presented at enrollment.
- **Validity periods:** Root CA 20 years; Issuing CA 10 years; Claim Signing Certificates 365 days (rotated).
- **Revocation:** certificates are revoked on key compromise, information inaccuracy, loss of conformant status, or C2PA direction. The CRL is regenerated and republished within 24 hours of a revocation. C2PA is notified of any compromise within 48 hours per CA Agreement §6.
- **Certificate status:** provided via CRL (RFC 5280) at the published distribution point. OCSP is not currently offered; CRL is the authoritative status mechanism.

5. Facility, Management & Operational Controls

- **Physical/logical security:** the Root CA private key is held offline (air-gapped storage) and used only to sign the Issuing CA and CRLs. The Issuing CA key is held in a controlled, access-restricted environment.
- **Separation of duties:** WritersLogic operates as a **single-operator CA** at current scale; the Founder performs all CA roles. Dual control and role separation will be introduced as staffing permits.
- **Audit logging:** every certificate issuance, revocation, and CRL generation is logged with timestamp, operator, and subject.
- **Records retention:** CA operational records and issued-certificate records are retained for **7 years**.
- **Disaster recovery:** encrypted, offline backups of CA keys and the CA database are maintained in geographically separate locations. A documented compromise and disaster-recovery procedure governs key restoration and, if required, key rollover and re-issuance.

6. Technical Security Controls

- **Key generation & protection (Assurance Level 1):** CA keys are ECDSA P-384, generated with OpenSSL, stored encrypted at rest with filesystem access restricted to the operator. The Root CA key is kept offline. This meets Assurance **Level 1** (software-based key protection with documented controls).
- **Level 2 path:** for Assurance Level 2, the Root and Issuing CA keys will be generated and held in a FIPS 140-2/3 **Hardware Security Module** via a witnessed key ceremony, and Generator Product instances will present hardware-backed attestation (Dynamic Evidence).
- **Algorithms:** ECDSA P-384 with SHA-384, consistent with existing C2PA Trust List members.

7. Certificate & CRL Profiles

- Certificates are X.509 v3 conforming to C2PA Certificate Policy §7.1. Claim Signing Certificates carry the C2PA Assurance Level extension (c2pa-al, base arc 1.3.6.1.4.1.62558.3) at the issued level. CRLs conform to RFC 5280.
- Root CA G1: CN=WritersLogic C2PA Root CA G1, SHA-256 0E:E5:CD:D3:18:CF:A2:20:29:50:72:10:3D:DF:45:09:AC:59:1A:43:FE:5D:1E:63:9C:4D:4B:0C:4F:1E:FF:5D.
- Issuing CA G1 L1: CN=WritersLogic C2PA Claim Signing ICA G1 L1, SHA-256 C1:38:CE:78:FF:C7:14:DF:E5:0E:72:B9:32:BB:F7:E6:91:FF:2A:C7:B5:5E:45:04:2D:AD:DF:AA:A1:A2:8B:96.

8. Compliance Audit

- WritersLogic performs an internal self-assessment against this CPS and the C2PA Certificate Policy. Independent third-party audit will be undertaken if and when required by the C2PA Conformance Program or a higher assurance level.

9. Legal

- Governed by the executed C2PA Certification Authority Agreement (New York law). WritersLogic indemnifies the C2PA parties; C2PA aggregate liability is capped at US \$100; confidentiality obligations survive five years. Certificate services are offered on fair, non-discriminatory terms.