C2PA Standards Alignment

How CreatorGuard extends the Coalition for Content Provenance and Authenticity specification with identity binding and machine-readable authorization state.

TO	Enterprise Infrastructure Evaluation Committee / Chief Risk Officer	DATE	June 01, 2026
FROM	CreatorGuard Technology LLC Architecture Team	DOCKET	USPTO 85498 · Patent Pending
RE	C2PA Interoperability and Authorization Extension Architecture	VERSION	cgp-1.0

1. Alignment objective

This memorandum documents how CreatorGuard implements, aligns with, and extends the technical specifications established by the Coalition for Content Provenance and Authenticity (C2PA). CreatorGuard treats content provenance as an open, interoperable internet security standard and is designed to complement — not replace — existing C2PA infrastructure investments made by Adobe, Microsoft, Google, BBC, and other C2PA member organizations.

2. Core mapping to the C2PA specification

C2PA component	CreatorGuard implementation	Status
Assertions (atomic provenance facts)	CreatorGuard generates assertions tracking origin, creation timestamp, asset format, and identity of the registering entity. Struct	Aligned
Hard binding (SHA-256/384 content hash)	CreatorGuard applies SHA-256 cryptographic hash over the asset binary payload at ingestion. Any downstream byte-level altera	Aligned
Manifest store (chained provenance history)	Multiple manifests are chained sequentially to form a complete provenance history as the asset migrates across platforms and u	Aligned
Soft binding (decoupled verification)	When embedded manifests are stripped by legacy distributors, CreatorGuard uses structural fingerprinting to match the asset ba	Aligned
C2PA credential (signed manifest)	CreatorGuard outputs a W3C Verifiable Credential in JSON-LD format, signed with Ed25519Signature2020. Compatible with C2	Extended

3. What CreatorGuard adds above the C2PA baseline

C2PA establishes what happened to an asset and when. It does not establish who legally authorized its use or what permissions are attached. CreatorGuard fills this gap with two extension layers:

Extension layer	What it provides	Why C2PA alone does not solve this
Identity binding	Cryptographic binding of the content creation event to a ve[illegible]	C2PA manifests can be created by any party — [illegible]
Authorization state	Machine-readable governance signals: AI training authori[illegible]	C2PA records what happened[illegible]

4. Integration statement

CreatorGuard can consume provenance assertions generated by C2PA-compatible systems and extend them with identity binding and authorization state information without breaking the C2PA schema or causing compliance validation failures downstream. By utilizing structured JSON-LD Verifiable Credentials and standard Ed25519 cryptographic validation pathways, the CreatorGuard layer integrates into existing CDN pipelines and platform ingestion loops without requiring structural re-engineering of underlying C2PA infrastructure.
