C2PA Conformance Program

C2PA Technical Working Group Conformance Task Force

Version 0.1, 2025-06-02

Table of Contents

1. Introduction

With the increasing velocity of digital content and the increasing availability of powerful creation and editing techniques, establishing the provenance of media is critical to ensure transparency, understanding, and ultimately, trust.

To address this issue at scale for publishers, creators and consumers, the Coalition for Content Provenance and Authenticity (C2PA) has developed a technical specification (C2PA Content Credentials Specification) for providing content provenance and authenticity. It is designed to enable global, opt-in, adoption of digital provenance techniques through the creation of a rich ecosystem of digital provenance enabled applications for a wide range of individuals and organizations while meeting appropriate security requirements.

The Specification has seen wide-scale acceptance but is limited without a robust governance framework and conformance program to provide required transparency for relying parties and accountability for governed parties which need to demonstrate recognized conformance of Specification requirements. This is the intent of the C2PA Governance Framework and C2PA Conformance Program.

1.1. Note: Regarding this Interim Conformance Program Release v.0.1

The work of the C2PA is fluid as the organization has worked diligently to issue its C2PA Content Credentials Specification v2.2 while committing to a long-term C2PA Governance Framework and C2PA Conformance Program. The release of Spec 2.2 precedes the implementation of a fully-formed Conformance Program. Therefore, the interim C2PA Governance Framework and associated C2PA Conformance Program only includes limited governance structures it can to be able to comply with the Spec 2.2 release. They include:

- The C2PA Trust List comprised of CAs that issue signing certificates to Generator Products under the C2PA Certificate Policy.

- C2PA Conforming Products List comprised of Generator Product and Validator Product companies and their products that sign or validate C2PA Content Credentials Specification compliant C2PA Manifests under a minimal set of requirements in addition to self-asserting their compliance to the C2PA Content Credentials Specification (v2.2 or later).

In order to realize the full potential of C2PA's vision for content provenance and authenticity more broadly, it is of paramount importance to architect a transitive trust assurance framework (i.e. the C2PA Conformance Program) to allow participants to collectively add confidence in the trustworthiness of C2PA Content Credentials by conforming with the C2PA Content Credentials Specification and its encapsulating governing requirements that comprise its C2PA Governance Framework.

The C2PA Conformance Program assures holders of C2PA content credentials that Generator Product and Validator Products are in conformance with the C2PA Content Credentials Specification and other requirements of the C2PA Conformance Program by publishing a C2PA Trust List and a C2PA Conforming Products List that act in the interest of all governed parties, manifest consumers and relying parties of digital objects that contain hardbound C2PA Content Credentials. For this interim release, the C2PA only requires certification authorities and conforming products companies to self-assert they are meeting specification and implementation security requirements in addition to signing legal agreements over their responsibilities within the program.

The C2PA Manifest consumer acquires trust from the ecosystem's ability to govern actors to follow through on its commitments to conform to a set of governance requirements. The participants are:

- Governing Authority
- Administering Authority
- Governed Party

2. Glossary

The C2PA has established the following glossary to define the following terms and constructs germane to the C2PA ecosystem. Other terms not specified in this glossary may be found in the Trust Over IP Glossary located at (https://trustoverip.github.io/toip/glossary).

2.1. Administering Authority

The party that the C2PA Governing Authority empowers to operate its Conformance Program on its behalf. It recognizes and accredits key conformance roles which agree to participate in the program. The C2PA Conformance Task Force of the Technical Working Group operates in this capacity.

2.2. Applicant

An entity that has created a Generator Product or a Validator Product and wishes for it to be deemed a Conforming Product according to the governance framework of the C2PA Conformance Program, and added to the C2PA Conforming Products List.

2.3. Applicant's Representative

A natural person who is a duly-authorized employee or agent of the Applicant.

2.4. Assertion

Refer to Section 2, "Glossary", of the C2PA Content Credentials specification.

2.5. Asset

Refer to Section 2, "Glossary", of the C2PA Content Credentials specification.

2.6. Assurance Level

An indication to a Relying Party of the level of confidence that it may have that assertions and claims signed with a given C2PA Claim Signing Certificate reflect the intended behavior of the Generator Product instance. A higher Assurance Level allows the Relying Party to have a greater level of confidence.

The Assurance Level is conveyed through the `c2pa-al` (`1.3.6.1.4.1.62558.3`) X.509 v3 certificate extension in a C2PA Claim Signing Certificate. The value of this extension is an encoded OID value that corresponds to a numeric value no higher than the Max Assurance Level for a given conforming Generator Product. The OID values corresponding to each Assurance Level are defined in the C2PA `oid.txt` MIB definition file.

The Assurance Level in the C2PA Claim Signing Certificate that is issued to an instance of a

conforming Generator Product may be lower than the Max Assurance Level that the Generator Product is potentially eligible for, based on the Dynamic Evidence that is presented by that instance of the Generator Product

2.7. Attestation

"The process of providing a digital signature for a set of measurements securely stored in hardware, and then having the requester validate the signature and the set of measurements." NIST

2.8. C2PA Certificate Policy

A document that sets the requirements that SHALL be met by Certification Authorities (CAs) in the process of issuing digital certificates to Subscribers that implement C2PA Conforming Products that create assets with digital content and C2PA manifests, and the requirements that SHALL be met by the Subscribers in their use of the certificates.

2.9. C2PA Claim

Refer to Section 2, "Glossary", of the C2PA Content Credentials specification.

2.10. C2PA Claim Signing Certificate

An X.509 certificate issued by one of the Certification Authorities on the C2PA Trust List to an instance of the Conforming Implementer's conforming Generator Product, and names the Generator Product as the subject of the certificate.

2.11. C2PA Conformance Program

A risk-based governance program intended to hold Applicants who want to demonstrate their conformance to its requirements and then differentiate themselves through C2PA recognition by satisfying program requirements being acknowledged as achieving that level of conformance. It consists of a set of processes, policies, and requirements governing the designation of Applicant Generator Products or Validator Products as Conforming Products, and the designation of Certification Authorities as adhering to the C2PA Certificate Policy, as defined by the C2PA Technical Working Group Conformance Task Force.

Processes include:

- Evaluation of the C2PA-related functions of the Applicant Generator Product or Validator Product as adhering to the normative requirements of the C2PA Content Credentials specification
- Evaluation of security attributes of the Target of Evaluation, which includes the Applicant Generator Product against the Generator Product Security Requirements, which results in assigning it a Max Assurance Level
- Evaluation of the processes, controls, and technical capabilities of Certification Authorities as required by the C2PA Certificate Policy
- Signing of the requisite legal agreements to become a member of the program.

2.12. C2PA Conforming Products List

The canonical record of all Conforming Products that have been deemed conformant according to the stipulations of the C2PA Conformance Program

2.13. C2PA Content Credentials

Refer to Section 2, "Glossary", of the C2PA Content Credentials specification.

2.14. C2PA Content Credentials Specification

A globally recognized standard for providing digital asset content provenance and authenticity. It is designed to enable global, opt-in, adoption of digital provenance techniques through the creation of a rich ecosystem of digital provenance enabled applications for a wide range of individuals and organizations while meeting appropriate security requirements.

2.15. C2PA Governance Framework

A collection of governance documents which defines the C2PA trust ecosystem including roles, requirements and processes used by the C2PA Governing Authority to achieve greater assurance over the provenance and authenticity of digital asset content.

2.16. C2PA Manifest

Refer to Section 2, "Glossary", of the C2PA Content Credentials specification.

2.17. C2PA Trust List

Refer to Section 2, "Glossary", of the C2PA Content Credentials specification.

In the context of the C2PA Conformance Program, a C2PA-managed list of X.509 certificate trust anchors (either root or subordinate Certification Authorities) that issue certificates to conforming Generator Products under the C2PA Certificate Policy.

2.18. C2PA TSA Trust List

A C2PA-managed list of X.509 certificate trust anchors (either root or subordinate Certification Authorities) that issue time-stamp signing certificates to Time-Stamping Authorities (TSA).

2.19. Certification Authority

A trusted entity that issues, signs, and revokes digital certificates that bind public keys to subscriber identities. CAs are also known as PKI Certificate Authorities because they issue certificates based on public key infrastructure (PKI). These certificates contain credentials that confirm the possession of a private key by an entity, among other verified attributes. Generator Products sign C2PA Manifests using digital signing credentials issued by CAs.

An entity on the C2PA Trust List that is trusted by the C2PA Conformance Program to issue X.509 C2PA Claim Signing Certificates to instances of conforming Generator Products.

An organization that operates a Certification Authority may also operate a Time-Stamping Authority.

2.20. Claim Generator

Refer to Section 2, "Glossary", of the C2PA Content Credentials specification.

2.21. Conformance Criteria

A set of normative requirements that the C2PA expects a Governed Party to demonstrate its conformance as part of the C2PA Conformance Program. This criteria consists of requirements derived from the C2PA Content Credentials Specification itself, and other ancillary requirements outside of the C2PA Specification including Generator Product Security Requirements document and requirements in the C2PA Certificate Policy.

2.22. Conforming Implementer

An Applicant who has become a member of the C2PA Conformance Program, and has at least one Generator Product or Validator Product in good standing on the C2PA Conforming Products List.

2.23. Conforming Product

A Generator Product or a Validator Product that has been deemed conformant by the C2PA Conformance Program and added to the C2PA Conforming Products List with a status of `conformant`. A Generator Product that is deemed conformant is also assigned a Max Assurance Level that is recorded on the C2PA Conforming Products List.

Only instances of conforming Generator Products are eligible to receive C2PA Claim Signing Certificates from a Certification Authority on the C2PA Trust List.

2.24. Digital Content

Refer to Section 2, "Glossary", of the C2PA Content Credentials specification.

2.25. Dynamic Evidence

Attributes that a Certification Authority evaluates during automated enrollment for a C2PA Claim Signing Certificate by an instance of a Generator Product, usually relayed to the Certification Authority in the form of a verifiable hardware-backed artifact, such as a key or platform attestation report.

Dynamic Evidence may result in a particular instance of a Generator Product receiving a certificate of an Assurance Level that is lower than the Max Assurance Level that the Generator Product is potentially eligible for.

2.26. Generator Product

The set of software, hardware, and platform configurations created by an Applicant that work together as a system to produce digital Assets with C2PA manifests. The asset's active manifest contains assertions made by the Generator Product, and features a claim signed by a certificate where the Generator Product is the subject, about the provenance of the asset.

A Generator Product may integrate Claim Generator functions monolithically, or rely on a discrete Claim Generator service available either locally (e.g. on-device), or remotely (e.g. hosted in a cloud service). The monolithic or discrete Claim Generator service may be created by the Applicant or by a different entity.

Because the Generator Product is always the Signer in the C2PA Conformance Program, and is always the entity listed on the C2PA Conforming Products List, it is accountable for the conformance of the Assets with C2PA manifests that it generates with the normative requirements of the C2PA Content Credentials Specification, regardless of whether it integrates Claim Generator functions

directly or relies on a discrete service.

2.27. Generator Product Security Architecture Document

A filled-out version of the Generator Product Security Architecture Document Template, submitted by the Applicant to the C2PA Conformance Program as part of its application for inclusion on the C2PA Conforming Products List.

2.28. Generator Product Security Requirements

Security-related implementation requirements for a Generator Product to achieve a particular Max Assurance Level, detailed in a document of the same name.

2.29. Governed Party

An organization which desire to play a recognized role in the C2PA Conformance Program. It applies to the C2PA Conformance Program which requires them to sign a legal agreement and have their product reviewed prior to entering them on the C2PA Trust List or the Conforming Products List. Governed Parties of the C2PA ecosystem are Certification Authorities and Applicants that elect to apply and and abide by the C2PA Conformance Program requirements.

2.30. Governing Authority

The organization responsible for the trust of the ecosystem. It empowers an Administering Authority to manage the ecosystem and certifying entities to convey trust. The C2PA is the governing party of its conformance program driven by its Steering Committee.

2.31. Hosting Environment

Server-side environment hosting a subset of Generator Product or Validator Product mechanisms and functionalities.

2.32. Implementation Class - Backend

An implementation architecture for a Target of Evaluation in which assets, assertions, claims, and claim signatures are generated in one or more Hosting Environments, including those hosted on premises or on commercial cloud service providers.

2.33. Implementation Class - Distributed

An implementation architecture for a Target of Evaluation which is composed of Edge and Backend subsystems, where the generation of assets, assertions, claims, and claim signatures is distributed between those subsystems.

2.34. Implementation Class - Edge

An implementation architecture for a Target of Evaluation in which assets, assertions, claims, and claim signatures are generated on an endpoint that operates at the edge of the network, such as:

- Smartphones and smartphone applications
- Laptop and desktop computers
- Fixed-function mirrorless cameras and surveillance cameras

- Portable audio recorders

2.35. Manifest Consumer

The number and variety of consumers that rely upon the content provenance and authenticity of digital objects using content credentials are too numerous to capture in this document. In order for Manifest Consumers to consume Content Credentials supported by the C2PA, they MUST use C2PA-approved service providers. In addition, the C2PA Specification cites mandatory requirements for Manifest Consumers. While the C2PA mandates these requirements and discloses them in the Specification, it does not hold Manifest Consumers accountable to conform to these requirements within its governance framework.

2.36. Max Assurance Level

A numeric designation, chosen at the discretion of the C2PA Conformance Program, based on evaluating the security functions, properties, and attributes of an Applicant Generator Product against the Generator Product Security Requirements defined by the C2PA Conformance Program.

2.37. Registration Authority

An entity authorized by the Certification Authority to collect, verify, and submit information provided by Applicants and/or Subscribers which is to be entered into public key certificates. The term RA refers to hardware, software, and individuals that collectively perform this function, including tasks such as validating platform attestations and presence of potential Subscriber implementations on the C2PA Conforming Products List. The RA operates under the CA's authority and adheres to the guidelines set forth in the C2PA Certificate Policy.

2.38. Reliable Method of Communication

A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant's Representative.

2.39. Relying Party

An entity that evaluates the trustworthiness of Assertions made by a Signer in a C2PA Asset, based on the Signer's identity and the Assurance Level encoded into the C2PA Claim Signing Certificate.

2.40. Rich Execution Environment

Refer to NIST definition. Abbreviated as REE.

2.41. Root of Trust

Refer to NIST definition. Abbreviated as RoT.

2.42. Security Incident

"An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies." NIST

2.43. Signer

Refer to Section 2, "Glossary", of the C2PA Content Credentials specification.

In the C2PA Trust Model, the Assertions enumerated in the `created_assertions` object of the C2PA Claim are attributed to the Signer.

In the context of the C2PA Conformance Program, an instance of the conforming Generator Product listed on the C2PA Conforming Products List is always the Signer.

2.44. Static Evidence

Attributes of the Generator Product Target of Evaluation that are documented in the Generator Product Security Requirements document which the Administering Authority evaluates during its assessment of the Applicant's Generator Product, in order to assign a Max Assurance Level.

2.45. Subscriber

An Applicant that has become a customer of one of the Certification Authorities on the C2PA Trust List, and is eligible to receive C2PA Claim Signing Certificates for use by instances of their conforming Generator Product.

2.46. Target of Evaluation

The system which is evaluated by the C2PA Conformance Program for its functional correctness and the security of its implementation. It consists of the sum total of the Generator Product or Validator Product created by an Applicant, **and** the subsystems that it relies on to produce or validate Assets with C2PA Manifests. Those subsystems need not be created by the Applicant, but are necessary for the proper operation of the Generator Product or the Validator Product.

The functional capabilities and security properties of those subsystems contribute to the overall security of the Applicant's product, and are thus are considered by the C2PA Conformance Program when assigning an Assurance Level to a conforming Generator Product.

Targets of Evaluation can have Edge, Backend, or Distributed implementation architectures.

2.47. Time-Stamping Authority

A server that provides electronic certification and trust services by creating a hash of a document or digital information. The hash verifies the date and time of the document's creation or last modification, and acts as an independent witness to prove that the document has not changed since it was signed. This is similar to how a notary acts for online documents. TSAs, that are part of Applicant Certification Authorities, that want to be recognized as issuing digital signing credentials approved by the C2PA, must satisfy the requirements of the program to be considered approved and designated as such within its governance records.

2.48. Trusted Execution Environment

Refer to NIST definition. Abbreviated as TEE.

2.49. Validator

Refer to Section 2, "Glossary", of the C2PA Content Credentials specification.

2.50. Validator Product

The set of software, hardware, and platform configurations created by an Applicant that work together as a system to validate digital Assets with C2PA manifests.

A Validator Product may integrate Validator functions monolithically, or rely on a discrete Validator service available either locally (e.g. on-device), or remotely (e.g. hosted in a cloud service). The monolithic or discrete Validator service may be created by the Applicant or by a different entity.

Because the Validator Product is always the entity listed on the C2PA Conforming Products List, it is accountable for producing correct validation results in adherence with the normative requirements of the C2PA Content Credentials Specification, regardless of whether it integrates Validator functions directly or relies on a discrete service.

3. Purpose of the Program

The ultimate goal of the C2PA Conformance Program is to tackle the extraordinary challenge of trusting media in a context of rapidly evolving technology and the widespread adoption of powerful creation and editing techniques. To this end, the C2PA Conformance Program is designed to enable global, opt-in, adoption of digital provenance techniques through the creation of a rich ecosystem of digital provenance enabled applications for a wide range of individuals, organizations and devices, while meeting appropriate security and privacy requirements, as well as human rights considerations.

This goal cannot be achieved solely upon the issuance of the C2PA Content Credentials Specification; it needs a coordinated and regulated effort by all participants that play a role in conforming to the Specification to be accountable. Furthermore, it requires an unbiased and open governance process that enables Applicants to clearly understand the process of conformance and demonstrate that it meets the program's requirements for the benefit of a digital society. While this interim version for Spec v2.2 release does not purport to achieve these goals, it comprises a limited step by establishing essential roles and constructs needed for a robust governance and conformance program.

The C2PA Conformance Program rewards Applicant Generator Products, Validator Products and Certification authorities which successfully demonstrate conformance to program requirements by placing machine-readable access information for that Applicant in controlled and accessible lists so Manifest Consumers have confidence that they are working only with approved C2PA Conformance Program participants that have achieved that status. The administration of these trust lists is performed by the C2PA Administering Authority under the governance of its Governing Authority.

4. Program Scope

The scope of the C2PA Conformance Program includes all the tangible components: participants, processes and artifacts.

4.1. Program Participants

- Generator Product Company: An Applicant that has created a Generator Product.
- Validator Product Company: An Applicant that has created a Validator Product.
- Certification Authority
- Time-Stamping Authority
- Manifest Consumer

- Relying Party

5. Assurance Levels

As part of this Conformance Program, the C2PA has established the notion of a Max Assurance Level based on the security attributes of the implementation architecture of a Generator Product, and the notion of an Assurance Level which a particular instance of the Generator Product is eligible for based on the dynamic evidence it is able to present at the time of certificate enrollment with a Certification Authority.

The implementation security requirements associated with each Assurance Level is detailed in the C2PA Generator Product Security Requirements document.

For the interim implementation of the C2PA Conformance Program, two levels are in operation, Assurance Level 1 and Assurance Level 2. The Assurance Level associated with an instance of a Generator Product is encoded as the value of a custom X.509v3 certificate extension (as defined in the C2PA's `OID.txt` MIB definition file) in the C2PA Claim Signing Certificate that the instance of the Generator Product uses to sign C2PA Claims.

Relying Parties are advised to review and understand the implications of receiving Assets signed by C2PA Claim Signing Certificates of a particular Assurance Level.

6. Conformance Criteria

6.1. C2PA Content Credentials Specification Requirements

6.1.1. C2PA Content Credentials Specification Process Requirements

The C2PA Content Credentials Specification provides prescriptive guidance on the generation and validation of manifests that are hard-bound to Assets. The minimum release level of the C2PA Content Credentials Specification for applicability of this version of the C2PA Conformance Program is v2.2. The Specification includes normative requirements and non-normative recommendations. The C2PA Conformance Program has isolated the normative requirements (included in SHALL statements) and have attributed them to specific roles in the ecosystem where Applicants will eventually be held accountable against these role sets for C2PA recognition. The following role sets have been identified:

Generator Product Specific Requirements

The C2PA Content Credentials Specification includes over 300 normative requirements attributed to Generator Products which create C2PA manifests for consumers. The C2PA Conformance Program will eventually require Claim Generators to demonstrate complete conformance to these exacting requirements in order to receive its approval. Requirements for Generator Products include:

- Manifest Formatting
- Manifest Redaction
- Claim Signing
- Timestamp Insertion
- Cryptographic Hash Computation

- File-type Specific Handling Requirements

Validator Product Specification Requirements

The C2PA Content Credentials Specification includes over 150 normative requirements attributed to claims Validator Products which validate C2PA manifests for consumers. The C2PA Conformance Program will eventually require claims validators to demonstrate complete conformance to these exacting requirements in order to receive its approval. Requirements for Validator Products include:

- Conditions for a Fully Formed Manifest Sufficient for Validation

- Signature Validation

- Timestamp Validation

- Assertion Validation

- Cryptographic Hash Validation

- Validation Result Reporting

Certification Authority Specification Requirements

The C2PA Conformance Program has enumerated the normative requirements from the C2PA Content Credentials Specification that are applicable to Certification Authorities in the C2PA Certificate Policy.

6.2. Generator Product Implementation Security Requirements

Not all implementations of the C2PA Specification are the same. While all Generator Products and Validator Products are required to abide by the normative requirements of the C2PA Specification, the C2PA Governing Authority has established additional requirements that mandate specific security attributes when an Applicant is creating their implementation of a Generator Product.

An Applicant must, at a minimum, meet the implementation security requirements associated with Assurance Level 1 in order for their Generator Product to be included on the C2PA Conforming Products List.

6.3. Business Requirements

6.3.1. Conformance Program Fee Schedule

Application Fees to apply to the C2PA Conformance Program for Certification Authorities, Generator Product and Validator Product companies is free of charge.

Conformance Fee for adding Applicant records to the CA Trust List and the Conforming Products List are free of charge.

6.4. Process Requirements for Applicants of the C2PA Conformance Program

The following section describes the initial Applicant process for the C2PA Conformance Program from intake application to denoting recognition of an Applicant's meeting program requirements through its application or service being added to its respective trust list.

6.4.1. Application Intake Form

All Applicants (Certification Authorities, Generator Products and Validator Products) MUST apply to the C2PA Conformance Program using this Intake Form (LINK TO THE INTAKE FORM HERE) The intake form describes the governed role of the Applicant and (if applicable) the level of security implementation assurance it is seeking within the program.

6.4.2. Additional Evidence Requested

Depending on the role requested and the level of security implementation assurance requested on the intake form, the C2PA may request additional evidence to demonstrate that the application is meeting Conformance Program requirements.

Specifically, Applicants that are applying to the Conformance Program for the purpose of including their Generator Product on the C2PA Conforming Products List are required to submit a Generator Product Security Architecture Document, whose contents are described in the C2PA Generator Product Security Requirements document.

The C2PA Conformance Program will reach out to the Applicant's Point of Contact by email and provide a template in which it is seeking additional evidence. To protect both the Applicant and the C2PA over their respective responsibilities over this information, we suggest that the Applicant execute its Legal Agreement which covers responsibilities over this information

6.4.3. Legal Agreement Execution

Prior to accepting Applicants into the C2PA Conformance Program, each Applicant MUST sign a legal agreement with the C2PA committing to the C2PA Conformance Program requirements. The C2PA has established separate templates for its legal agreements depending on the role that the Applicants requests within the program (Generator Product, Validator Product and Certification Authority).

6.4.4. Evidence and Legal Agreement Review

The Administering Authority of the C2PA Conformance Program will review conformance evidence supplied by the Applicant to determine whether the Applicant has met conformance program requirements. This may involve asynchronous email back and forth. Once the Administrator has satisfied itself with the evidence and confirmed that the legal agreement has been executed, we will inform the Applicant of its status as approved or rejected (with feedback or recommendations to correct). If approved, the Administer will proceed to establishing an Applicant record on either the C2PA Trust List or the Conforming Products List.

6.4.5. Establishment of a Trust List Record

Approved Applicants will either appear on the Certification Authority Trust List or the C2PA Conforming Products List. The C2PA Administer will add attributes of the Applicant's trust list record based on information supplied on its Intake Form. Once a record has been established to the respective Trust List, the C2PA Administrator will preview the record and confirm the contents of the record prior to publishing. Once confirmed with the Applicant, the C2PA will publish the Trust List record.

6.4.6. Definition of Material Change Requiring New Conformance Program Application

Once a record of the Applicant's Generator Product is published on the C2PA Conforming Products

List, the product SHALL re-submit their Generator Product or Validator Product to the Conformance Program IF the product undergoes a "material change", one that constitutes a clear modification to the product's Conforming Product List record or its conformance to the Generator Product Security Requirements Document. The modified product SHALL be attributed to a new record id on the C2PA Conforming Products List.

6.5. Machine-Readable List Operation

6.5.1. Use of C2PA Machine-Readable Lists

- Approved Certification Authority Applicants of the C2PA Conformance Program appear on the C2PA Trust List.

- Approved Generator Products and Validator Products appear on the C2PA Conforming Products List.

- Applicants whose conforming Generator Products appear on the C2PA Conforming Products List MUST access the C2PA Trust List to determine whether a Certification Authority has been approved by the Conformance Program.

- Instances of conforming Generator Products MUST be issued a C2PA Claim Signing Certificate from a CA that appears on the C2PA Trust List.

- CAs that appear on the C2PA Trust List MUST only issue C2PA Claim Signing Certificates to instances of Generator Products that have a record with a `status` of `conformant` on the C2PA Conforming Products List.

- Conforming Validator Products SHALL regularly refresh the C2PA Trust List to determine whether a C2PA Claim is signed with a C2PA Claim Signing Certificate that cryptographically ladders up to a Certification Authority on the C2PA Trust List.

- Validator products SHOULD access the C2PA Conforming Products List to determine whether Generator Products are approved and recognized by the C2PA Conformance Program. Manifest consumers SHOULD review the C2PA Trust List and C2PA Conforming Products List to determine whether CAs, Generator Products, or Validator Products have been approved by the C2PA and have an active status in the program.

6.5.2. Security Controls Over C2PA Machine-Readable Lists

The C2PA Conformance Program mandates tight access controls over the C2PA Trust List, the C2PA TSA Trust List, and the C2PA Conforming Products List while maintaining high availability to relying parties.

Access controls to the machine-readable lists are limited to designated members of the C2PA Conformance Program Task Force which administers the program. All changes to any of the machine-readable lists require multi-party approval quorum.

6.5.3. Removal of Conforming Products List / C2PA Trust List Record

The C2PA reserves the right to and remove Applicants from the C2PA Trust List and C2PA TSA Trust List, or revoke the `conformant` status of a Generator Product or Validator Product on the C2PA Conforming Products List.

Factors indicating the need for removal MAY originate from the global marketplace or within the C2PA itself. If an action has been taken for machine-readable list removal, the Governed Party will be formally notified and required to appear before the C2PA Conformance Program Task Force where

evidence will be considered concerning the party's violation of the terms of its acceptance as an approved service provider of its conformance program. Based on this evaluation, the Conformance Task Force will make a recommendation for removal to the C2PA Steering Committee for its final decision.

6.5.4. Dispute Mediation and Arbitration

The C2PA Conformance Program has mediation measures in place to support appeals of C2PA actions. It has established an independent committee which acts in the interests of all parties to mediate disputes between parties. Any dispute between the C2PA Conformance Program and a Governed Party not resolved by mediation shall be settled by the arbitration process defined in the legal agreement between the parties.

6.5.5. Versioning

This Interim Conformance Program v.01 will continue as described in this document until a planned, more robust Conformance Program is adopted and placed into operation.