



C2  
PA

Coalition for  
Content Provenance  
and Authenticity

# C2PA Governance Framework

C2PA Technical Working Group Conformance Task Force

Version 0.1, 2025-06-02

# Table of Contents

1. Introduction	1
2. Note: Regarding this Governance Framework Release v.0.1	1
3. Glossary	2
4. Purpose	9
5. Scope	9
6. Objectives	10
7. Principles	10
8. Revisions	11
9. Extensions	11
10. Risk Assessment	11
11. C2PA Conformance Program	11
12. Governance Requirements	13
13. Business Requirements	14
14. Information Trust Requirements	14
15. Privacy, Inclusion, Equitability and Accessibility Requirements	14
16. Legal Agreements	15

# 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](#).

This [C2PA Governance Framework](#) has been created using published templates issued by the Trust Over IP Project (<https://trustoverip.org/our-work/deliverables/>). Trust Over IP (ToIP) is a part of the Linux Foundation Decentralized Trust Foundation (LFDT) and is hosted by the Linux Foundation under its Joint Development Foundation legal structure. It produces a wide range of tools and deliverables organized into five categories:

1. Specifications to be implemented in code
2. Recommendations to be followed in practice
3. Guides to be executed in operation
4. Whitepapers to assist in decision making
5. Glossaries to be incorporated in other documents

## 2. Note: Regarding this Governance Framework 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](#)

## 3. Glossary

### 3.1. 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.

### 3.2. 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](#).

### 3.3. Applicant's Representative

A natural person who is a duly-authorized employee or agent of the [Applicant](#).

### 3.4. Assertion

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

### 3.5. Asset

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

### 3.6. 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](#)

### 3.7. 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](#)

### 3.8. 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.

### 3.9. C2PA Claim

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

### 3.10. 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.

### 3.11. 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.

### 3.12. 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

### 3.13. C2PA Content Credentials

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

### 3.14. 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.

### 3.15. 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.

### 3.16. C2PA Manifest

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

### 3.17. 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](#).

### 3.18. 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).

### 3.19. 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](#).

### 3.20. Claim Generator

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

### 3.21. 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](#).

### 3.22. 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](#).

### 3.23. 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](#).

### 3.24. Digital Content

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

### 3.25. 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.

### 3.26. 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.

### **3.27. 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](#).

### **3.28. 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.

### **3.29. 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.

### **3.30. 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.

### **3.31. Hosting Environment**

Server-side environment hosting a subset of [Generator Product](#) or [Validator Product](#) mechanisms and functionalities.

### **3.32. 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.

### **3.33. 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.



### 3.34. 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

### 3.35. 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.

### 3.36. 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](#).

### 3.37. 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](#).

### 3.38. 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.

### 3.39. 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](#).

### 3.40. Rich Execution Environment

Refer to [NIST definition](#). Abbreviated as REE.

### 3.41. Root of Trust

Refer to [NIST definition](#). Abbreviated as RoT.

### 3.42. 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](#)

### 3.43. 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.

### 3.44. 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](#).

### 3.45. 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](#).

### 3.46. 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 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.

### 3.47. 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.

### 3.48. Trusted Execution Environment

Refer to [NIST definition](#). Abbreviated as TEE.

### 3.49. Validator

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

### 3.50. 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.

Other terms not specified in this [Glossary](#) may be found in the Trust Over IP Glossary located at (<https://trustoverip.github.io/toip/glossary>).

## 4. Purpose

The goal of the [C2PA Content Credentials Specification](#) is to tackle the extraordinary challenge of trusting media in a context of rapidly evolving technology and the democratization of powerful creation and editing techniques. To this end, the Specification 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 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.

The consistent application of the Content Credentials Specification's requirements upon digital objects raises public confidence on their source and provenance trail. This is especially critical with the advent of artificially produced content where provenance is questioned.

## 5. Scope

The scope of the [C2PA Governance Framework](#) includes all the tangible components of C2PA ecosystem (participants, requirements, processes and artifacts) so that relying parties have clarity on

the measures that the C2PA [Governing Authority](#) has enacted in order for consumers to rely upon content credentials.

The [C2PA Conformance Program](#) rewards Applicant generators, [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](#).

## 5.1. Program Participants

- [Governing Authority](#)
- [Administering Authority](#)
- [Generator Product Company](#)
- [Validator Product Company](#)
- [Certification Authority](#)
- [Time-Stamping Authority](#)
- [Manifest Consumer](#)
- [Relying Party](#)

## 6. Objectives

The objectives of the C2PA Governance Framework are: - Provide a generally accepted method of communicating provenance rights to digital content that mitigates authenticity risks from artificial intelligence engines and bad actors; - Expand the value content credentials can bring to the global economy by enabling cryptographically verifiable digital content credentials; - Make it easy and profitable for a wide range of generator and [Validator Products](#) to generate and validate content credentials that is recognized by the C2PA; - Attract developers to build generator functionality into products that exact a stated level of security implementation assurance; - Assist jurisdictions in understanding and incorporating content credential requirements for digital objects so that they are integrated into numerous critical business processes and workflows that require a stated level of assurance; - While maintaining an opt-in posture, establish C2PA as a Global Root of Trust for C2PA Content Credentials - Encourage new use cases for the use of content credentials - Establish a model for its Conformance Program which allows Applicants which demonstrate their conformance to C2PA requirements to be publicly recognized and approved.

## 7. Principles

The C2PA has established a set of guiding principles for C2PA designs, specifications and this governance framework. It can be found at: <https://c2pa.org/principles/>. The principles include the following content areas: - Overarching Goals - Expected Users - Privacy - Global Audience / Accessibility - Interoperability - Fit with Existing Workflows - Performance - Simplicity and Cost Burden - Extensibility - Misuse - References

## 8. Revisions

The C2PA is a Joint Development Project of the Linux Foundation. As such, revisions of this governance framework adheres to the defined deliverable development process found later in this document at C2PA Specification Revision Control.

## 9. Extensions

The C2PA Content Specification allows actors in a workflow to make cryptographically signed assertions about the produced C2PA asset. This signature is issued by the vendor whose software or hardware was used to generate the C2PA content credential, which is why it is called the C2PA Generator Product.

In some use cases, an individual or organization may wish to describe their own identity or assert additional metadata that can not be directly represented as by the features of the core C2PA specification. In these cases, it is recommended to use an extensions to Content Credentials that supports the identification of the actor(s) who are making these statements, along with the ability for them to securely represent their relationship to the media asset and the specific assertions they wish to make.

An example of such an assertion is the [Creator Assertions Working Group's identity assertion](#).

## 10. Risk Assessment

The C2PA Risk Assessment process allows for: - Proper consideration and identification of potential risks; - Critical analysis of potential risks in terms of likelihood and severity needed to calculate a systematic risk impact score; - Triage of risks for further treatment; - Treatment of the risks using a variety of options that include creation of risk mitigation requirements as part of the governance framework; and - Performance of an annual review of risks to ensure criticality of current risks and the consideration of emerging risks.

One of the risk treatment options is to mitigate risk by creating mandates (documented with **SHALL** and **MUST** statements) on the governance framework. The degree of conformance is dependent on C2PA Conformance Program requirements to hold governed parties accountable to that requirement. The C2PA Conformance Program is not designed to reduce risk to zero. It is designed to mitigate risks that it can within the governing rules of the ecosystem and the participation of all roles in their conformance.

Therefore, the C2PA governance processes oversees and assesses the design and operation of its Conformance Program to mitigate risk to the degree it can assert within the constructs of its authority.

The risk assessment is informed by the Harm Assessment ([LINK](#)) and Security Considerations ([LINK](#)) documentation.

## 11. C2PA Conformance Program

The C2PA Specification has seen wide-scale acceptance but is limited without a robust governance and conformance program to provide required transparency and accountability for actors which need to demonstrate recognized conformance of Content Credential Specification requirements. This is the intent of the C2PA Conformance Program. It is a risk-based governance program intended to hold Applicants who want to demonstrate their conformance and differentiate themselves through

recognition by satisfying program requirements and being acknowledged as achieving that level of conformance.

An overview of the C2PA Conformance Program can be found as a controlled document to this governance framework at: [ADD LINK HERE](#)

## 11.1. 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](#).

## 12. Governance Requirements

In addition to requirements the C2PA has defined for governed roles in its ecosystem, it also has established governance requirements for itself and its C2PA [Administering Authority](#) that governs on its behalf.

### 12.1. Steering Committee Charter

The C2PA has an established Steering Committee empowered to govern its operation. The role of the Steering Committee is documented in its charter located at <https://c2pa.org/about/charter/>. A summary of its role is as follows:

The C2PA Steering Committee approves the formation and planned activities of its technical working groups, task forces and its Conformance Program. Work includes: - Documenting and applying industry workflow requirements, informed by subject matter experts and partner organizations leading to the development of content provenance specifications. - Developing best practices and reference designs for applying those standards to the targeted industry workflows - Ensuring that the specifications can be used in ways that respect privacy and personal control of data, and promote tool availability for a wide range of organizations - Ensuring that specifications meet appropriate security requirements - Promoting selected specifications to become global standards - Overseeing its Conformance Program to ensure equitability, openness and fair treatment of all participants for the benefit of its extended ecosystem..

### 12.2. C2PA Content Credentials Specification Revision Control

The C2PA is a Joint Development Project of the Linux Foundation. As such, the C2PA adheres to the following defined deliverable development process. 1. **Pre-Draft**. Any Working Group Participant or Contributor may submit a proposed initial draft document as a candidate Draft Deliverable of that Working Group. The Working Group chair will designate each submission as a "Pre-Draft" document. 2. **Draft**. Each Pre-Draft document of a Working Group must first be Approved by the Working Group Participants of that Working Group to become a Draft Deliverable. Once the Working Group approves a document as a Draft Deliverable, the Draft Deliverable becomes the basis for all going forward work on that deliverable. 3. **Working Group Approval**. Once a Working Group believes it has achieved the objectives for its deliverable as described in the Scope, it will progress its Draft Deliverable to "Working Group Approved" status. 4. **Final Approval**. Upon a Draft Deliverable reaching Working Group Approved status, the Executive Director or his/her designee will present that Working Group Approved Draft Deliverable to all Steering Members for Approval. Upon Approval by the Steering Members, that Draft Deliverable will be designated an "Approved Deliverable." 5. **Publication and Submission**. Upon the designation of a Draft Deliverable as an Approved Deliverable, the Executive Director will publish the Approved Deliverable in a manner agreed upon by the Working Group Participants (i.e., Project Participant only location, publicly available location, Project maintained website, Project member website, etc.). The publication of an Approved Deliverable in a publicly accessible manner must include the terms under which the Approved Deliverable and/or source code is being made available under, as set forth in the applicable Working Group Charter.

### 12.3. Governance Requirements over its Conformance Program

The C2PA Steering Committee has empowered the C2PA Conformance Task Force of the Technical



Working Group to administer its conformance program but maintains oversight responsibility. The Steering Committee is responsible for the charter document of its Conformance Program and major organization and process decisions in its operations including its self-funding model. A summary of key governance processes it oversees are as follows:

### **12.3.1. Application Review**

The C2PA Conformance Program team will receive intake applications from interested Applicants. After approval, the Applicant will be entered into the program as an Applicant seeking approval and then ready to go through the process of demonstrating conformance.

### **12.3.2. Legal Agreements**

Certification Authority, Generator Product and Validator Product Applicants MUST sign legal agreements with the C2PA in order to be placed on its respective trust list as approved participants of the C2PA Conformance Program.

### **12.3.3. Participant Revocation**

The C2PA reserves the right to remove Applicants from C2PA trust lists. These actions require formal notification to the Applicant and careful consideration of evidence that the Applicant has violated the terms of its acceptance as an approved service provider of its conformance program. Once revoked, the Applicant's trust list record will be denoted as "revoked"

### **12.3.4. Appeals Process**

The C2PA Conformance Program has an appeals process that can be enacted by Applicants to appeal decisions of its approval or disapproval of Applicants.

## **13. Business Requirements**

The C2PA Steering Committee is charged with oversight and approval of business requirements of its operation. This includes the administration and funding of its conformance program.

## **14. Information Trust Requirements**

The C2PA mandates that service providers that are approved by the C2PA to participate within its ecosystem not only conform to the requirements of its Specification, but have demonstrated that they meet generally accepted security and Certification Authority requirements. In addition, the C2PA has outlined varying levels of security requirements attributed to implementations of Generator Products. These requirements and [Assurance Levels](#) are defined at {INSERT LINK TO SECURITY IMPLEMENTATION REQUIREMENTS}

## **15. Privacy, Inclusion, Equitability and Accessibility Requirements**

In accordance with its [Guiding Principles](#), and based on continuous guidance from the Threats and Harms Task Force, the C2PA Governance Framework establishes mechanisms to address potential harms, support equitable participation, and safeguard personal information. This includes:



- Exploring advisory structures to provide guidance on the management of the conformance program to help avert, mitigate or reduce harm;
- Considering measures to reduce financial and procedural barriers for implementations that serve the public interest; and
- Promoting measures to adhere to industry best practices, regulatory standards, and C2PA guidelines for protecting Personally Identifiable Information (PII) as part of the conformance process.

This informs the development of detailed policies and processes in future iterations of this framework.

## 16. Legal Agreements

Certification Authority, Generator Product and Validator Product Applicants **MUST** sign legal agreements with the C2PA in order to be placed on its respective trust list as approved participants of the C2PA Conformance Program.