C2PA Certificate Policy

C2PA Technical Working Group Conformance Task Force

Version 0.1, 2025-06-02

Table of Contents

1. Introduction

1.1. Standard Terms

The key words "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 RFC8174) when, and only when, they appear in all capitals, as shown here.

1.2. Glossary

1.2.1. 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.

1.2.2. 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.

1.2.3. Applicant's Representative

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

1.2.4. Assertion

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

1.2.5. Asset

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

1.2.6. 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

1.2.7. 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

1.2.8. 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.

1.2.9. C2PA Claim

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

1.2.10. 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.

1.2.11. 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.

1.2.12. 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

1.2.13. C2PA Content Credentials

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

1.2.14. 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.

1.2.15. 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.

1.2.16. C2PA Manifest

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

1.2.17. 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.

1.2.18. 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).

1.2.19. 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.

1.2.20. Claim Generator

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

1.2.21. 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.

1.2.22. 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.

1.2.23. 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.

1.2.24. Digital Content

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

1.2.25. 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.

1.2.26. 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.

1.2.27. 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.

1.2.28. 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.

1.2.29. 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.

1.2.30. 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.

1.2.31. Hosting Environment

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

1.2.32. 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.

1.2.33. 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.

1.2.34. 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

1.2.35. 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.

1.2.36. 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.

1.2.37. 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.

1.2.38. 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.

1.2.39. 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.

1.2.40. Rich Execution Environment

Refer to NIST definition. Abbreviated as REE.

1.2.41. Root of Trust

Refer to NIST definition. Abbreviated as RoT.

1.2.42. 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

1.2.43. 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.

1.2.44. 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.

1.2.45. 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.

1.2.46. 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.

1.2.47. 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.

1.2.48. Trusted Execution Environment

Refer to NIST definition. Abbreviated as TEE.

1.2.49. Validator

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

1.2.50. 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.

1.3. Overview

This Certificate Policy ("CP") establishes the requirements governing the issuance of C2PA Claim Signing Certificates for use by implementers of the technical specifications developed by the Coalition for Content Provenance and Authenticity.

The policy sets the requirements that SHALL be met by a Certification Authority (CA) in the process of issuing C2PA Claim Signing Certificates to Subscribers that implement Generator Products, and the requirements that SHALL be met by the Subscribers in their use of the certificates. Instances of the Subscribers' Generator Products use the certificates to cryptographically sign a C2PA Claim, to imbue an Asset with C2PA Content Credentials.

C2PA Claim Signing Certificates under this policy SHALL only be issued to instances of Generator Products that have successfully passed the C2PA Conformance Program, as documented through their inclusion in the C2PA Conforming Products List. Digital certificates issued under this CP indicate an Assurance Level that can be used by a Relying Party as part of its trust evaluation of an Asset that contains C2PA Content Credentials.

Certification Authorities that comply with this Certificate Policy and want to issue certificates under the C2PA Conformance Program MUST apply to the C2PA Governing Authority for inclusion on the C2PA Trust List .

- **Title:** C2PA Certificate Policy
- **Identifier:** `1.3.6.1.4.1.62558.1.1`
- **Current Version:** 0.1
- **Date of Approval:** 2025-06-02
- **Organization:** The Coalition for Content Provenance and Authenticity (C2PA)

1.3.1. Revision History

Date	Version	Changes
2025-06-02	0.1	Initial publication.

1.4. Normative References

- BCP 14

- RFC 2119
- RFC 8174
- RFC 5280
- RFC 3161

1.5. Certificate Usage

1.5.1. Intended Use

Certificates issued under this CP are to be used exclusively by instances of the Generator Products named as the subjects of the certificates, which have been implemented by the Subscribers, and which are enumerated on the C2PA Conforming Products List, to digitally sign C2PA claims at the Assurance Level indicated by the certificate.

1.5.2. Prohibited Use

Any use of certificates issued under this policy outside of the C2PA Content Credentials Specification or the C2PA Conformance Program is strictly prohibited.

1.6. Policy Administration

This CP is administered by the Administering Authority on behalf of the Governing Authority.

1.6.1. Contact Information

trust-list-admin@c2pa.org

1.6.2. CP Approval Procedures

The Governing Authority approves the CP and any amendments. Amendments are made either by updating the entire CP or by publishing an addendum. The Governing Authority determines whether an amendment to this CP requires notice or an OID change.

1.7. Definitions and Acronyms

- **CA:** Certification Authority
- **CN:** Common Name
- **CP:** Certificate Policy
- **CPS:** Certificate Practice Statement
- **CSR:** Certificate Signing Request
- **DN:** Distinguished Name
- **HSM:** Hardware Security Module
- **O:** Organization (in the Distinguished Name field of a certificate)
- **OID:** Object Identifier
- **OU:** Organizational unit (in the Distinguished Name field of a certificate)
- **PKI:** Public Key Infrastructure

- **RA:** Registration Authority
- **TEE:** Trusted Execution Environment

2. Publication and Repository Responsibilities

This section outlines the mechanisms for disseminating the Certificate Policy and the practices for maintaining a repository of issued certificates.

2.1. Publication

This CP and the C2PA Trust List containing CAs that issue certificates under this CP SHALL be made publicly available on the C2PA website (https://c2pa.org), ensuring transparency and accessibility for all interested parties.

There is no stipulation for the public disclosure of CPSs by CAs that issue certificates under this CP.

2.2. Repositories

A CA issuing certificates under this CP SHALL establish and maintain a secure repository containing records of all certificates issued under this CP. A record for an issued certificate SHALL be stored for at least 1 year after its expiry date. Records in this repository SHALL include essential details such as certificate serial numbers, subject names, validity periods, X.509v3 extensions and their values, and revocation status. The repository SHALL be subject to stringent access controls and regular audits to ensure its integrity and confidentiality.

3. Identification and Authentication

3.1. Naming

3.1.1. Types of Names

A CA issuing certificates under this CP SHALL use X.501 Distinguished Names (`DN`).

3.1.2. The Use of Meaningful Names

The subject of the certificate SHALL be the specific Generator Product, created by the Subscriber, that is issued a certificate for signing C2PA Claims, and it SHALL be identified in the `DN` field of the certificate as follows:

1. The value of `DN` field SHALL match the corresponding record for the Generator Product as listed on the C2PA Conforming Products List.
2. All values of the `DN` SHALL be in plain ASCII text

3.1.3. Anonymity

CAs issuing certificates under this CP SHALL NOT issue anonymous or pseudonymous certificates. However, issued certificates SHALL NOT uniquely identify the instance of the Generator Product to which they are issued. For example, an issued certificate SHALL NOT carry the unique serial number of a particular device to which it is issued.

3.1.4. Uniqueness of Names

The names of Subscribers shall be unique within a subordinate Issuer CA's and Customer's Sub-domain for a specific type of Certificate. Name uniqueness is not violated when multiple certificates are issued to the same entity. For example, A CA MAY issue certificates with the same Subject `DN` under this CP to multiple units of the same device model, or multiple instances of the same application. For example, there can be as many certificates bearing the same `DN` as there are instances of a mobile media editing application running on millions of smartphones at any moment in time.

3.2. Initial Identity Validation

3.2.1. Authenticating the Identity of the Applicant Organization

An Issuer CA must take reasonable measures to verify that the entity submitting the request for a Certificate to be used to sign C2PA conformant claims, controls the application associated with the name referenced in the Certificate, or was authorized by the application owner to act on their behalf. Issuer CAs and RAs shall check the accuracy of information sources and databases to ensure the data is considered accurate, including reviewing the database provider's terms of use. Prior to using any data source as a Reliable Data Source, Issuer CAs and RAs must evaluate the source for its reliability, accuracy, and resistance to alteration or falsification.

The CA SHALL verify the identity of the Applicant, and the authenticity of the Applicant's Representative's application for certificates using a verification process meeting the following requirements:

1. The CA SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:
    a. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
    b. A third party database that is periodically updated and considered a Reliable Data Source such as a Legal Entity Identifier (LEI) data reference;
    c. A site visit by the CA or a third party who is acting as an agent for the CA; or
    d. An Attestation by an independent accountant, lawyer, government official, or other reliable third party in the Applicant's jurisdiction that includes a copy of supporting documentation used to establish the Applicant's legal existence (such as a certificate of registration, articles of incorporation, operating agreement, statute, or regulatory act) and its current status.
2. The CA MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.
3. In cases A and D above, the CA SHALL verify that the status of the Applicant is not designated by labels such as "ceased," "inactive," "invalid," "not current," or the equivalent.
4. If the `O` field in the `DN` is to include a Doing Business As (DBA) or tradename:
    a. The CA SHALL verify the Applicant's right to use the DBA/tradename using at least one of the following:
    b. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
    c. A Reliable Data Source;
    d. Communication with a government agency responsible for the management of such DBAs or

trade names;

e. An Attestation Letter accompanied by documentary support; or

f. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

g. If an Attestation is used as evidence for the validation of the attributes described in this section, then the CA SHALL verify that the letter was written by an accountant, lawyer, government official, or other reliable third party in the Applicant's jurisdiction customarily relied upon for such information. An Attestation SHALL include a copy of documentation supporting the fact to be attested. The CA SHALL use a Reliable Method of Communication to contact the sender and to confirm the Attestation is authentic.

5. An Applicant may request that the CA or RA follow the procedure in section 3.2.17 of the Minimum Security Requirements for Issuance of Mark Certificates to verify that they have the rights to a registered mark which is eligible for use as a logotype (as defined in RFC 3709 and RFC 9399) in the issued certificate.

6. The CA or RA SHALL use a Reliable Method of Communication to verify the authority and approval of an Applicant's Representative to perform one or more of the following:

   a. To request issuance or revocation of certificates; or

   b. assign responsibilities to others to act in these roles

7. Provided that the CA or RA uses a Reliable Method of Communication, the CA or RA MAY establish the authenticity of the application for certificates directly with the Applicant's Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA or RA deems appropriate.

3.2.2. Authenticating the Identity of the Applicant's Representative

The CA SHALL confirm that the Applicant's Representative is a natural person who is:

1. Authorized to act on behalf of the Applicant, including being authorized to submit applications for digital certificates for the Applicant's Generator Product;
2. Authorized to bind the Applicant to the terms and conditions of the Subscriber Agreement

3.2.3. Proof of Conformance

Existence on the C2PA Conforming Products List

The CA SHALL verify the following about the Applicant's Generator Product:

1. The Generator Product for which the Applicant is requesting certificates, as identified by its `DN`, exists on the C2PA Conforming Products List, and has a status of `conformant`.

The CA SHALL obtain the maximum Level of Assurance designation for certificates that the Applicant's Generator Product is eligible for, based on the value of the `maxAssuranceLevel` field for the corresponding entry for the Generator Product on the C2PA Conforming Products List. The CA SHALL NOT issue certificates to an Applicant indicating an assurance level that is higher than this field value. It SHALL issue certificates to Applicants at a level that is at or below the `maxAssuranceLevel`.

Maximum Assurance Level

The CA SHALL obtain the maximum Level of Assurance designation for certificates that the Applicant's Generator Product is eligible for, based on the value of the `maxAssuranceLevel` field for the corresponding entry for the Generator Product on the C2PA Conforming Products List. The CA SHALL NOT issue certificates to an Applicant indicating an assurance level that is higher than this field value. It SHALL issue certificates to Applicants at all levels at or below the `maxAssuranceLevel`.

3.3. Identification and Authentication for Certificate Issuance and Certificate Renewal

The CA SHALL require the use of secure access credentials (for example, usernames and passwords, client certificates, or bearer tokens) for certificate enrollment.

The CA SHALL verify the Subscriber's ownership of the key pair for which certificate issuance is requested, for example by verifying a signed Certificate Signing Request (CSR) provided by the Subscriber, or by inspecting relevant configuration in a key management system.

3.4. On-Going Subscriber Identification and Authentication

The CA SHALL re-authenticate the identity of the Subscriber after no more than 398 days since the last authentication, using the procedure described under Initial Identity Validation.

3.5. Identification and Authentication for Re-key Requests

Re-keying is not allowed under this CP.

3.6. Identification and Authentication for Revocation Requests

Revocation requests MAY be initiated by the Subscriber, the CA or the C2PA. If Subscriber requested, the CA SHALL verify the authenticity of the revocation request and revoke the certificate within 72 hours.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

The Applicant initiates the certificate request process by submitting a formal application to become a Subscriber using the method designated by the CA. The Applicant SHALL provide all requisite information and documentation as specified in this CP. This includes:

1. Information about the Generator Product for which the certificate is requested, including its record number on the C2PA Conforming Products List

2. The Assurance Level of the certificates which the Applicant will be requesting for their Generator Product, which SHALL NOT exceed the maximum Assurance Level recorded for said product on the C2PA Conforming Products List
3. If required by the Assurance Level indicated for the Applicant's Generator Product on the C2PA Conforming Products List, evidence of the ability to produce verifiable artifacts using one of the `attestationMethods` on the Generator Product record on the C2PA Conforming Products List.

4.2. Certificate Application Processing

1. Upon receiving the application, the CA SHALL review the submitted information and documentation for completeness and accuracy.
2. The CA SHALL perform the necessary identity validation procedures as outlined in Identification and Authentication
3. If required by the Assurance Level indicated for the Applicant's product on the C2PA Conforming Products List, the CA SHALL confirm the Applicant's ability to obtain platform attestation reports in a format that the CA is able to decode and process.

4.3. CA Access Credentials

Upon successful completion of the application process, the CA SHALL associate new or existing secure access credentials (for example, usernames and passwords, client certificates, or bearer tokens) with the newly-approved Subscriber, for use in authenticating Subscriber requests for certificate enrollment.

4.4. Certificate Issuance

1. All certificate signing operations performed by a Root CA SHALL be performed by at least two individuals in trusted roles (i.e. the CA system operator, system officer, or PKI administrator). One of these individuals must deliberately command the Root CA to perform a certificate signing operation.
2. Certificate issuance SHALL be subject to the process outlined in Identification and Authentication for Certificate Issuance and Certificate Renewal.
3. If required by the Max Assurance Level indicated for the Subscriber's product on the C2PA Conforming Products List, the CA SHALL request and verify the Dynamic Evidence required for said Assurance Level.
    a. Dynamic Evidence may include key attestation reports, application attestation reports, platform attestation reports, or other verifiable artifacts backed by a hardware root-of-trust.
    b. When validating key and platform attestation reports, the CA SHALL follow the requirements defined in Requirements for Validating Dynamic Evidence.
4. Upon successful verification of the above evidence, the CA MAY issue a C2PA Claim Signing Certificate that complies with the attributes defined in the Certificate Profile section of this CP to the Subscriber's specific device or instance of an application.
5. If the Dynamic Evidence presented by the instance of the Generator Product does not meet the requirements for the requested Assurance Level, the CA MAY evaluate the evidence against the requirements of the next-lower Assurance Level, if applicable.

4.5. Certificate Acceptance

1. Certificate acceptance by the Subscriber SHALL indicate the Subscriber's acceptance of the terms of a Subscriber Agreement that includes required stipulations of this CP.
2. The acceptance SHALL be implicit through successful installation and use of the certificate by an instance of the Generator Product.
3. Certificates issued under this CP are to be used exclusively by the C2PA Conforming Product named as subjects of the certificates, which have been implemented by the named Subscribers, and which are enumerated on the C2PA Conforming Products List, to digitally sign C2PA claims at the Assurance Level indicated by the certificate. Any usage for any other purpose is strictly prohibited.

4.6. Key Pair and Certificate Usage

1. Private keys corresponding to Root certificates SHALL NOT be used to sign certificates except in the following cases:
    a. Self-signed certificates to represent the Root CA itself;
    b. Certificates for Subordinate CAs and Cross-Certified CA certificates;
    c. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and
    d. Certificates for OCSP Response verification.
2. The use of a specific key is determined by the key usage extension in the X.509 certificate.
3. The private key associated with the public key to which a certificate has been issued under this CP SHALL remain under the exclusive control of the instance of the Generator Product and SHALL NOT be exported or shared with other devices, instances of applications, or parties except as allowed by the Generator Product Security Requirements.
4. Certificates issued under this CP are to be used exclusively by the Generator Product named as subjects of the certificates, which have been implemented by the named Subscribers, and which are enumerated on the C2PA Conforming Products List, to digitally sign C2PA claims at the Assurance Level indicated by the certificate. Any usage for any other purpose is strictly prohibited.

4.7. Certificate Renewal

1. For certificate renewal, the Subscriber SHALL generate a new key pair and initiate the certificate enrollment process to obtain a certificate for the newly-generated public key.
2. A CA SHALL NOT issue a new certificate for a key pair for which it had previously issued a certificate.
3. The renewal SHALL be subject to the process outlined in Identification and Authentication for Certificate Issuance and Certificate Renewal.

4.8. Certificate Re-key

1. Re-keying SHALL NOT be permitted by CAs operating in conformance with this CP.
2. If a new key pair is required, the Subscriber SHALL follow the process outlined in Certificate Renewal.

4.9. Certificate Modification

1. Certificate modifications SHALL NOT be permitted by CAs operating in conformance with this CP.
2. If changes to the subject information are necessary, the CA and the Subscriber SHALL follow the process outlined in Initial Identity Validation.

4.10. Certificate Revocation

The CA SHALL revoke a certificate under any of the following circumstances:

1. A change of status for the Generator Product on the C2PA Conforming Products List to any status that begins with `revoked`
2. A request by the C2PA Governing Authority
3. Subscriber request
4. Suspected or confirmed compromise of the Generator Product or attestation failure (for applicable assurance levels)
5. C2PA request or a change of status for the Generator Product on the C2PA Conforming Products List to any status that begins with `revoked`
6. Confirmed exposure of the private key
7. Non-compliance with this CP
8. Certificate misuse

4.11. Certificate Status Services

The CA SHALL provide Online Certificate Status Protocol (OCSP) responses to indicate the revocation status of certificates up to the required record keeping time stipulated in Publication and Repository Responsibilities.

This CP makes no stipulation about the use of certificate revocation lists (CRL).

4.12. End of Subscription

Upon termination of the subscription or cessation of relevant activities, the Subscriber SHALL follow industry best practices for destroying the private key(s).

4.13. Key Escrow and Recovery

1. Key escrow and recovery are NOT supported under this CP.
2. The Subscriber Agreement SHALL state that the Subscriber is solely responsible for the protection and management of their private keys.

5. Facility, Management, and Operational Controls

This section details the physical, procedural, and personnel controls necessary to safeguard the CA's operations and maintain the integrity of the PKI system, particularly as it relates to the issuance and

management of certificates. While physical security remains important, the emphasis here is on logical and procedural controls, reflecting the nature of the environment where these certificates will be used.

5.1. Physical Security Controls

5.1.1. Site Security

1. The CA's facilities housing critical PKI infrastructure and sensitive data SHALL be located in a secure environment with controlled access. This MAY be a dedicated facility or a secure area within a larger building.
2. Physical security measures, such as locks, access control systems, and visitor management procedures, should be implemented to prevent unauthorized physical access.

5.1.2. Restricted Areas

1. Areas containing sensitive systems or data, such as server rooms or data centers, should have restricted access, limited to authorized personnel only.
2. Multi-factor authentication mechanisms SHALL be deployed for accessing these restricted areas.

5.1.3. Equipment Security

Critical equipment, including servers, network devices, and any hardware security modules (HSMs) , SHALL be physically secured to prevent unauthorized access, tampering, or theft.

5.2. Procedural Controls

5.2.1. Documented Procedures

Comprehensive and up-to-date documentation SHALL be maintained for all CA operational procedures, including:

1. Certificate issuance, renewal, and revocation processes.
2. Key generation and management practices within devices or applications.
3. Attestation validation procedures when required by a particular Assurance Level.
4. Incident response and disaster recovery plans.
5. Security policies, guidelines, and access control measures.

5.2.2. Separation of Duties

1. Critical functions, such as attestation validation, certificate issuance, and revocation, SHALL be segregated among different individuals or teams to prevent conflicts of interest and minimize the risk of fraud or error.
2. Dual control mechanisms SHALL be deployed for physical access to CA equipment and any access required to perform specific CA operations (i.e., m of n rule where m represents the number of key shareholders required to perform an operation and n represents the total number of key shares).

5.2.3. Change Management

1. A formal change management process SHALL be established to control and document all changes to the CA's infrastructure, software, or procedures.
2. All changes SHALL undergo thorough testing and approval before implementation.
3. Rollback and/or roll-forward plans SHALL be in place to revert changes in the event of unforeseen issues.

5.3. Personnel Controls

5.3.1. Clearances

The CA's policies and procedures SHALL specify the background checks and clearance procedures required for Trusted Roles and non-trusted roles. As a minimum, verification checks on permanent staff SHALL be performed at the time of job application and every five years for those individuals undertaking Trusted Roles.

5.3.2. Training and Awareness

1. All personnel involved in CA operations SHALL undergo regular security awareness training, including PKI concepts, data protection, incident response, attestation validation (if applicable), and their specific roles and responsibilities.
2. Periodic retraining SHALL occur to verify the continued trustworthiness of personnel involved in the activities related to key management and certificate management. This training SHALL be performed if there is a material change in PKI operation.

5.3.3. Access Control

1. Access to CA systems and data SHALL be granted on a need-to-know basis, adhering to the principle of least privilege.
2. Strong password policies, multi-factor authentication, and regular access reviews SHALL be implemented.

5.4. Audit Logging Procedures

5.4.1. Comprehensive Logging

1. Detailed audit logs SHALL be maintained for all system and user activities related to certificate operations, including issuance, revocation, attestation validation (if applicable), and access attempts.
2. Logs SHALL include identities of the Subscribers and CA systems and personnel requesting operations, timestamps, actions taken, and relevant data or parameters.

5.4.2. Log Protection and Integrity

1. Audit logs SHALL be securely stored and protected against unauthorized access, modification, or deletion.
2. Cryptographic mechanisms or write-once media can be employed to ensure log integrity.

5.4.3. Log Review and Analysis

1. Regular reviews of audit logs SHALL be conducted to identify any suspicious or unauthorized activity.
2. Automated log analysis tools MAY be utilized to detect anomalies or patterns indicative of potential security breaches.

5.5. Records Archival

5.5.1. Archival Policy

1. The CA SHALL have a well-defined records archival policy, stipulating the types of records to be archived, their retention periods, and secure storage and retrieval mechanisms.
2. Archival practices SHALL adhere to relevant legal and regulatory requirements.

5.5.2. Secure Storage

Archived records SHALL be stored in a secure location or utilizing secure cloud-based solutions, protecting them from unauthorized access, damage, or destruction.

5.5.3. Access and Retrieval

1. Access to archived records should be restricted to authorized personnel only.
2. Documented retrieval procedures SHALL ensure the timely and accurate recovery of archived information when needed.

5.6. Key Changeover

5.6.1. Key Changeover Process

1. A secure and documented process SHALL be in place for the periodic rotation of CA keys.
2. The changeover process should minimize disruption to Subscribers and maintain the chain of trust.
3. CAs SHOULD encourage Subscribers to retain key rotation agility.

5.6.2. Subscriber Notification

Subscribers SHOULD be notified in advance of any planned key changeover events, allowing them sufficient time to update their systems and configurations.

5.7. Compromise and Disaster Recovery

5.7.1. Incident Response Plan

1. A comprehensive incident response plan SHALL outline procedures for handling security breaches, key compromises, natural disasters, or any other events that MAY disrupt CA operations.
2. The plan should define roles and responsibilities, communication protocols, and escalation

procedures.

3. Regular drills and exercises should test the plan's effectiveness.

5.7.2. Backup and Recovery

1. Secure backups of all critical data, including certificate databases, key material, configuration files, and audit logs, SHALL be maintained.
2. Backups should be stored off-site and regularly tested to ensure recoverability.
3. A documented recovery plan outlining the steps to restore operations after a disaster or system failure SHALL be in place.

5.8. CA or RA Termination

5.8.1. Termination Procedures

1. Procedures SHALL be established for the orderly termination of the CA's operations or the revocation of an RA's delegation.
2. These procedures should address the secure handling and disposal of sensitive data, keys, and equipment.
3. Subscribers SHALL receive advance notification, allowing them ample time to transition to alternative CAs or RAs.

6. Technical Security Controls

This section details the technical measures and safeguards implemented to protect the cryptographic keys and ensure the security of the Subscriber Generator Product and the CA's infrastructure.

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation and Installation by CAs

1. The Certification Authority SHALL maintain effective controls to provide reasonable assurance that the integrity of keys and certificates it manages is established and protected throughout their life cycles.
2. The CA SHALL maintain controls to provide reasonable assurance that CA key pairs are generated in accordance with the CA's disclosed business practices and defined procedures specified within detailed key generation ceremony scripts.
3. The CA's disclosed business practices SHALL include but are not limited to:
    a. generation of CA keys are undertaken in a physically or cloud secured environment;
    b. generation of CA keys are performed by personnel in trusted roles under the principles of multiple person control and split knowledge;
    c. generation of CA keys occur within FIPS 140-2 Level 2 or higher cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's CPS;
    d. generation of CA keys are witnessed by an independent party and/or recorded; and
    e. CA key generation activities are logged.

4. The CA key generation script includes the following:
    a. definition of roles and participant responsibilities;
    b. approval for conduct of the key generation ceremony;
    c. cryptographic hardware (or Cloud-Based HSM) and activation materials required for the ceremony;
    d. specific steps performed during the key generation ceremony;
    e. physical security requirements for the ceremony location (If not using Cloud-Based HSM);
    f. procedures for secure storage of cryptographic hardware and activation materials following the key generation ceremony (If not using Cloud-Based HSM)
    g. sign-off from participants and witnesses indicating whether key generation ceremony was performed in accordance with the detailed key generation ceremony script; and
    h. notation of any deviations from the key generation ceremony script.

6.1.2. Key Pair Generation and Installation by Subscribers

1. Claim signing key pairs SHALL be generated by the Subscribers or by key management systems on behalf of Subscribers. The CA SHALL NOT generate claim signing key pairs.
2. Requirements for key pair generation by Subscribers are defined in the C2PA Conformance Program's Implementation Security Requirements document, and MAY vary by the Assurance Level of the implementation.
3. The CA SHALL issue certificates only for claim signing keys that meet the applicable requirements in the C2PA Content Credentials specification and the Certificate Profile section of this CP.
4. Regardless of the Assurance Level, Subscribers SHALL only use the keys that have been issued certificates under this CP for signing C2PA claims generated by the devices or applications that are the subject of the certificates.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Controls for CA Keys

Key Storage

1. The CA's private keys for the root and issuing CAs SHALL be stored and used within a secure cryptographic device meeting FIPS 140-2 Level 2 or higher, housed within a 3-tier data center or an HSM housed in a commercial cloud provider environment.
2. The CA private key SHALL NOT exist in plaintext outside the cryptographic module boundary.

Key Usage and Access Control

1. CAs SHALL use multi-party controls to ensure that no single individual has uniliteral physical or logical access to root or intermediate CA signing keys.
2. The usage of the root and intermediate CA private keys SHALL occur directly on the cryptographic module (e.g. a physical or a cloud-hosted HSM).

Key Backup and Recovery

1. CAs SHALL document a formal plan for key backup and recovery that is reviewed annually
2. All backups of the CA private keys SHALL be accounted for and protected under the same multi-person control as the original key.
3. At least one copy of the CA private key SHALL be stored off-site. For all other keys, backup, when permitted, SHALL provide security controls consistent with the protection provided by the original cryptographic module
4. Backed up private keys SHALL NOT be exported or stored in plaintext form outside the cryptographic module.

Key Archival

CA private keys SHALL NOT be archived.

Key Destruction

No stipulation.

6.2.2. Controls for Subscriber Keys

Control requirements for Subscriber keys are defined in the C2PA Conformance Program's Generator Product Security Requirements document, and MAY vary by the Assurance Level of the implementation.

6.3. Activation Data

Activation data is NOT applicable under this policy.

6.4. Computer Security Controls

1. The Subscriber's Generator Product SHALL adhere to platform-specific security guidelines and best practices to protect against unauthorized access, malware, and other cyber threats.
2. Security measures such as secure coding practices, code signing, and regular security updates SHALL be employed.
3. Access to sensitive data or functionalities within the Generator Product SHALL be restricted and protected by appropriate authentication and authorization mechanisms.

6.5. Lifecycle Security Controls

1. Throughout the certificate lifecycle, from issuance to revocation, security controls SHALL be in place to ensure the confidentiality, integrity, and availability of certificates and associated data.
2. Certificate issuance and revocation processes SHALL be protected against unauthorized actions and tampering.
3. Certificate status information SHALL be readily available and accessible to relying parties through mechanisms such as OCSP or CRLs.

6.6. Network Security Controls

1. The instance of the Generator Product SHALL employ secure communication protocols and practices when interacting with the CA or RA during certificate operations.
2. Network traffic SHALL be protected against eavesdropping, tampering, and unauthorized access.
3. Remote access to CA systems, made by CA employees or external systems, if permitted, SHALL require authentication.
4. Connections made by CA employees or CA systems to remote computer systems SHALL be authenticated.
5. Access to diagnostic ports SHALL be is securely controlled.
6. Controls (e.g., firewalls) SHALL be in place to protect the CA's internal network domain from any unauthorized access from any other domain.
7. Controls SHALL be in place to limit the network services (e.g., HTTP, FTP, etc.) available to authorized users in accordance with the CA's access control policies.
8. The security attributes of all network services used by the CA organization SHALL be documented by the CA.
9. Routing controls SHALL be in place to ensure that computer connections and information flows do not breach the CA's access control policy.
10. The CA SHALL maintain local network components (e.g., firewalls and routers) in a physically secure environment and audit their configurations periodically for compliance with the CA's configuration requirements.
11. Sensitive data SHALL be encrypted when exchanged over public or untrusted networks.

6.7. Time-Stamping Authorities

Organizations that operate CAs that issue certificates in accordance with this CP MAY also provide an RFC 3161-compliant Time-Stamping Authority (TSA), and the organization MAY apply to the Conformance Program for inclusion on the C2PA TSA Trust List. The TSA MAY operate several identifiable Time-Stamp Units (TSU).

Two forms of Time-Stamping Authorities are permitted under this CP:

- Backend TSA, operated as a service by the CA.
- On-Device TSA, intended for use on mobile/edge devices to support local time-stamping without requiring a network connection.

6.7.1. General TSA Requirements

1. The CA SHALL disclose its TSA practices including the hashing algorithms, the expected life time of the time-stamp signature, subscriber and relying party obligations (if any), any limitations on the use of the time-stamp and information on how to verify the time-stamp, the intended time-accuracy, and logging of TSA events including how long logs are maintained (and hence are available to provide supporting evidence).
2. The time values the TSU uses in the time-stamp shall be traceable to at least one of the real time values distributed by a UTC(k) laboratory.
3. The intended accuracy SHALL be defined in the time-stamp, and the time included in the time-stamp SHALL be synchronized with this accuracy. The declared accuracy SHOULD be of 1 second

or better. TSA clock synchronization SHALL be maintained when a leap second occurs as notified by the appropriate body.

4. The TSA SHALL detect if the time that would be applied in a time-stamp drifts outside the declared accuracy. In this situation, the TSU SHALL stop time-stamp issuance.
5. The time-stamp SHALL be signed using Private Keys that are reserved exclusively for this purpose. A TSU SHALL have a single time-stamp signing key active at a time.
6. The TSA SHALL only accept time-stamp requests that use SHA2-256, SHA2-384, and SHA2-512 hashing algorithms, per the normative requirements of the C2PA Content Credentials specification.

6.7.2. Backend TSA

1. TSU signing keys SHALL be generated and stored within a secure cryptographic device which is a trustworthy system that has been assured to EAL 4 or higher in accordance with ISO/IEC 15408, or equivalent internationally recognized evaluation criteria for IT security, or as meeting at least FIPS 140-2 level 3, FIPS 140-3 level 3, or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats.

6.7.3. On-Device TSA

1. The On-Device TSA SHALL attempt to synchronize its time at least once every 24 hours with an online time source whose time values are traceable to at least one of the real time values distributed by a UTC(k) laboratory. The trusted online time source MAY be a Backend TSA on the C2PA TSA Trust List. In such a case, the On-Device TSA SHALL adhere to the following procedure:
2. The On-Device TSA application SHALL run in a Trusted Execution Environment
3. TSU signing keys SHALL be generated and stored within a Trusted Execution Environment.

7. Certificate, CRL, and OCSP Profiles

This section outlines the technical specifications and formats for the certificates, Certificate Revocation Lists (CRLs), and Online Certificate Status Protocol (OCSP) responses associated with this CP. It also defines the X.509 v3 extension to indicate the assurance level of each certificate.

7.1. Certificate Profiles

7.1.1. Certificate Profiles for Certification Authorities

Root

```
# Summary of Certificate Profile Constraints for a self-signed C2PA Root CA
certificate

Profile: C2PA Root CA

Core Fields:
  Version: v3
```

```
  Serial Number: Positive integer (high entropy recommended) up to 20 octets
  Signature Algorithm: RSA (PSS or SHA2 variants) or ECDSA (SHA2 variants)
  Issuer Name: Matches Subject Name (Self-Signed). Requires C, O, CN attributes.
  Validity Period: Long-term (e.g., 20 years typical). Specific dates set at
generation.
  Subject Name: Unique name for the Root CA. Requires C, O, CN attributes. Matches
Issuer Name.
  Subject Public Key Info:
    Algorithm: rsaEncryption or id-ecPublicKey
    RSA Key Size: 3072 bits or larger
    ECC Curve: P-384 or P-521

Extensions:
  Subject Key Identifier:
    Presence: MUST
    Critical: FALSE
    Value: Hash of public key (RFC 5280 Method 1 - SHA-1)
  Authority Key Identifier:
    Presence: MUST
    Critical: FALSE
    Value: Must contain keyIdentifier matching Subject Key Identifier (using RFC 5280
Method 1 - SHA-1). Issuer/Serial optional.
  Key Usage:
    Presence: MUST
    Critical: TRUE
    Bits: keyCertSign, cRLSign
  Basic Constraints:
    Presence: MUST
    Critical: TRUE
    Value: cA=TRUE, pathLenConstraint=2 or less
  Certificate Policies:
    Presence: OPTIONAL
    Critical: FALSE
  Authority Information Access:
    Presence: MUST NOT
  CRL Distribution Points:
    Presence: MUST NOT
```

Claim Signing Issuing CA

```
# Summary of Certificate Profile Constraints for the last intermediate CA which issues
C2PA Claim Signing leaf certificates

Profile: C2PA Claim Signing Issuing CA

Core Fields:
  Version: v3
  Serial Number: Positive integer (high entropy recommended) up to 20 octets
  Signature Algorithm: RSA (PSS or SHA2 variants) or ECDSA (SHA2 variants)
  Issuer Name: Matches Subject Name of signing issuing CA (either Root CA or another
```

```
subordinate).
  Validity Period: Max 1827 days.
  Subject Name: Unique name for the Issuing CA. Requires C, O, CN attributes.
  Subject Public Key Info:
    Algorithm: rsaEncryption or id-ecPublicKey
    RSA Key Size: 3072 bits or larger
    ECC Curve: P-384 or P-521

Extensions:
  Subject Key Identifier:
    Presence: MUST
    Critical: FALSE
    Value: Hash of public key (RFC 5280 Method 1 - SHA-1)
  Authority Key Identifier:
    Presence: MUST
    Critical: FALSE
    Value: Must contain keyIdentifier (matching the SKI of the CA that issued this
cert (root or intermediate), using RFC 5280 Method 1). Issuer/Serial optional.
  Key Usage:
    Presence: MUST
    Critical: TRUE
    Bits: keyCertSign, cRLSign
  Basic Constraints:
    Presence: MUST
    Critical: TRUE
    Value: cA=TRUE, pathLenConstraint=0
  Extended Key Usage:
    Presence: MUST
    Critical: FALSE
    Value: Must contain c2pa-kp-claimSigning in addition to at least one of id-kp-
emailProtection, id-kp-documentSigning
  Certificate Policies:
    Presence: MUST
    Critical: FALSE
    Value: Must contain c2pa-certificate-policy OID (1.3.6.1.4.1.62558.1.1).
Qualifiers optional.
  Authority Information Access:
    Presence: MUST (if CRL Distribution Points is not present)
    Critical: FALSE
    Value: Sequence of AccessDescription. Must include one with accessMethod=id-ad-
ocsp. Should include one with accessMethod=id-ad-caIssuers. accessLocation must be
HTTP URI.
  CRL Distribution Points:
    Presence: MUST (if Authority Information Access with id-ad-ocsp is not present)
    Critical: FALSE
    Value: Must contain HTTP URI pointing to CRL location.
```

TSA Issuing CA

```
# Summary of Certificate Profile for the last intermediate CA which issues TSA time-
```

```
stamp signing leaf certificates

Profile: C2PA TSA Issuing CA

Core Fields:
  Version: v3
  Serial Number: Positive integer (high entropy recommended) up to 20 octets
  Signature Algorithm: RSA (PSS or SHA2 variants) or ECDSA (SHA2 variants)
  Issuer Name: Matches Subject Name of signing Root CA.
  Validity Period: Max 5479 days
  Subject Name: Unique name for the TSA Issuing CA. Requires C, O, CN attributes.
  Subject Public Key Info:
    Algorithm: rsaEncryption or id-ecPublicKey
    RSA Key Size: 3072 bits or larger
    ECC Curve: P-384 or P-521

Extensions:
  Subject Key Identifier:
    Presence: MUST
    Critical: FALSE
    Value: Hash of public key (RFC 5280 Method 1 - SHA-1)
  Authority Key Identifier:
    Presence: MUST
    Critical: FALSE
    Value: Must contain keyIdentifier (matching the SKI of the CA that issued this
cert (root or intermediate), using RFC 5280 Method 1). Issuer/Serial optional.
  Key Usage:
    Presence: MUST
    Critical: TRUE
    Bits: keyCertSign, cRLSign
  Basic Constraints:
    Presence: MUST
    Critical: TRUE
    Value: cA=TRUE, pathLenConstraint=0
  Extended Key Usage:
    Presence: MUST
    Critical: FALSE
    Value: Must contain exactly id-kp-timeStamping.
  Certificate Policies:
    Presence: MUST
    Critical: FALSE
    Value: Must contain c2pa-certificate-policy OID (1.3.6.1.4.1.62558.1.1).
Qualifiers optional.
  Authority Information Access:
    Presence: MUST (if CRL Distribution Points is not present)
    Critical: FALSE
    Value: Sequence of AccessDescription. Must include one with accessMethod=id-ad-
ocsp. Should include one with accessMethod=id-ad-caIssuers. accessLocation must be
HTTP URI.
  CRL Distribution Points:
    Presence: MUST (if Authority Information Access with id-ad-ocsp is not present)
```

```
    Critical: FALSE
    Value: Must contain HTTP URI pointing to CRL location.
```

7.1.2. Certificate Profiles for Leaf Certificates

OCSP Responder Leaf Certificates

```
# Summary of C2PA OCSP Responder Certificate Profile Constraints (leaf certificate)

Profile: C2PA OCSP Responder

Core Fields:
  Version: v3
  Serial Number: Positive integer (high entropy recommended) up to 20 octets
  Signature Algorithm: RSA (PSS or SHA2 variants) or ECDSA (SHA2 variants) - EdDSA
excluded.
  Issuer Name: Matches Subject Name of signing Issuing CA.
  Validity Period: Specific dates set at generation (Max duration not specified by
C2PA profile).
  Subject Name: Unique name for the OCSP Responder. Requires C, O, CN attributes.
  Subject Public Key Info:
    Algorithm: rsaEncryption or id-ecPublicKey
    RSA Key Size: 2048 bits or larger
    ECC Curve: P-256, P-384, or P-521

Extensions:
  Subject Key Identifier:
    Presence: MUST
    Critical: FALSE
    Value: Hash of public key (RFC 5280 Method 1 - SHA-1)
  Authority Key Identifier:
    Presence: MUST
    Critical: FALSE
    Value: Must contain keyIdentifier (matching Issuing CA SKI, using RFC 5280 Method
1). Issuer/Serial optional.
  Key Usage:
    Presence: MUST
    Critical: TRUE
    Bits: digitalSignature
  Basic Constraints:
    Presence: MUST
    Critical: TRUE
    Value: cA=FALSE
  Extended Key Usage:
    Presence: MUST
    Critical: FALSE
    Value: Must contain exactly id-kp-OCSPSigning.
  OCSP NoCheck:
    Presence: MUST
    Critical: FALSE
```

```
    Value: NULL
  Authority Information Access:
    Presence: MUST NOT
  CRL Distribution Points:
    Presence: MUST NOT
```

C2PA Claim Signing Leaf Certificates - Assurance Level 1

```
# Summary of C2PA Claim Signing Leaf Certificate Profile Constraints for Assurance
Level 1

Profile: C2PA Claim Signing Leaf - Assurance Level 1

Core Fields:
  Version: v3
  Serial Number: Positive integer (high entropy recommended) up to 20 octets
  Signature Algorithm: RSA (PSS or SHA2 variants), ECDSA (SHA2 variants), or Ed25519
  Issuer Name: Matches Subject Name of signing Claim Signing Issuing CA.
  Validity Period: Max 366 days (Assurance Level 1)
  Subject Name: Must match C2PA Conforming Products List (CPL) entry. Requires C, O,
CN attributes.
  Subject Public Key Info:
    Algorithm: rsaEncryption, id-ecPublicKey, or id-Ed25519
    RSA Key Size: 2048 bits or larger
    ECC Curve: P-256, P-384, or P-521
    EdDSA Curve: Ed25519 (implied by algorithm)

Extensions:
  Subject Key Identifier:
    Presence: MUST
    Critical: FALSE
    Value: Hash of public key (RFC 5280 Method 1 - SHA-1)
  Authority Key Identifier:
    Presence: MUST
    Critical: FALSE
    Value: Must contain keyIdentifier (matching Issuing CA SKI, using RFC 5280 Method
1). Issuer/Serial optional.
  Key Usage:
    Presence: MUST
    Critical: TRUE
    Bits: digitalSignature, nonRepudiation (contentCommitment)
  Basic Constraints:
    Presence: MUST
    Critical: TRUE
    Value: cA=FALSE
  Extended Key Usage:
    Presence: MUST
    Critical: FALSE
    Value: Must contain c2pa-kp-claimSigning in addition to at least one of id-kp-
emailProtection, id-kp-documentSigning
```

```
  Certificate Policies:
    Presence: MUST
    Critical: FALSE
    Value: Must contain c2pa-certificate-policy OID (1.3.6.1.4.1.62558.1.1).
Qualifiers optional.
  Authority Information Access:
    Presence: MUST
    Critical: FALSE
    Value: Sequence of AccessDescription. Must include one with accessMethod=id-ad-
ocsp. Should include one with accessMethod=id-ad-caIssuers. accessLocation must be
HTTP URI.
  CRL Distribution Points:
    Presence: OPTIONAL
    Critical: FALSE
    Value (if present): Must contain HTTP URI pointing to CRL location.
  C2PA Assurance Level (id-c2pa-al):
    Presence: MUST
    Critical: FALSE
    OID: 1.3.6.1.4.1.62558.3
    Value: 1.3.6.1.4.1.62558.3.10 (c2pa-assuranceLevel-1)
  C2PA CPL Record ID (c2pa-cpl-record):
    Presence: MUST
    Critical: FALSE
    OID: 1.3.6.1.4.1.62558.4
    Value: UTF8String (SIZE 36) containing UUID from CPL.
```

C2PA Claim Signing Leaf Certificates - Assurance Level 2

```
# Summary of C2PA Claim Signing Leaf Certificate Profile Constraints for Assurance
Level 2

Profile: C2PA Claim Signing Leaf

Core Fields:
  Version: v3
  Serial Number: Positive integer (high entropy recommended) up to 20 octets
  Signature Algorithm: RSA (PSS or SHA2 variants), ECDSA (SHA2 variants), or Ed25519
  Issuer Name: Matches Subject Name of signing Claim Signing Issuing CA.
  Validity Period: Max 90 days (Assurance Level 2)
  Subject Name: Must match C2PA Conforming Products List (CPL) entry. Requires C, O,
CN attributes.
  Subject Public Key Info:
    Algorithm: rsaEncryption, id-ecPublicKey, or id-Ed25519
    RSA Key Size: 2048 bits or larger
    ECC Curve: P-256, P-384, or P-521
    EdDSA Curve: Ed25519 (implied by algorithm)

Extensions:
  Subject Key Identifier:
    Presence: MUST
```

```
    Critical: FALSE
    Value: Hash of public key (RFC 5280 Method 1 - SHA-1)
  Authority Key Identifier:
    Presence: MUST
    Critical: FALSE
    Value: Must contain keyIdentifier (matching Issuing CA SKI, using RFC 5280 Method
1). Issuer/Serial optional.
  Key Usage:
    Presence: MUST
    Critical: TRUE
    Bits: digitalSignature, nonRepudiation (contentCommitment)
  Basic Constraints:
    Presence: MUST
    Critical: TRUE
    Value: cA=FALSE
  Extended Key Usage:
    Presence: MUST
    Critical: FALSE
    Value: Must contain c2pa-kp-claimSigning in addition to at least one of id-kp-
emailProtection, id-kp-documentSigning
  Certificate Policies:
    Presence: MUST
    Critical: FALSE
    Value: Must contain c2pa-certificate-policy OID (1.3.6.1.4.1.62558.1.1).
Qualifiers optional.
  Authority Information Access:
    Presence: MUST
    Critical: FALSE
    Value: Sequence of AccessDescription. Must include one with accessMethod=id-ad-
ocsp. Should include one with accessMethod=id-ad-caIssuers. accessLocation must be
HTTP URI.
  CRL Distribution Points:
    Presence: OPTIONAL
    Critical: FALSE
    Value (if present): Must contain HTTP URI pointing to CRL location.
  C2PA Assurance Level (id-c2pa-al):
    Presence: MUST
    Critical: FALSE
    OID: 1.3.6.1.4.1.62558.3
    Value: 1.3.6.1.4.1.62558.3.20 (c2pa-assuranceLevel-2)
  C2PA CPL Record ID (c2pa-cpl-record):
    Presence: MUST
    Critical: FALSE
    OID: 1.3.6.1.4.1.62558.4
    Value: UTF8String (SIZE 36) containing UUID from CPL.
```

TSA Time-Stamp Signing Leaf Certificates

```
# Human-readable summary of C2PA TSA Time-Stamp Signing Leaf Certificate Profile
Constraints
```

```
Profile: C2PA TSA Time-Stamp Signing Leaf

Core Fields:
  Version: v3
  Serial Number: Positive integer (high entropy recommended) up to 20 octets
  Signature Algorithm: RSA (PSS or SHA2 variants) or ECDSA (SHA2 variants) - EdDSA
excluded.
  Issuer Name: Matches Subject Name of signing TSA Issuing CA.
  Validity Period: Max 4110 days
  Subject Name: Unique name for the TSA service. Requires C, O, CN attributes.
  Subject Public Key Info:
    Algorithm: rsaEncryption or id-ecPublicKey
    RSA Key Size: 2048 bits or larger
    ECC Curve: P-256, P-384, or P-521

Extensions:
  Subject Key Identifier:
    Presence: MUST
    Critical: FALSE
    Value: Hash of public key (RFC 5280 Method 1 - SHA-1)
  Authority Key Identifier:
    Presence: MUST
    Critical: FALSE
    Value: Must contain keyIdentifier (matching TSA Issuing CA SKI, using RFC 5280
Method 1). Issuer/Serial optional.
  Key Usage:
    Presence: MUST
    Critical: TRUE
    Bits: digitalSignature, nonRepudiation (contentCommitment)
  Basic Constraints:
    Presence: MUST
    Critical: TRUE
    Value: cA=FALSE
  Extended Key Usage:
    Presence: MUST
    Critical: TRUE
    Value: Must contain exactly id-kp-timeStamping.
  Certificate Policies:
    Presence: MUST
    Critical: FALSE
    Value: Must contain c2pa-certificate-policy OID (1.3.6.1.4.1.62558.1.1).
Qualifiers optional.
  Authority Information Access:
    Presence: MUST (if CRL Distribution Points is not present)
    Critical: FALSE
    Value: Sequence of AccessDescription. Must include one with accessMethod=id-ad-
ocsp. Should include one with accessMethod=id-ad-caIssuers. accessLocation must be
HTTP URI.
  CRL Distribution Points:
    Presence: MUST (if Authority Information Access with id-ad-ocsp is not present)
```

```
    Critical: FALSE
    Value: Must contain HTTP URI pointing to CRL location.
```

7.2. CRL Profile

This CP makes no stipulations about the use of CRLs.

8. Compliance Audit and Other Assessments

This section defines the requirements for compliance audits and assessments to verify adherence to this CP and maintain the integrity of the PKI system, specifically focusing on the processes and controls surrounding the issuance and management of certificates.

8.1. Compliance Audits

1. Regular Audits:
    a. The CA SHOULD undergo regular compliance audits conducted by an independent, qualified third-party auditor.
    b. Audits SHOULD assess the CA's adherence to this CP, relevant industry standards (e.g., WebTrust for CA), and any applicable legal or regulatory requirements.
    c. The audit frequency SHALL depend on the risk profile and assurance level, but at a minimum, annual audits are recommended.
2. Audit Scope:
    a. Audits SHOULD cover all aspects of the CA's operations relevant to this CP, with particular emphasis on:
        i. Certificate issuance, renewal, and revocation processes.
        ii. Attestation validation procedures.
        iii. Key management practices within devices or applications and the CA's infrastructure.
        iv. Logical and procedural security controls.
        v. Personnel security and training related to attestation validation and certificate management.
        vi. Incident response and disaster recovery procedures.
3. Audit Reports:
    a. The CA SHOULD make audit reports available to the C2PA Steering Committee and other authorized parties upon request.
    b. Audit reports SHOULD clearly identify any non-conformities or areas for improvement.
    c. Audit reports SHOULD be in International English or be accompanied by a professional translation to English.
    d. The CA SHOULD take corrective action to address any identified deficiencies.

8.2. Other Assessments

1. Vulnerability Assessments and Penetration Tests:

a. The CA SHOULD conduct regular vulnerability assessments and penetration tests on its infrastructure, systems, and attestation validation processes (if applicable) to identify and address security weaknesses.

b. These assessments SHOULD be performed by qualified security professionals and SHOULD also include reviews of the security of the Generator Product platforms and any attestation services used.

c. Remediation plans SHOULD be developed and implemented to address any identified vulnerabilities.

2. Security Incident Reviews:

a. In the event of a Security Incident, the CA SHALL conduct a thorough review to determine the root cause, impact, and lessons learned.

b. The review SHALL result in actionable recommendations to prevent similar incidents in the future.

c. Incident reports SHALL be shared with the C2PA Steering Committee and the C2PA Technical Working Group Conformance Task Force.

The CA's commitment to regular compliance audits and other assessments demonstrates its dedication to maintaining a secure and trustworthy PKI environment for C2PA content origination.

9. Other Business and Legal Matters

This section outlines various business and legal considerations pertinent to the issuance and utilization of certificates under this CP, delineating the financial obligations, confidentiality and privacy safeguards, intellectual property rights, and dispute resolution mechanisms.

9.1. Fees

9.1.1. Fees for Services

The CA MAY levy reasonable fees for services rendered under this CP, encompassing certificate issuance, renewal, revocation, and technical support. The fee structure SHALL be transparently published and readily accessible to Subscribers.

9.1.2. Fee Adjustments

The CA reserves the right to modify its fee structure with prior notification to Subscribers, ensuring transparency and predictability in cost management.

9.1.3. Subscriber Responsibility

The Subscriber assumes full responsibility for any and all fees incurred under this CP.

9.2. Financial Responsibility

9.2.1. Subscriber's Financial Obligation

The Subscriber bears the financial responsibility for all fees associated with the certificate lifecycle, including issuance, renewal, and any potential revocation fees.

9.2.2. CA’s Limited Liability

The CA SHALL NOT be held liable for any financial losses or damages incurred by the Subscriber as a consequence of certificate misuse, compromise, or revocation, unless such losses directly arise from the CA’s negligence or willful misconduct.

9.3. Confidentiality of Business Information

9.3.1. CA’s Commitment to Confidentiality

The CA pledges to uphold the confidentiality of all non-public Subscriber business information obtained during the certificate application and validation processes.

9.3.2. Information Sharing Restrictions

Such information SHALL NOT be shared with any third parties without the Subscriber’s explicit written consent, except when mandated by law or regulation, or required for independent auditing purposes.

9.4. Privacy of Personal Information

9.4.1. Compliance with Privacy Laws

The CA commits to collecting and processing personal information in strict accordance with applicable privacy laws and regulations.

9.4.2. Purpose Limitation

Personal information SHALL be collected and utilized solely for the purposes explicitly outlined in this CP, including but not limited to identity verification and certificate issuance.

9.4.3. Data Subject Rights

Subscribers retain the right to access, rectify, or erase their personal information held by the CA, subject to legal and regulatory constraints.

9.5. Intellectual Property Rights

9.5.1. Subscriber’s Ownership

The Subscriber maintains full ownership and control over all intellectual property rights associated with the claim generation implementation that signs using certificates issued under this CP.

9.5.2. CA’s Non-Claim

The CA asserts no claim or ownership over any intellectual property rights pertaining to the Subscriber’s implementation.

9.6. Representations and Warranties

9.6.1. CA Representations

By issuing a Certificate, the CA makes the certificate warranties listed herein to the following Certificate Beneficiaries:

1. The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate;
2. The C2PA with whom the Issuing CA has entered into a contract for inclusion of a CA record in the C2PA Trust List; and
3. All Relying Parties who reasonably rely on a Valid Certificate.

The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with these Requirements and its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

1. **Right to Use Domain Name or IP Address**: That, at the time of issuance, the CA
    a. implemented a procedure for verifying that the Applicant either had the right to use, or had control of, product name listed in the Certificate's `subject` field and `subjectAltName` extension;
    b. followed the procedure when issuing the Certificate; and
    c. accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
2. **Authorization for Certificate**: That, at the time of issuance, the CA
    a. implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject;
    b. followed the procedure when issuing the Certificate; and
    c. accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
3. **Accuracy of Information**: That, at the time of issuance, the CA
    a. implemented a procedure for verifying the accuracy of all of the information contained in the Certificate;
    b. followed the procedure when issuing the Certificate; and
    c. accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
4. **Subscriber Agreement**: That, if the CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
5. **Status**: That the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
6. **Revocation**: That the CA revokes the Certificate for any of the reasons specified in this CP.

A Root CA SHALL be responsible for the performance and warranties of the Issuing CA, for the Issuing CA's compliance with this CP, and for all liabilities and indemnification obligations of the Issuing CA under this CP, as if the Root CA were the Issuing CA issuing the Certificates

9.6.2. Subscriber Representations

By applying for and utilizing certificates under this CP, the Subscriber represents and warrants the following:

1. The information furnished in the certificate application is accurate, complete, and truthful.
2. They possess the requisite legal authority to request and utilize certificates under this CP.
3. They SHALL adhere to all stipulations and restrictions delineated in this CP.
4. They SHALL employ the certificates solely for their intended purpose, refraining from any prohibited activities.

9.7. Disclaimers of Warranties

9.7.1. CA’s Disclaimer

No stipulation.

9.7.2. Content Disclaimer

No stipulation.

9.8. Limitations of Liability

9.8.1. CA’s Limited Liability

No stipulation.

9.8.2. Exclusion of Consequential Damages

No stipulation.

9.9. Indemnities

No stipulation.

9.10. Term and Termination

9.10.1. Term

This CP becomes effective when approved by the C2PA Governing Authority. Amendments to this CP become effective upon publication. This CP has no specified term.

9.10.2. Termination

This CP, as amended from time to time, SHALL remain in force until it is replaced by a new version. Termination of this CP is at the discretion of the C2PA Governing Authority.

9.10.3. Termination Rights

No stipulation.

9.10.4. Post-Termination Obligations

No stipulation.

9.11. Individual Notices and Communications with Participants

9.11.1. Written Communication

All official notices and communications between the CA and the Subscriber SHALL be in writing and conveyed electronically or by mail. .

9.11.2. Contact Information

All parties SHALL maintain accurate and up-to-date contact information to facilitate effective communication.

9.12. Amendments

9.12.1. Policy Modification

The C2PA Governing Authority retains the right to amend this CP at any time, reflecting evolving security best practices, technological advancements, or regulatory changes.

9.12.2. Subscriber Notification

Subscribers SHALL be promptly notified of any material changes to the CP through appropriate channels, ensuring they remain informed of their obligations and responsibilities.

9.12.3. Acceptance of Amendments

Continued utilization of certificates after CP amendments constitutes the Subscriber’s acceptance of the revised terms and conditions.

9.13. Dispute Resolution Procedures

No stipulation.

9.14. Governing Law

9.14.1. Jurisdiction

This CP and any agreements arising from it SHALL be governed by SHALL be construed pursuant to the laws of the State of Delaware (without regard to conflict of laws principles). The state and federal courts of Delaware, U.S.A. SHALL have jurisdiction and the parties waive any other jurisdiction.

9.15. Compliance with Applicable Law

9.15.1. Legal Compliance

Both the CA and the Subscriber are obligated to comply with all applicable laws and regulations pertaining to the issuance, use, and management of certificates under this CP.

9.16. Miscellaneous Provisions

9.16.1. Governing Agreements

Between the C2PA Governing Authority and CAs

The relationship between the C2PA Governing Authority and the CAs SHALL be governed by the Certification Authority Agreement and this Certificate Policy.

Between CAs and Subscribers

The relationship between the CA and the Subscriber SHALL be governed by the CA's Subscriber Agreement.

9.16.2. Waiver

No stipulation.

9.16.3. Severability

In the event that any provision of this CP is deemed invalid or unenforceable, the remaining provisions SHALL remain in full force and effect, and the invalid or unenforceable provision SHALL be replaced with a valid and enforceable provision that most closely approximates the intent of the original provision.

9.17. Other Provisions

No stipulation.

Appendix A: Requirements for Validating Dynamic Evidence

A.1. Requirements for Assurance Level 1 Certificates

Security Objective	Requirement
O.1 Conforming GP instance provides proof of its eligibility during automated certificate enrollment.	CA SHALL verify that the entity attempting certificate enrollment is an instance of a Subscriber's Generator Product, through an authentication method commonly accepted for certificate enrollment (e.g. SCEP, EST, ACME, client certificates, etc.).

Security Objective	Requirement
O.2 GP TOE protects the confidentiality of the signing key.	No stipulation.
O.3 - GP TOE protects the Claim Generator from exploits, misconfiguration and misuse.	No stipulation.
O.4 - GP TOE protects the asset and assertions from being tampered with at generation.	No Stipulation.
O.5 - GP TOE protects the traffic between subsystems and components of those subsystems from being intercepted and/or modified.	No stipulation.
O.6 - Hosting environment is protected from exploit, misconfiguration and misuse.	No stipulation.

A.2. Requirements for Assurance Level 2 Certificates

Security Objective	Requirement
O.1 Conforming GP instance provides proof of its eligibility during automated certificate enrollment.	CA SHALL verify that the entity attempting certificate enrollment is an instance of a Subscriber’s Generator Product, through requesting and validating verifiable, hardware-backed artifacts that attest to the package names, hashes, code signing certificates or other certificates of the entity requesting certificate enrollment. CA SHALL NOT issue a certificate if the entity attempting certificate enrollment is unable to present this evidence, or if the values in the hardware-backed artifacts do not meet the aforementioned requirements.
O.2 GP TOE protects the confidentiality of the signing key.	CA SHALL verify that the key pair for which certificate enrollment is being attempted is generated and stored within a hardware-backed platform keystore service or Key Management Service, by requesting and validating verifiable, hardware-backed artifacts that attest to the security attributes of the key and its possession by an instance of the Subscriber’s Generator Product. CA SHALL NOT issue a certificate if the entity attempting certificate enrollment is unable to present this evidence, or if the values in the hardware-backed artifacts do not meet the aforementioned requirements.

Security Objective	Requirement
O.3 - GP TOE protects the Claim Generator from exploits, misconfiguration and misuse.	CA SHALL verify that the platform on which the Claim Generator integrated with the instance of the Generator Product attempting certificate enrollment is running has booted securely into authenticated software images by requesting and validating verifiable artifacts backed by a hardware root of trust. CA SHALL NOT issue a certificate if the entity attempting certificate enrollment is unable to present this evidence, or if the values in the hardware-backed artifacts do not meet the aforementioned requirements.
O.3 - GP TOE protects the Claim Generator from exploits, misconfiguration and misuse.	CA SHALL verify that the platform on which the Claim Generator integrated with the instance of the Generator Product attempting certificate enrollment is running has security patches no older than the latest patch or version required to fix or otherwise mitigate any vulnerabilities with a CRITICAL or HIGH severity ratings in the NIST Common Vulnerability Scoring System (CVSS, https://nvd.nist.gov/vuln-metrics/cvss) version 3 or greater, within 90 days of detection, by requesting and validating verifiable artifacts backed by a hardware root of trust. CA SHALL NOT issue a certificate if the entity attempting certificate enrollment is unable to present this evidence, or if the values in the hardware-backed artifacts do not meet the aforementioned requirements.
O.3 - GP TOE protects the Claim Generator from exploits, misconfiguration and misuse.	CA SHALL verify, depending on the method which the Applicant has selected: 1. the recency of application of security patches of the Claim Generator integrated with the instance of the Generator Product requesting certificate enrollment is no older than 90 days 2. that the revision (e.g. version, branch, or commit identifier) of the Claim Generator integrated with the instance of the Generator Product attempting certificate enrollment is one that is registered in good standing with the CA, by requesting and validating verifiable artifacts backed by a hardware root of trust. CA SHALL NOT issue a certificate if the entity attempting certificate enrollment is unable to present this evidence, or if the values in the hardware-backed artifacts do not meet the aforementioned requirements.

Security Objective	Requirement
O.4 - GP TOE protects the asset and assertions from being tampered with at generation.	CA SHALL verify that the platform on which software in the GP TOE that processes/modifies the Digital Content and/or Assertions is running has booted securely into authenticated software images, by requesting and validating verifiable artifacts backed by a hardware root of trust. CA SHALL NOT issue a certificate if the entity attempting certificate enrollment is unable to present this evidence, or if the values in the hardware-backed artifacts do not meet the aforementioned requirements.
O.4 - GP TOE protects the asset and assertions from being tampered with at generation.	CA SHALL verify that the platform on which all such software in the GP TOE is running has security patches no older than the latest patch or version required to fix or otherwise mitigate any vulnerabilities with a CRITICAL or HIGH severity ratings in the NIST Common Vulnerability Scoring System (CVSS, https://nvd.nist.gov/vuln-metrics/cvss) version 3 or greater, within 90 days of detection, by requesting and validating verifiable artifacts backed by a hardware root of trust. CA SHALL NOT issue a certificate if the entity attempting certificate enrollment is unable to present this evidence, or if the values in the hardware-backed artifacts do not meet the aforementioned requirements.
O.4 - GP TOE protects the asset and assertions from being tampered with at generation.	CA SHALL verify, depending on the method which the Applicant has selected: 1. the recency of application of security patches of all such software in the GP TOE is no older than 90 days 2. that the revision (e.g. version, branch, or commit idenitifer) of the all such software in the GP TOE attempting certificate enrollment is one that is registered in good standing with the CA, by requesting and validating verifiable artifacts backed by a hardware root of trust. CA SHALL NOT issue a certificate if the entity attempting certificate enrollment is unable to present this evidence, or if the values in the hardware-backed artifacts do not meet the aforementioned requirements.
O.5 - GP TOE protects the traffic between subsystems and components of those subsystems from being intercepted and/or modified.	No stipulation.

Security Objective	Requirement
O.6 - Hosting environment is protected from exploit, misconfiguration and misuse.	No stipulation.

A.3. Platform-specific Guidance

While the CA is required to validate the above requirements, the specific methods for doing so varies by the specific service/platform. This section attempts to provide specific guidance for different types of platforms and attestation methods.

Generally, key and platform attestation flows require the CA to issue a unique, dynamic challenge (usually referred to as a nonce) to the entity from which it is requesting attestation. Platform attestation providers in turn include the challenge nonce in the attestation report, and the CA SHALL verify that the challenge nonce in the attestation report matches the one that it issued to the instance of the Generator Product requesting certificates. CAs SHALL follow the recommendations of attestation service/platform providers when generating nonces.

A.3.1. Android Key Attestation

Android Key Attestation can be used for validating the security attributes of Subscriber C2PA Claim Signing Key, validating the identity and integrity of the instance of the Generator Product requesting certificates, and validating the integrity of the Android platform on which the application is running.

Security objectives addressed by this service/platform: . Security Objective 1 . Security Objective 2 . Security Objective 3 . Security Objective 4

Resources

1. Main documentation
2. Attestation certificate structure and schema for the `attestation` X.509v3 extension
3. Helper libraries

Guidance on Values

Guidance on Values for Assurance Level 1

No stipulation.

Guidance on for Assurance Level 2

Based on the values of the attributes in the Android Key Attestation Certificate `attestation` extension

Requirement Source	Attestation Certificate Chain Attribute	Value
Security Objective O.3, Security Objective O.4	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `attestationSecurityLevel`	`1` (`TrustedEnvironment`) or `2` (`StrongBox`)
Security Objective O.3, Security Objective O.4	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `keyMintSecurityLevel`	`1` (`TrustedEnvironment`) or `2` (`StrongBox`)

Requirement Source	Attestation Certificate Chain Attribute	Value
Security Objective O.1, Security Objective O.2, Security Objective O.3, Security Objective O.4	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `attestationChallenge`	Matches the value of the challenge issued by the CA
Security Objective O.1	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `softwareEnforced.attestationApplicationID` [Tag 709] → `package_infos` set element → `package_name`	Matches the package name of the Subscriber's Generator Product app that's registered with the CA
Security Objective O.1	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `softwareEnforced.attestationApplicationID` [Tag 709] → `package_infos` set element → `version`	Matches one of the versions of the Subscriber's Generator Product app that's registered with the CA
Security Objective O.1	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `softwareEnforced.attestationApplicationID` [Tag 709] → `signature_digests` → set element	Matches the SHA-256 digests of the Subscriber's Generator Product app's signing certificates registered with the CA
Claim Signing Certificate Profile constraint	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `hardwareEnforced.purpose` [Tag 1]	Set with an item whose value is equivalent to: `SIGN` / `2` as described in KeyPurpose.aidl
Claim Signing Certificate Profile constraint	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `hardwareEnforced.algorithm` [Tag 2]	Equivalent to `RSA` / `1` or `EC` / `3` as described in Algorithm.aidl
Claim Signing Certificate Profile constraint	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `hardwareEnforced.keySize` [Tag 3]	For RSA keys, one of: `2048`, `3072`, `4096`. For EC keys, one of: `256`, `384`, `521`
Claim Signing Certificate Profile constraint	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `hardwareEnforced.digest` [Tag 5]	Set with items whose values are equivalent to: `SHA_2_256` / `4` `SHA_2_384` / `5`, or `SHA_2_512` / `6` as described in Digest.aidl
Claim Signing Certificate Profile constraint	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `hardwareEnforced.padding` [Tag 6]	[For RSA keys only] Equivalent to: `RSA_PSS` / `3` as described in PaddingMode.aidl
Claim Signing Certificate Profile constraint	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `hardwareEnforced.ecCurve` [Tag 10]	Equivalent to: `P_256` / `1`, `P_384` / `2`, or `P_521` / `3` as described in EcCurve.aidl Please note: Matches the corresponding value in Tag 3 for EC keys.
Security Objective O.2	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `hardwareEnforced.origin` [Tag 702]	Equivalent to: `GENERATED` / `0` as described in KeyOrigin.aidl

Requirement Source	Attestation Certificate Chain Attribute	Value
Security Objective O.4	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `hardwareEnforced.rootOfTrust` [Tag 704] → `deviceLocked` [Element 2 of sequence]	Equivalent to `true`
Security Objective O.4	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `hardwareEnforced.rootOfTrust` [Tag 704] → `verifiedBootState` [Element 3 of sequence]	`0` (`Verified`)
Security Objective O.4	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `hardwareEnforced.osPatchLevel` [Tag 706]	4 months or less relative to the month of the CSR submission. Cannot be in the future relative to the month of the CSR submission. For example, for a CSR submitted in the month of August 2026, an acceptable value would be any of `202608`, `202607`, `202606`, or `202605`.
Security Objective O.1	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `hardwareEnforced.attestationIdBrand` [Tag 710]	If Subscriber's Generator Product app is intended to run on only a specific OEM device brand, matches the value registered with the CA
Security Objective O.1	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `hardwareEnforced.attestationIdManufacturer` [Tag 716]	If Subscriber's Generator Product app is intended to run on only a specific OEM device brand, matches the value registered with the CA
Security Objective O.1	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `hardwareEnforced.attestationIdModel` [Tag 717]	If Subscriber's Generator Product app is intended to run on only a specific OEM device model, matches the value registered with the CA
Security Objective O.4	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `hardwareEnforced.vendorPatchLevel` [Tag 718]	90 days or less from the date of the CSR submission. Cannot be in the future relative to the date of the CSR submission. For example, for a CSR submitted on June 20th, 2026, a value of `20260505` is acceptable (46 day difference), while a value of `20260105` is not (166 day difference).

Requirement Source	Attestation Certificate Chain Attribute	Value
Security Objective O.4	Leaf certificate → 1.3.6.1.4.1.11129.2.1.17 → `hardwareEnforced.bootPatchLevel` [Tag 718]	90 days or less from the date of the CSR submission. Cannot be in the future relative to the date of the CSR submission. For example, for a CSR submitted on June 20th, 2026, a value of `20260505` is acceptable (46 day difference), while a value of `20260105` is not (166 day difference).

A.3.2. Google Play Integrity

Guidance under development. Refer to Google Play Integrity documentation.

A.3.3. Apple App Attest

Guidance under development. Refer to Apple App Attest documentation.

A.3.4. Qualcomm Wireless Edge Services (QWES)

Guidance under development. Refer to Qualcomm WES documentation.

A.3.5. IETF Remote ATtestation ProcedureS (RATS)

Guidance under development. Refer to RFC 9334.

A.3.6. AWS Key Management Service

Guidance under development. Refer to AWS KMS documentation.

A.3.7. AWS Nitro Enclaves Attestation

Guidance under development. Refer to AWS Nitro Enclaves Attestation documentation.

A.3.8. Microsoft Azure Key Vault and Azure Managed HSM

Guidance under development. Refer to Azure Managed HSM key attestation documentation.

A.3.9. Microsoft Azure Attestation

Guidance under development. Refer to Azure Attestation documentation.

A.3.10. Google Cloud Platform Cloud HSM Key Attestation

Guidance under development. Refer to GCP Cloud HSM Key Attestation documentation.

A.3.11. Google Cloud Confidential VM Attestation

Guidance under development. Refer to GCP Confidential VM Attestation documentation.