Trufo
CP + CPS

Certificate Policy
Certification Practices Statement
Version 2.1

March 2026

trufo.ai

Contents

1 Introduction

Trufo is an umbrella entity that operates multiple services. The Trufo Certificate Authority (TCA) is the Certification Authority (CA) described in this CP/CPS and operates the public key infrastructure (PKI) defined herein. This PKI is designed to support C2PA and CAWG in the context of digital content provenance.

To achieve this, the Trufo Certificate Authority (TCA) performs PKI services that include the issuing and renewal of digital certificates via both manual handshakes and Enrollment over Secure Transport (EST) endpoints. The TCA also maintains a number of other services in the provenance ecosystem, including but not limited to: OCSP endpoints, TSA endpoints, Trufo Key Management (TKM).

For convenience, the document includes tags that indicate relevance:

`C2PA` anything specific to C2PA Claim Signing certificates.

`CAWG` anything specific to CAWG Identity certificates.

1.1 Overview

This document details the Certificate Policy (CP) and Certification Practice Statement (CPS) of entities participating in this PKI.

This CP/CPS abides by the following guidelines:

- C2PA Certificate Policy v0.1 (2025-06-02)
- C2PA Generator Product Security v0.1 (2025-06-02)
- CAWG (pending trust model)

While the TCA does not provide WebPKI services, the TCA intends to meet CAB Forum requirements as they are relevant to the trust ecosystem of digital content provenance.

- CAB Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates (PTCs).
- CAB Forum, Guidelines for Extended Validation Certificates (EVCs).
- CAB Forum, Guidelines for the Issuance and Management of Code Signing Certificates (CSCs).

There are a number of services that the TCA provides:

- C2PA/CAWG Root CA Trust
- C2PA Claim Signing Issuance (Level 1 and Level 2)
- C2PA Timestamping
- CAWG Identity Issuance
- OCSP Responders
- HSM Key Management

This CP/CPS governs certificate policy and certification practice requirements applicable to TCA's CA services. Trufo may publish additional documents (e.g., terms and privacy materials) that apply to use of Trufo-operated services.

1.2 Document Name and Identification

This document is the Trufo Certificate Policy and Certification Practice Statement (the "CP/CPS"). This CP/CPS is organized according to the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647).

1.2.1 Policy Object Identifiers (OIDs)

The enterprise OID arc assigned to Trufo by IANA is `1.3.6.1.4.1.62524`:

iso (1) org (3) dod (6) internet (1) private (4) enterprise (1) Trufo.ai (62524)

Trufo allocates the following OID arc for certificate policy identification under this CP/CPS:

`1.3.6.1.4.1.62524.1.1` (CP/CPS policy identifier)

Trufo allocates the following OID arc for identifying this CP/CPS document and its published revisions:

`1.3.6.1.4.1.62524.1.1.2.1`

Where applicable, certificates issued under this CP/CPS MAY include certificate policy identifiers (e.g., in the Certificate Policies extension) and/or other OID-based signaling (e.g., EKUs) to indicate applicability of a particular certificate policy regime or profile. C2PA and CAWG ecosystem-specific identifiers, when required, are reflected in the applicable certificate profile sections (see §7).

1.2.2 Document Versioning

The provisions of this CP/CPS are amended periodically. Trufo maintains a revision history to enable relying parties and other stakeholders to reference a particular version of this CP/CPS. The most recent version of this CP/CPS is publicly available at https://trufo.ai/cpcps.

The table below specifies all revisions made:

Date	Version	Changelog
2024/10/23	1.0	Initial publication.
2026/01/31	2.0	C2PA + CAWG Conformance.
2026/03/21	2.1	Operational updates from web-based RA platform.

1.2.3 Conformance Statements (C2PA / CAWG)

This CP/CPS describes the certificate policy and certification practices applicable to TCA's CA services as they relate to the C2PA and CAWG ecosystems. Trufo intends for the PKI services described in this CP/CPS to conform to applicable requirements of the following inputs, as in scope for TCA's services:

- C2PA Certificate Policy v0.1 (2025-06-02).
- C2PA Generator Product Security v0.1 (2025-06-02).
- CAWG Identity Assertion requirements and related CAWG materials, noting that portions of the CAWG trust model may evolve.

Where these ecosystems require specific certificate semantics (e.g., EKUs, policy OIDs, extensions) or operational behaviors (e.g., status checking expectations), TCA expresses

those requirements concretely in the certificate profile sections (§7) and the applicable operational and control sections (§2 through §6).

1.3 PKI Participants

This PKI includes the entities and roles necessary to issue, manage, validate, and revoke certificates used in the C2PA and CAWG provenance ecosystems. The participant set includes:

- Certification Authorities (Root and Issuing CAs) operated by TCA.
- Registration Authority (RA) functions that validate Applicants and Subscribers and authorize issuance.
- Subscribers (certificate holders), including organizations operating C2PA Conforming Generator Products and entities holding CAWG identity certificates.
- Relying Parties (validators/verifiers) that evaluate signatures, certificate chains, and revocation status.
- Repositories and online status services used for certificate discovery and status checking.
- Timestamping Authority (TSA) and OCSP responder services where applicable.
- Auditors and other oversight roles as required by applicable programs.

RA interactions are supported via RA-issued CSR JWTs that authorize EST enrollment. Public service endpoints supporting validation (including OCSP and TSA) are provided as described in §2 and summarized in Appendix B.

C2PA In the C2PA ecosystem, Subscribers include organizations operating Conforming Generator Products. C2PA Generator Products may be deployed in server, distributed, or edge configurations and may operate at different assurance levels (e.g., Level 1 and Level 2). Relying parties include C2PA Validator Products that validate C2PA claims and their associated certificate chains, potentially at different validator levels. Higher-assurance configurations may require increased RA responsibilities and validation rigor as described in this CP/CPS.

CAWG In the CAWG ecosystem, Subscribers include certificate holders that create CAWG identity assertions, and relying parties include validators that verify those assertions in accordance with CAWG requirements. Where CAWG trust model inputs reference external registries (e.g., publisher lists), those inputs are treated as relying-party validation signals and are handled as described in the applicable identification/authentication and profile sections.

1.4 Certificate Usage

This section describes the intended and prohibited usages of certificates issued under this CP/CPS. Certificate usage is defined by the applicable certificate profiles (including key usage, EKU, basic constraints, and policy OIDs) and by the requirements of the C2PA and CAWG trust ecosystems.

C2PA TCA issues certificates for (a) C2PA claim signing and (b) C2PA timestamping. Claim signing certificates are intended to sign C2PA claims/manifests in accordance with

the applicable C2PA profile and constraints (including EKU and policy signaling where applicable). Timestamping certificates are intended to produce RFC 3161 time-stamp tokens used in provenance validation.

CAWG TCA issues CAWG identity certificates for signing CAWG identity assertions in accordance with the CAWG profile. Where CAWG specifies semantics that are expressed outside of X.509 (e.g., COSE signature semantics or profile-specific fields), TCA uses certificate profile constraints and policy signaling to ensure relying parties can interpret the intended usage and assurance regime. Timestamping MAY be used in support of CAWG identity assertions where required by the applicable profile.

1.4.1 Appropriate Certificate Uses

Appropriate uses are those that match the certificate's intended purpose as signaled by its EKU, key usage, basic constraints, and policy OIDs.

- CA certificates are used to issue and revoke certificates and to produce supporting PKI artifacts as permitted by key usage and basic constraints.

C2PA Claim signing end-entity certificates are used to sign C2PA manifests/claims in conformance with the applicable certificate profile, including any required EKUs and policy identifiers. Timestamping end-entity certificates are used to produce RFC 3161 time-stamp tokens. TCA's timestamping service is designed to support relying parties that validate time-stamp tokens as part of provenance validation, including where a third-party TSA implementation is used in accordance with the applicable profile and this CP/CPS.

CAWG CAWG identity certificates are used to sign CAWG identity assertions where the relying party expects and validates the applicable CAWG profile. The certificate profile constraints and policy signaling are intended to allow relying parties to distinguish CAWG identity assertion signatures from other types of signatures.

1.4.2 Prohibited Certificate Uses

Prohibited uses include any use that conflicts with the certificate's profile constraints or that could mislead relying parties about the semantics of a signature. The following are non-exhaustive examples of prohibited uses:

- Using a timestamping certificate for general document signing, or using a claim signing (or identity) certificate for timestamping, when the applicable EKU/profile does not permit that usage.
- Using CA private keys for purposes other than CA operations.
- Representing a certificate as being issued under a different policy, profile, or assurance regime than its actual policy identifiers and profile constraints indicate.
- Modifying, stripping, or selectively presenting certificate chain, status, or profile data in a manner intended to mislead relying parties.

Any usage not consistent with the certificate profile and this CP/CPS is prohibited.

1.4.3 Delegated / Third-Party Service Constraints

Where TCA uses a third party to operate timestamping services, such third-party operation SHALL meet the delegated TSA operator requirements described in §6.8 (including §6.8.4). Such third-party timestamping services are subject to at least annual audit by TCA.

Other delegation of CA or RA functions is not supported under this CP/CPS unless explicitly described in a future revision.

1.5 Policy Administration

This CP/CPS is maintained and administered under Trufo's umbrella in accordance with the roles and procedures described in §1.5.1 through §1.5.4.

1.5.1 Organization Administering the Document

The Trufo Policy Authority (TPA) administers the CP portions of this CP/CPS. The TPA is a lightweight function that consolidates applicable external program requirements (including C2PA requirements and, as applicable, CAWG and other ecosystem requirements as they mature) into a coherent set of policy commitments that TCA is expected to follow.

The Trufo Certificate Authority (TCA) administers and operates under the CPS portions of this CP/CPS and is the implementor and operator of the CA services described herein.

The TPA and TCA are appointed by Trufo's executive management.

1.5.2 Contact Person / Contacts

External parties may contact TCA regarding this CP/CPS and PKI operations at:

Trufo Certificate Authority
228 Park Ave S, PMB 87518
New York, NY 10003-1502, USA
ca@trufo.ai

1.5.3 Person Determining CPS Suitability

The Trufo Policy Authority (TPA) determines CPS suitability with respect to the consolidated policy commitments captured in this CP/CPS, including alignment to applicable external program requirements. Trufo designates a C2PA conformance administrator responsible for determining CPS suitability and operational conformance with the C2PA Certificate Policy and related C2PA requirements.

1.5.4 CP/CPS Approval Procedures

This CP/CPS is reviewed by the Trufo Policy Authority (TPA) at least annually. This CP/CPS is additionally reviewed upon updates to any external certificate policies or requirements to which this CP/CPS conforms, and whenever recommended by the TPA or the C2PA conformance administrator. Approved revisions are published in accordance with the versioning provisions in §1.2.2.

1.6 Definitions and Acronyms

The following definitions, acronyms, and normative language conventions are used throughout this CP/CPS.

1.6.1 Definitions

Applicant
: An entity (typically an organization) applying for the issuance of a Certificate under this CP/CPS. For C2PA Claim Signing certificates, the Applicant is the organization associated with a Conforming Generator Product.

Applicant's Representative
: A natural person authorized to act on behalf of the Applicant in requesting certificate issuance, revocation, or other PKI services, and who is authorized to bind the Applicant to the Subscriber Agreement.

Assurance Level
: A designation (Level 1 or Level 2) indicating the security requirements and validation rigor applied to a C2PA Generator Product, as defined by the C2PA Generator Product Security Requirements.

Attestation Letter
: A letter attesting Subject Information, written by a legal entity with knowledge of the facts being attested.

CA Certificate
: A Certificate issued to a Certification Authority, enabling that CA to issue subordinate certificates.

Certificate
: An electronic document conforming to X.509 v3 that uses a digital signature to bind a Public Key to an identity (Subject).

Certificate Chain
: An ordered sequence of Certificates from an end-entity leaf certificate to a trusted Root CA certificate, enabling validation of the leaf certificate's authenticity.

Certificate Policy (CP)
: A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements.

Certificate Signing Request (CSR)
: A message sent from an Applicant to a CA to apply for a Certificate, typically containing the public key to be certified and proof of possession of the corresponding private key.

Certification Authority (CA)
: An entity authorized to issue, manage, revoke, and renew Certificates. In this CP/CPS, the term encompasses both Root CAs and Issuing CAs.

Certification Practice Statement (CPS)
: A statement of the practices that a Certification Authority employs in issuing, managing, revoking, and renewing Certificates.

Claim Signing Certificate
: An end-entity Certificate issued under this CP/CPS for the purpose of signing C2PA claims/manifests. See §7.4.1.

EST Endpoint
: A network service implementing Enrollment over Secure Transport (RFC 7030) for automated certificate lifecycle operations (enrollment and renewal), with authentication material as described in this CP/CPS.

Conforming Generator Product
: A software or hardware product that conforms to C2PA specifications and is listed on the C2PA Conforming Products List (CPL).

Conforming Products List (CPL)
: The official registry maintained by C2PA of products that have demonstrated conformance to C2PA specifications. Each product is identified by a unique UUID.

Delegated Operator
: An entity that operates signing infrastructure under this PKI hierarchy pursuant to a written agreement with TCA. Delegated Operators receive certificates (typically leaf certificates) enabling them to perform signing operations.

Distinguished Name (DN)
: An X.501 identifier used in the Subject and Issuer fields of X.509 Certificates, composed of Relative Distinguished Names (RDNs) such as Country (C), Organization (O), and Common Name (CN).

End-Entity Certificate (Leaf Certificate)
: A Certificate issued to a Subscriber for operational use (e.g., claim signing, timestamping, OCSP signing, identity assertion signing), as opposed to a CA Certificate.

Extended Key Usage (EKU)
: An X.509 v3 extension that indicates the purposes for which the certified public key may be used, beyond or in addition to the basic Key Usage extension.

Generator Product
: A C2PA-compliant product capable of creating C2PA claims. Generator Products are categorized by deployment type (Server, Distributed, Edge) and Assurance Level (Level 1, Level 2).

Hardware Protected Environment (HPE)
: A hardware-based security mechanism such as a Trusted Execution Environment (TEE) or Hardware Security Module (HSM) that protects cryptographic keys from unauthorized access.

Hardware Security Module (HSM)
: A dedicated cryptographic processor designed for the protection of the cryptographic key lifecycle, typically certified to standards such as FIPS 140-2/3.

Identity Assertion
: In the CAWG context, a signed statement binding an identity (e.g., a named actor) to a C2PA manifest, enabling attribution of content to specific individuals or organizations.

Initial Identity Validation (IIV)
: The process by which the CA/RA validates the identity of an Applicant before issuing a Certificate. See §3.2.

Issuing CA
: A subordinate CA that issues end-entity Certificates and/or further subordinate CA Certificates. In this PKI, Issuing CAs are signed by the Root CA.

Key Pair
: A Private Key and its mathematically associated Public Key.

Key Usage
: An X.509 v3 extension that defines the purpose(s) for which the key certified in a Certificate may be used (e.g., digitalSignature, keyCertSign).

Logotype
: A graphical image (logo) associated with a certificate Subject, included via the RFC 9399 Logotypes extension.

OCSP Responder
: An online service that processes Certificate status requests and returns signed responses indicating whether a Certificate is valid, revoked, or unknown.

Organization Validation (OV)
: The process by which TCA validates an Applicant's organizational identity and authenticates an authorized representative for purposes of certificate issuance.

Policy Authority (PA)
: The entity responsible for approving and maintaining the Certificate Policy. For this PKI, the Trufo Policy Authority (TPA) serves this role.

Private Key
: The secret component of a Key Pair, used to create digital signatures or decrypt data. Private Keys must be protected from unauthorized disclosure.

Proof of Possession (PoP)
: Demonstration that an Applicant or Subscriber controls the Private Key corresponding to the Public Key submitted for certification, typically via a signed CSR.

Product Validation (PV)
: The process by which TCA validates a C2PA Generator Product's identity and conformance status (including matching the product to the C2PA Conforming Products List) as part of claim signing certificate issuance.

Public Key
: The public component of a Key Pair, included in a Certificate and used by Relying Parties to verify digital signatures or encrypt data.

Registration Authority (RA)
: An entity that performs identification and authentication functions on behalf of a CA. In this CP/CPS, RA functions are provided by Trufo-operated RA services that authorize CA enrollment flows.

Relying Party
: An entity that relies upon the information contained within a Certificate (e.g., to verify a digital signature or validate the identity of a Subscriber).

Repository
: A system for storing and retrieving Certificates, Certificate status information, and related PKI artifacts.

Revocation
: The process of invalidating a Certificate before its natural expiration, typically due to key compromise, cessation of operations, or policy violation.

Root CA
: The top-level CA in a PKI hierarchy that issues its own self-signed Certificate and serves as the ultimate trust anchor.

Provisioning Secret
: A confidential, short-lived JWT authorization token issued by the RA for use in authenticating an EST enrollment request at the CA, as described in §4.

Subject
: The entity identified by the Certificate, indicated in the Subject DN and/or Subject Alternative Name (SAN) extension.

Subscriber
: An entity that has been issued a Certificate under this CP/CPS and is bound by the Subscriber Agreement. For C2PA Claim Signing, the Subscriber is typically the organization operating the Conforming Generator Product.

Subscriber Agreement
: A binding agreement between the CA and Subscriber specifying the parties' rights, obligations, and liabilities with respect to Certificates issued under this CP/CPS.

Time-Stamp Token (TST)
: A cryptographically signed assertion that a datum existed at a particular time, produced by a Time-Stamp Authority in accordance with RFC 3161.

Timestamping Authority (TSA)
: A trusted service that issues Time-Stamp Tokens, providing proof that data existed at a specific point in time.

Trust Anchor
: A CA Certificate (typically a Root CA) that is explicitly trusted by a Relying Party as the starting point for certificate chain validation.

Trust List
: A list of trusted CA Certificates maintained by a trust ecosystem (e.g., the C2PA Trust List) for use by Relying Parties in validating certificate chains.

Trusted Execution Environment (TEE)
: A secure area of a processor that guarantees code and data loaded inside are protected with respect to confidentiality and integrity.

Trusted Role
: A role performed by personnel who have been vetted and authorized to perform sensitive CA operations. See §5.2.1.

Validator Product
: A C2PA-compliant product capable of verifying C2PA claims and validating the associated certificate chains and revocation status.

1.6.2 Acronyms

The following acronyms are used throughout the document.

Acronym	Expansion
AIA	Authority Information Access
C2PA	Coalition for Content Provenance and Authenticity
CA	Certification Authority
CAB	Certificate Authority/Browser (Forum)
CAWG	Creator Assertions Working Group
CDP	CRL Distribution Point
CN	Common Name

Acronym	Expansion
COSE	CBOR Object Signing and Encryption
CP	Certificate Policy
CPL	Conforming Products List
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CRMF	Certificate Request Message Format
CSR	Certificate Signing Request
DN	Distinguished Name
EKU	Extended Key Usage
EST	Enrollment over Secure Transport
FIPS	Federal Information Processing Standards
GP	Generator Product
HPE	Hardware Protected Environment
HSM	Hardware Security Module
IANA	Internet Assigned Numbers Authority
IIV	Initial Identity Validation
IPTC	International Press Telecommunications Council
KMS	Key Management Service
LEI	Legal Entity Identifier
MDB	MongoDB
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OV	Organization Validation
OID	Object Identifier
PII	Personally Identifiable Information
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PV	Product Validation
PoP	Proof of Possession
PP	Privacy Policy
PTP	Precision Time Protocol
RA	Registration Authority
RCA	Root Certification Authority
RDN	Relative Distinguished Name
RFC	Request for Comments
RSA	Rivest–Shamir–Adleman (algorithm)
SAN	Subject Alternative Name
SHA	Secure Hash Algorithm
SKI	Subject Key Identifier
S/MIME	Secure/Multipurpose Internet Mail Extensions
TCA	Trufo Certificate Authority
TEE	Trusted Execution Environment
TKM	Trufo Key Management
TLS	Transport Layer Security
ToS	Terms of Service

Acronym	Expansion
TPA	Trufo Policy Authority
TSA	Time-Stamp Authority / Timestamping Authority
TST	Time-Stamp Token
TSU	Time-Stamping Unit
UUID	Universally Unique Identifier

1.6.3 Normative Language

The following terms are used in this CP/CPS with their RFC 2119 meanings:

Shall / Must
: Indicates an absolute requirement. Non-compliance constitutes a violation of this CP/CPS.

Shall Not / Must Not
: Indicates an absolute prohibition. Non-compliance constitutes a violation of this CP/CPS.

Should / Recommended
: Indicates a recommendation. Deviation is permitted where there is a valid reason, but the implications must be understood and carefully weighed.

Should Not / Not Recommended
: Indicates a recommendation against a practice. Deviation is permitted where there is a valid reason, but the implications must be understood and carefully weighed.

May / Optional
: Indicates an item that is truly optional. Implementations may choose to include or exclude the item based on their requirements.

1.6.4 Normative and Informative References

This CP/CPS references the following RFCs as applicable:

- RFC 2119 (Key words for use in RFCs to Indicate Requirement Levels)
- RFC 3161 (Time-Stamp Protocol)
- RFC 3647 (Certificate Policy and Certification Practices Framework)
- RFC 5019 (Lightweight OCSP Profile)
- RFC 5035 (ESSCertIDv2)
- RFC 5280 (X.509 PKI Certificate and CRL Profile)
- RFC 6960 (OCSP)
- RFC 7030 (Enrollment over Secure Transport)
- RFC 9399 (Logotypes in X.509 Certificates)

2 Publication and Repository Responsibilities

2.1 Repositories

The TCA maintains a central repository at https://trufo.ai/tca/repository to allow access to documents and endpoints related to the TCA's certification policies and practices. This repository is maintained with resources sufficient to provide a commercially reasonable response time for access at all times.

Public service base URLs are:

Service	URL
CA services (certificate lifecycle endpoints)	https://ca.trufo.ai
TSA services (RFC 3161 timestamping)	https://tsa.trufo.ai
OCSP services (certificate status checking)	https://ocsp.trufo.ai
Repository (public CA and CP/CPS docs)	https://trufo.ai/tca/repository

CA certificates are available for download in DER format at:

Certificate	URL
Root CA	https://ca.trufo.ai/root-ca.crt
C2PA Claim Signing Issuing CA	https://ca.trufo.ai/c2pa-ca.crt
C2PA Timestamping CA	https://ca.trufo.ai/ctsa-ca.crt
CAWG Identity CA (Interim)	https://ca.trufo.ai/temp-cawg-ca.crt
OCSP Signing CA	https://ca.trufo.ai/ocsp-signing-ca.crt

The TCA also maintains internal certificate records repositories necessary for auditability and lifecycle management. These repositories include auditable records of (i) all certificates issued under the C2PA Certificate Policy, retained for at least one (1) year after certificate expiry, (ii) all registered entities, and (iii) all relevant PKI events. The TCA implements these controls using an internal database (retained for at least one (1) year) and PKI event logging via AWS CloudTrail (retained for seven (7) years).

2.2 Publication of Certification Information

This CP/CPS is available at https://trufo.ai/cpcps.

C2PA In support of the C2PA ecosystem, TCA publishes C2PA-specific materials at https://trufo.ai/tca/repository/c2pa-certificate-policy.pdf and https://trufo.ai/tca/repository/c2pa-generator-product-policy.pdf.

Trufo's Terms of Service (ToS) and Privacy Policy (PP) documents are available on Trufo's main website. Trufo may update the foregoing documents as the C2PA and CAWG ecosystem matures, and TCA may update the foregoing repositories and CP/CPS as the ecosystem matures.

Where applicable, certificates issued by TCA (other than root certificates) include Authority Information Access (AIA) fields that identify (i) this CP/CPS, (ii) the issuing CA certificate(s) required for path construction (via a CA Issuers URL), and (iii) the relevant OCSP endpoint. These intermediate CA certificates are published at the CA Issuers URL and are also available from the CA certificate download URLs in §2.1.

Appendix A provides a certificate profile summary, and Appendix B provides a consolidated endpoint quick reference.

2.3 Time or Frequency of Publication

The TCA updates this CP/CPS annually, and additionally as needed when significant changes are made. Historical versions of this CP/CPS are made accessible at https://trufo.ai/tca/repository/cpcps. Subscribers will be notified of updates to this CP/CPS, and of material changes to Trufo's Terms of Service and Privacy Policy, in accordance with §1.5.4.

Certificate status information is provided via OCSP. See §4.10 for certificate status service operational requirements, including OCSP response freshness requirements following revocation.

Revocation request processing timelines are described in §4.9.5.

2.4 Access Controls on Repositories

The contents of TCA's central repository and online API endpoints are made available on the Internet in a public, anonymous, and read-only manner. Only authorized parties are given write access; no other entities are permitted to modify the data held in these central repositories.

Public repository and service endpoints are served over HTTPS using TLS 1.2 or higher.

Requests are subject to moderate rate limit restrictions as protection against Denial of Service attacks; certain participants in this PKI may be exempt from this rate limit.

Internal certificate records repositories are restricted to authorized personnel and systems under least-privilege access controls, and are maintained to support audit and lifecycle management needs.

3 Identification and Authentication

This section defines how Subscribers (and where applicable, their authorized representatives) are identified and authenticated during certificate lifecycle events.

3.1 Naming

3.1.1 Types of Names

All certificates issued by TCA under this CP/CPS use X.501 Distinguished Names (DNs) in the certificate Subject. Where a profile requires additional identity information, such information is included in the Subject Alternative Name (SAN) and/or other extensions as specified in §7.

3.1.2 Need for Names to Be Meaningful

Names submitted during the certificate application process must be meaningful, unambiguous, and consistent with the identity information validated by the RA and/or CA, and must not imply identities or attributes that were not validated.

`C2PA` C2PA Claim Signing certificates are intended to identify a specific Conforming Generator Product. The certificate Subject is constructed to align with the corresponding identity record on the C2PA Conforming Products List (CPL) and must not imply identities or attributes beyond what was validated.

`CAWG` CAWG identity certificates are intended to identify the relevant CAWG identity subject per the applicable CAWG trust model and certificate profile. The certificate Subject and any additional name-bearing fields must not imply identities or attributes beyond what was validated.

Detailed Subject and SAN construction rules (including any ecosystem-specific name semantics) are specified in §7.5.1.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymous or pseudonymous certificates are not issued under this CP/CPS.

`C2PA` C2PA Claim Signing end-entity certificates are not intended to uniquely identify a particular Generator Product instance. Accordingly, the Subject DN identifies the Generator Product (as represented by its CPL record) and does not embed per-instance identifiers such as a unique device serial number.

3.1.4 Rules for Interpreting Various Name Forms

Relying parties and internal systems interpret names using standard X.509/X.501 semantics and ASN.1 syntax. For operational purposes (including logging and diagnostics), DNs may be rendered using a conventional string form (e.g., RFC 4514). Such rendering is for presentation only and does not alter the underlying encoded DN.

3.1.5 Uniqueness of Names

C2PA Multiple C2PA Claim Signing certificates may be issued with the same Subject DN to support multiple instances or deployments of a single Conforming Generator Product. In such cases, the Subject DN identifies the Generator Product (via the CPL identity) rather than a unique instance.

CAWG CAWG identity certificates require that the full combination of Subject attributes together with any additional identifying attributes specified by the applicable CAWG certificate profile is unique among active (non-revoked) certificates issued by TCA for the applicable certificate type.

3.1.6 Recognition, Authentication, and Role of Trademarks

Where a certificate request includes trademarks, trade names, or logotypes, the Applicant is required to provide documentation supporting its right to use the asserted mark. TCA and/or the RA validates such requests in order to avoid enabling misleading representations to relying parties.

Where supported by the applicable profile, logotype information may be conveyed using mechanisms defined in RFC 9399. For both C2PA and CAWG contexts, relying party display of any trademark or logotype is subject to the relying party's trust evaluation.

3.2 Initial Identity Validation

TCA and/or the RA may use lawful means of communication and investigation to ascertain the identity of an Applicant, and may refuse to issue a certificate where requirements are not satisfied.

For C2PA issuance, identity-validation evidence is captured through documented Organization Validation (OV) and Product Validation (PV) submissions. TCA personnel authorized to perform RA functions SHALL review submitted materials, SHALL record review outcomes, and SHALL approve or reject submissions in accordance with this CP/CPS and applicable program requirements.

C2PA At a minimum, PV submissions SHALL include product identity and conformance information (including product name, CPL `record_id`, applicable assurance level, and applicable specification version), security and implementation information required by policy, representative attestations, and supporting evidence required for review.

For each PV submission, TCA and/or the RA SHALL record a review decision (approval or rejection) together with review notes sufficient for auditability and repeatability of issuance decisions.

Only approved PV records are eligible for issuance authorization, and issuance SHALL be bound to the validated product identity and validated assurance level represented by the approved PV record.

For Level 2 requests, PV review SHALL include verification of device-attestation evidence and verification that key generation and key protection controls satisfy applicable Level 2 hardware-protected environment requirements.

TCA retains Initial Identity Validation (IIV) records (including organizational identity

validation evidence, authorized representative authentication evidence, and C2PA generator product validation evidence where applicable) for at least one (1) year after expiry of all certificates issued in reliance on the IIV.

TCA notifies the Applicant's representative of the outcome of the IIV process in accordance with the timelines described in §4.

All certificate requests establish possession of the private key related to the request and are verified at the level of assurance appropriate to the certificate type requested (including C2PA Claim Signing, CAWG identity certificates, and timestamping (TS) certificates where applicable). TCA and/or the RA inspects documents relied upon for verification for signs of alteration or falsification. Any compromise in the integrity of verification evidence or material misrepresentation of Applicant identity constitutes grounds for refusal of certificate issuance.

3.2.1 Method to Prove Possession of Private Key

An Applicant proves possession of the private key corresponding to the public key to be certified by submitting a Certificate Signing Request (CSR) signed by that private key, in accordance with PKCS #10, or by using an equivalent proof-of-possession mechanism supported by TCA.

3.2.2 Authentication of Organization Identity

Where a certificate request includes an organization identity, TCA and/or the RA verifies the Applicant organization.

Organization identity may be verified using documentation and/or evidence from one or more reliable sources, which may include: (i) a government agency, incorporating agency, or registration agency in the jurisdiction of the Applicant's legal creation; (ii) reputable third-party business registries (including, where applicable, LEI-related sources); (iii) a site visit by TCA, the RA, or a qualified agent; and/or (iv) a professional attestation or comparable documentation.

At a minimum, OV submissions include legal identity and registration/location information (including legal name, registration jurisdiction/address details, and physical office details), together with organization identifiers and supporting documentation required by policy.

Upon approval, TCA records validated organization attributes for use in issuance authorization decisions. OV approval remains valid only for its approved validity period and is not relied upon for issuance after expiration.

C2PA C2PA claim-signing issuance additionally requires approved PV records. TCA and/or the RA verifies that the Generator Product exists on the C2PA Conforming Products List (CPL), verifies the applicable assurance level and conformance status, and verifies validated product information (including product name and CPL `record_id`) prior to CSR JWT issuance.

3.2.3 Authentication of Individual Identity (if applicable)

Where an individual's identity is validated as part of a certificate request (including for an Applicant's Representative), TCA and/or the RA verifies the individual's identity using

one or more reliable methods. Such methods may include validation of a government-issued photo ID (e.g., passport, driver's license, national ID, or equivalent) and a secure video communication with the individual.

C2PA When the OV submitter is not the authorized representative, representative signature is obtained through a separate signing process. A one-time signing token is issued with bounded lifetime, prior pending tokens for the organization are invalidated on resend, and signed terms/authorization attestations are recorded on the OV record. Where the representative email corresponds to an account, representative signing requires authenticated account login matching that email.

3.2.4 Non-verified Subscriber Information

Certificate fields and any associated published metadata do not include Subscriber information that has not been validated to the assurance level expected by relying parties. Where non-verified information is collected for operational purposes (e.g., contact information), it is not represented as an identity attribute in issued certificates.

TCA may issue test certificates that are not chained to production trust anchor(s). Such test certificates may be issued without validation of Subscriber information and are clearly indicated as being for testing purposes.

3.2.5 Validation of Authority

TCA and/or the RA verifies that the Applicant's Representative is authorized to request issuance and revocation and to bind the Applicant to the Subscriber Agreement and related terms. As part of this validation, TCA may initiate contact (by phone or email) using a publicly discoverable organization contact channel in order to confirm the Representative's authority.

C2PA For RA-integrated C2PA issuance, authority to register, list, and revoke instance credentials is enforced through account-authenticated endpoints requiring activated accounts with MFA-verified session tokens and organization-level permissions. CSR JWT issuance itself is machine-authenticated by client assertion signed with a registered instance credential (no API key or Bearer token on the CSR JWT endpoint).

C2PA For RA-integrated C2PA issuance, CSR JWT issuance additionally enforces active service/subscription and validation gates (including approved PV and approved, non-expired OV) before authorization material is issued for CA enrollment.

3.2.6 Criteria for Interoperation / Delegated RA

TCA does not delegate RA functions to external entities. If TCA delegates RA functions in the future, the delegated RA will be contractually bound to follow this CP/CPS and applicable program requirements, and TCA will maintain oversight, auditability, and the ability to revoke delegated privileges.

3.2.7 Validation of Software and Hardware

C2PA For C2PA claim signing issuance, TCA validates the Generator Product identity and conformance status in addition to validating the Applicant organization and authen-

ticating the authorized representative.

Generator product validation confirms that the generator product information provided by the Applicant matches the official C2PA Conforming Products List (CPL) record, including the product name, the CPL record identifier, and the applicable C2PA specification version.

For Level 1 generator products, generator product validation includes collection of an attestation by an authorized representative that (i) the product has passed the C2PA conformance program and the CPL record is accurate, (ii) the product implementation is faithful to the security architecture documentation submitted to the C2PA program, and (iii) the product satisfies applicable C2PA Level 1 security and correctness requirements.

For Level 2 generator products, generator product validation additionally requires evidence required by the applicable C2PA Level 2 requirements, including device-attestation evidence and evidence that key generation and key protection controls satisfy the applicable hardware-protected environment requirements.

TCA may require submission of supporting documentation, including a copy of the Applicant's C2PA conformance application, as part of generator product validation.

Where the Applicant intends to use automated enrollment, TCA confirms that the generator product can be configured to send and receive enrollment messages in the required format(s).

3.3 Identification and Authentication for Renewal Requests

For renewal requests, the requestor is authenticated and TCA determines whether identity re-validation is required. For C2PA RA-integrated issuance, renewal-equivalent requests are gated by active authorization checks at CSR JWT issuance time (including approved PV/OV state and OV expiration checks).

Automated renewal-equivalent issuance uses EST `simpleenroll` with fresh short-lived authorization material rather than a separate `simplereenroll` endpoint.

3.4 Identification and Authentication for Re-key Requests

Re-key requests are not supported under this CP/CPS. Where a change of key material is required, TCA uses key rotation procedures (i.e., issuance of a new certificate under the applicable issuance process) rather than in-place re-keying.

3.5 Identification and Authentication for Revocation Requests

Revocation requests are authenticated using an appropriate method based on the request context and the Subscriber's validated identity and authority.

For revocation requests where the Subscriber's IIV has expired (for example, where key compromise is discovered after the IIV has lapsed), TCA takes appropriate steps to authenticate the request and processes the revocation in a timely manner.

4 Certificate Life Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

C2PA A certificate application may be submitted by the Subscriber organization associated with a Conforming Generator Product, or by an authorized representative acting on behalf of that organization. Requests are limited to parties authorized to act for the Applicant organization (including, where applicable, an approved delegated RA).

CAWG For CAWG identity certificates, permitted Applicants and authorized representatives are determined by the applicable CAWG trust model and certificate profile. During interim operation, TCA evaluates CAWG identity certificate applications on a case-by-case basis.

4.1.2 Enrollment Process and Responsibilities

Enrollment includes the following steps, in no particular order:

- The Applicant submits an application for Initial Identity Validation (IIV). Requirements specific to the requested certificate type (e.g., C2PA and CAWG) must be followed.
- The Subscriber pays applicable fees to the CA.
- The Subscriber accepts the Subscriber Agreement and applicable Terms of Service.
- Upon successful validation and authorization, the RA issues a short-lived provisioning JWT for automated enrollment.
- The Subscriber may enroll via a manual web portal flow or via an EST endpoint.

The provisioning secret is confidential JWT authentication material for EST enrollment and must be protected by the Subscriber. For RA-integrated C2PA flows, the JWT is generated by RA and presented to CA EST using HTTP Basic authentication (password field).

For non-test EST endpoints, provisioning JWTs are one-time use via JTI consumption. Subscribers should delete provisioning material promptly after successful enrollment.

If a provisioning secret is lost prior to use, the Subscriber requests re-issuance through an authenticated support channel. The TCA invalidates the prior provisioning secret and issues a replacement provisioning secret after confirming the requestor's authorization and that the applicable identity validation remains valid.

If a provisioning secret is suspected or confirmed to be compromised, the Subscriber must promptly notify the TCA. The TCA invalidates the provisioning secret and conducts a security assessment. Where a certificate may have been issued based on compromised authentication material, TCA evaluates whether revocation is required in accordance with §4.9.

For automated enrollment via EST (direct), issuance proceeds as follows:

- The Subscriber generates a key pair. For Level 2 issuance, the Subscriber generates and protects the key material in a secure manner consistent with applicable

assurance level requirements.

- The Subscriber obtains a short-lived CSR JWT from RA after RA authorization checks.
- The Subscriber submits a CSR via EST enrollment (`simpleenroll`), authenticated using the provisioning JWT.
- The CA validates JWT signature and claims, validates leaf type/path alignment, and validates the CSR and proof of possession.
- For production endpoints, the CA consumes the JWT JTI to enforce one-time use.
- The CA infers applicable issuance context (including product and instance context, where present) from the authenticated JWT claims.
- The Subscriber deletes the provisioning secret.
- For subsequent certificates (including renewals), the Subscriber repeats RA authorization and submits a new `simpleenroll` request with fresh JWT authorization material.

For RA-integrated C2PA enrollment, CSR JWT issuance proceeds through the following controls:

- The instance signs a `client_assertion` JWT using a registered instance credential key.
- RA verifies assertion signature, audience, expiry, issuer/subject consistency, and credential revocation state.
- RA enforces service and validation gates (including subscription status, product validation status, and organization validation status/expiry).
- RA issues an HS256 CSR JWT containing issuance claims used by CA EST enrollment.

The canonical RA endpoint for C2PA CSR JWT issuance is `/ra/c2pa/csr-jwt`.

The TCA's EST certificate lifecycle endpoints are served over HTTPS at https://ca.trufo.ai. For C2PA claim signing issuance, the following endpoints are supported:

Operation	Path	Method	Description
CA Certificates	`/.well-known/est/{leaf_type}/cacerts`	GET	CA certificates for path construction (where supported)
Enrollment	`/.well-known/est/{leaf_type}/simpleenroll`	POST	Issuance request (CSR + authentication material, as applicable)

For Subscriber leaf certificates, renewal requests are treated as new certificate requests. Use of a new key pair for renewal is strongly encouraged and same-key renewal is strongly discouraged.

CAWG interim and CTSA leaf types are also supported through leaf-type EST enrollment endpoints when authorized JWT enrollment material is provided by the applicable RA workflow.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

During certificate application processing, TCA verifies that the contents of the Certificate Signing Request (CSR), including relevant X.509 fields, match what was approved as part of the Applicant's Initial Identity Validation (IIV).

4.2.2 Approval or Rejection of Certificate Applications

If the Applicant's Initial Identity Validation (IIV) is not expired and the CSR passes all required checks, TCA issues the requested certificate.

TCA reserves the right to reject any CSR if TCA suspects (i) foul play by a third-party bad actor, (ii) a violation of applicable subscriber policy, or (iii) circumstances that would harm TCA's reputation or business interests.

4.2.3 Time to Process Certificate Applications

TCA typically completes Initial Identity Validation (IIV) and notifies the Applicant's representative of the outcome within five (5) business days, provided the Subscriber has all required documentation available. Additional time may be required where provisioning secret dissemination is complex due to the nature of the C2PA Generator Product or CAWG entity, and where additional auditing of C2PA Generator Product requirements is required.

Manual enrollment for C2PA claim signing and CAWG identity certificates typically completes within forty-eight (48) hours. Automated enrollment via EST is processed in real time.

Manual enrollment for timestamping (TSA) certificates typically completes within seventy-two (72) hours.

Unforeseen events may delay processing.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

During certificate issuance, TCA checks that the CSR contents match the certificate profile and that the request is authorized in accordance with the applicable enrollment mechanism.

C2PA For C2PA claim signing issuance, TCA performs any required audits of the Generator Product based on the applicable assurance level requirements, as applicable to the Subscriber's Generator Product.

4.3.2 Notification to Subscriber of Issuance

For manual issuance workflows, the issued certificate is delivered to the Subscriber via a secure communication channel.

For automated issuance workflows, the issued certificate is delivered to the Subscriber as

the response to the EST enrollment request.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

For manual issuance workflows, certificate acceptance is assumed after forty-eight (48) hours. Subscribers are solely responsible for installing issued certificates.

For automated issuance workflows, acceptance is indicated by successful completion of the EST enrollment transaction.

4.4.2 Publication of the Certificate by the CA

The TCA does not publish Subscriber (leaf) certificates in a general-access directory.

The TCA provides the Subscriber certificate to the Subscriber as part of issuance. Relying parties are expected to receive the leaf certificate (and any applicable chain) via the signed object or other application-level distribution.

The TCA publishes and operates the artifacts and services needed for validation, including CA certificates (as applicable) and revocation/status information via OCSP, as described in §2 and §4.9–§4.10, and summarized in Appendix B.

Intermediate CA certificates are made available to relying parties via the AIA CA Issuers URL in issued certificates, and are also published via the CA certificate download URLs.

4.4.3 Notification of Certificate Issuance to Other Entities

TCA may notify other relevant entities of certificate issuance as required by legal agreements or internal procedures. Any such notification is made in a secure manner based on the needs of the Subscriber and applicable operational requirements.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

`C2PA` C2PA claim signing certificates are used only for signing C2PA manifests on (or on behalf of) the Conforming Generator Product registered with C2PA conformance and operated by the Subscriber. The Subscriber is liable for misuse of certificates. Private key storage follows procedures submitted by the Subscriber as part of its conformance application.

`CAWG` CAWG identity certificates are used only for signing CAWG identity assertions. The Subscriber is liable for misuse of certificates. During interim operation, private keys are encrypted and/or stored in secure hardware.

4.5.2 Relying Party Public Key and Certificate Usage

Relying party signature validation behavior is driven by the applicable ecosystem (C2PA and/or CAWG) and the applicable certificate profile. Relying parties validate certificate

chains and perform applicable profile checks. Relying parties also perform revocation/status checking as described in §4.9 through §4.10.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

Renewal is allowed and expected as a certificate approaches expiration. The cadence of renewal should not materially differ from the certificate validity duration requested by the Subscriber.

For Subscriber leaf certificates, renewal requests are treated as new certificate requests. Use of a new key pair for renewal is strongly encouraged and same-key renewal is strongly discouraged. For automated issuance, renewal-equivalent requests are performed using EST `simpleenroll` with fresh authorization material.

Renewal is not used to change the Subject DN or other certificate information.

4.6.2 Who May Request Renewal

Only the certificate subject or an authorized representative of the certificate subject may request renewal. Requests are authenticated in accordance with the identification and authentication requirements described in §3.

4.6.3 Processing Renewal Requests

Renewal requests are processed by confirming that the Subscriber's Initial Identity Validation (IIV) has not expired, that the CSR includes the required proof-of-possession elements, and that the certificate information requested in the CSR matches what was approved.

4.6.4 Notification of New Certificate Issuance to Subscriber

Notification of renewal issuance follows the mechanisms described in §4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Conduct constituting acceptance of a renewal certificate follows §4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

Publication of a renewal certificate follows §4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of renewal issuance to entities other than the Subscriber follows §4.4.3.

4.7 Certificate Re-key

Re-key as a distinct operation is not supported under this CP/CPS.

Renewal requests are handled under the renewal workflow (§4.6) and are treated as new certificate requests. Use of a new key pair for renewal is strongly encouraged and same-key renewal is strongly discouraged.

Emergency key replacement (for example, in response to suspected compromise) follows the revocation process (§4.9) and is followed by a new initial registration.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Any changes to certificate information require a separate new Initial Identity Validation (IIV) process, except for correction of obvious errata (for example, a typographical error).

4.8.2 Who May Request Certificate Modification

Certificate modification is not supported under this CP/CPS except for correction of obvious errata (for example, a typographical error). The Subscriber or TCA may initiate a request for correction of such errata.

4.8.3 Processing Certificate Modification Requests

Upon receiving a request for modification, TCA determines whether the request is limited to correction of obvious errata. Requests that are not limited to obvious errata are not processed as "modification" and instead require a new issuance workflow, including a new IIV process as applicable.

Where a replacement certificate is issued to correct obvious errata, processing is performed in a manner consistent with the application processing and issuance requirements described in §4.2 and §4.3. The superseded certificate is revoked to reduce relying party confusion, and status is made available via the certificate status services.

4.8.4 Notification of New Certificate Issuance to Subscriber

If a modified (replacement) certificate is issued, TCA notifies the Subscriber using a secure communication channel appropriate to the enrollment method.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Acceptance of a modified (replacement) certificate follows the same conduct criteria as described in §4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

Publication of a modified (replacement) certificate follows the publication practices described in §4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Where applicable, notifications related to modification issuance to entities other than the Subscriber follow the practices described in §4.4.3.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

A certificate is revoked when the binding between the subject and the subject's public key is no longer considered valid.

Circumstances that may lead to revocation include:

- Identifying information or affiliation components of any names in the certificate becoming invalid.
- Privilege attributes asserted in the Subscriber's certificate being reduced.
- The Subscriber violating the stipulations of its Subscriber agreement.
- Reason to believe that the private key has been compromised.
- The Subscriber or another authorized party requesting revocation of the certificate.
- The certificate being determined to have been mis-issued or otherwise requiring revocation under applicable operational requirements.
- Revocation being directed by an applicable program authority where in scope.

When revocation occurs, the certificate status is made available via the certificate status services.

4.9.2 Who Can Request Revocation

The Subscriber (or an authorized representative), TCA (and/or its RA functions), and (where applicable) a program authority may request revocation of a certificate. TCA verifies the identity and authority of the entity requesting revocation to ensure that the request is legitimate and authorized.

4.9.3 Procedure for Revocation Request

Revocation requests are submitted via a manual process (for example, through a web portal or authenticated support channel). Automated revocation endpoints are not supported.

The revocation process generally follows these steps:

1. The requesting entity submits a revocation request identifying the certificate to be revoked and explaining the reason for the request.
2. TCA records the identity of the requesting entity and the reason for revocation.
3. Where applicable, TCA may request confirmation from the Subscriber or a known administrator using an out-of-band communication method.
4. Upon authentication and authorization of the request, TCA proceeds to revoke the certificate.

5. If the request originates from a third party, TCA investigates the request through established procedures to assess its validity.

TCA maintains the ability to respond to high-priority revocation requests.

4.9.4 Revocation Request Grace Period

Subscribers are required to request revocation as soon as possible after the need for revocation has been identified.

4.9.5 Time to Process Revocation Requests

TCA processes authenticated revocation requests as quickly as practical.

For revocation requests subject to applicable program requirements (for example, authenticated Subscriber-initiated requests), TCA completes revocation within seventy-two (72) hours of receiving a validated request.

For manual revocation requests, TCA typically processes the request within forty-eight (48) hours of receiving a validated request.

Following completion of a revocation action, certificate status information is updated via the certificate status services in accordance with §4.10.1.

4.9.6 Revocation Checking Requirements

C2PA Validator products must check certificate revocation status via OCSP. OCSP status information may be included in the C2PA manifest; otherwise, the validator uses the TCA OCSP endpoint, ideally with stapling where supported.

CAWG Validator products must check certificate revocation status via OCSP. Where OCSP status information is not otherwise available via the relying party's validation context, the validator uses the TCA OCSP endpoint, ideally with stapling where supported.

4.9.7 CRL Issuance Frequency (if applicable)

No stipulation.

4.9.8 Maximum Latency for CRLs (if applicable)

No stipulation.

4.9.9 On-line Revocation/Status Checking Availability

See §4.10.2.

4.9.10 On-line Revocation Checking Requirements

Validator products are required to check and display certificate validity.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements re Key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

No stipulation. Certificate suspension is not supported.

4.9.14 Who Can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The TCA operates a public OCSP endpoint. OCSP responses are signed using an OCSP responder certificate issued under the OCSP Signing CA subordinate to the Root CA.

Following completion of a revocation action, the data used to produce OCSP responses is updated within one (1) hour.

The TCA also operates a gated OCSP endpoint with SLA guarantees for validator products that sign applicable usage agreements.

4.10.2 Service Availability

The public OCSP endpoint is rate-limited and is provided with a 99% service level agreement (SLA).

The gated OCSP endpoint is provided with a 99.99% service level agreement (SLA).

4.10.3 Operational Features

No stipulation.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

No stipulation. TCA does not provide private key escrow or recovery for Subscriber private keys.

5 Facility, Management, and Operational Controls

This section details the physical, procedural, and personnel controls necessary to safeguard CA operations and maintain PKI system integrity. Given TCA's cloud-based infrastructure, emphasis is on logical controls, access management, and procedural safeguards.

5.1 Physical Controls

Physical controls address site security, equipment protection, and environmental safeguards. For cloud-hosted PKI services, the cloud provider is responsible for data center physical security.

All CA private keys are stored in FIPS 140-2 Level 3 Hardware Security Modules (HSMs) via AWS Cloud. CA key material does not leave the HSM. Access to root CA key operations is highly procedural and is performed under documented controls.

C2PA For C2PA Level 2 Conforming Generator Products, claim signing keys are stored in a Hardware Protected Environment (for example, a TEE or HSM) with dynamic attestation and binary image authentication, in accordance with C2PA Generator Product Security v0.1.

5.2 Procedural Controls

Procedural controls define documented procedures, dual-control mechanisms, separation of duties, and change management processes for CA operations.

5.2.1 Trusted Roles

TCA defines and enforces logical separation of trusted roles. While an individual may hold more than one role, any two-party approval workflow requires two different individuals for the same operation.

Trusted roles include:

- Root CA (RCA) Initiator: initiates Root CA signing requests (MFA required).
- Root CA (RCA) Approver: approves Root CA signing requests (MFA required) and is distinct from the Initiator for any given operation.
- CA Administrator: manages Issuing CA operations (MFA required).
- CA Operator: performs Issuing CA signing via service account for leaf certificate issuance.
- TSA Operator: provides operational oversight of TSA servers (monitoring, availability, incident response); timestamp signing is automated.
- Auditor: read-only access to logs and certificates.

5.2.2 Number of Persons Required per Task (Dual Control)

TCA follows the two-person rule for sensitive operations involving keys that are not directly issuing leaf certificates. For root signing operations, the two key custodian roles

are the Initiator and the Approver.

No single individual has unilateral access to any non-leaf CA signing key. The signing of certain leaf certificates by Issuing CA certificates may be completed by an administrator in accordance with the applicable operational controls.

5.2.3 Identification and Authentication for Each Role

Personnel acting in trusted roles are authenticated using AWS SSO with named role profiles. Multi-factor authentication (MFA) is required for console and CLI access. Allowable MFA methods include passkey and TOTP.

TCA records role-based access and key-management operations in audit logs, including AWS CloudTrail records identifying actions by IAM identity.

5.2.4 Separation of Duties

TCA segregates root, issuing, and leaf operations into separate AWS accounts with separate IAM access. Sensitive operations are performed under the two-person rule.

For programmatic operations, TCA uses service accounts that are assigned minimum necessary permissions (least privilege). Service accounts do not directly access key material and may only invoke signing operations through approved APIs.

C2PA Conformance approval for Generator Products is not handled by TCA.

5.3 Personnel Controls

Personnel controls cover background checks, training, access control, and qualification requirements for trusted personnel.

TCA requires background checks and security training for personnel in trusted roles and enforces least-privilege access controls.

All personnel undergo background checks at hire and every five (5) years. Personnel with access to CA services are qualified in security and PKI concepts. Access to CA systems and data is granted on a need-to-know basis.

Trusted personnel who fail to comply with this CP/CPS are subject to internal administrative or disciplinary processes.

Independent contractors assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this section.

5.4 Audit Logging Procedures

TCA maintains audit logs of PKI events, including:

- PKI key generation and registration.
- Certificate requests and their results.
- Certificate issuance and renewal.
- Certificate revocation.
- System access attempts.

The date and time of these events are recorded, along with the responsible user or process as applicable.

TCA implements audit logging using AWS CloudTrail for KMS-related operations and a secure MongoDB log for each CA API call.

5.5 Records Archival

TCA archives CA records for at least one (1) year.

TCA retains AWS CloudTrail records for seven (7) years and retains records in its internal database for at least one (1) year.

5.6 Key Changeover

TCA performs key changeover using documented procedures intended to minimize disruption to Subscribers and relying parties.

Subscribers are notified of key retirement. More than one CA key and certificate may be active during a transition period, but only one is used for each distinct CA role.

Key changeover operations are recorded in audit logs, including AWS CloudTrail records retained for seven (7) years.

5.7 Compromise and Disaster Recovery

TCA maintains backups of critical CA system data. If TCA suspects that a CA private key has been compromised or lost, an incident response process is initiated to assess the degree and scope of the incident and determine appropriate action.

As applicable, affected PKI participants and other appropriate entities are notified. Where required to restore secure operations, TCA generates new key material and issues replacement certificates.

5.8 CA, RA, OCSP, or TSA Termination

TCA provides advance notification for termination of CA, RA, OCSP, or TSA services.

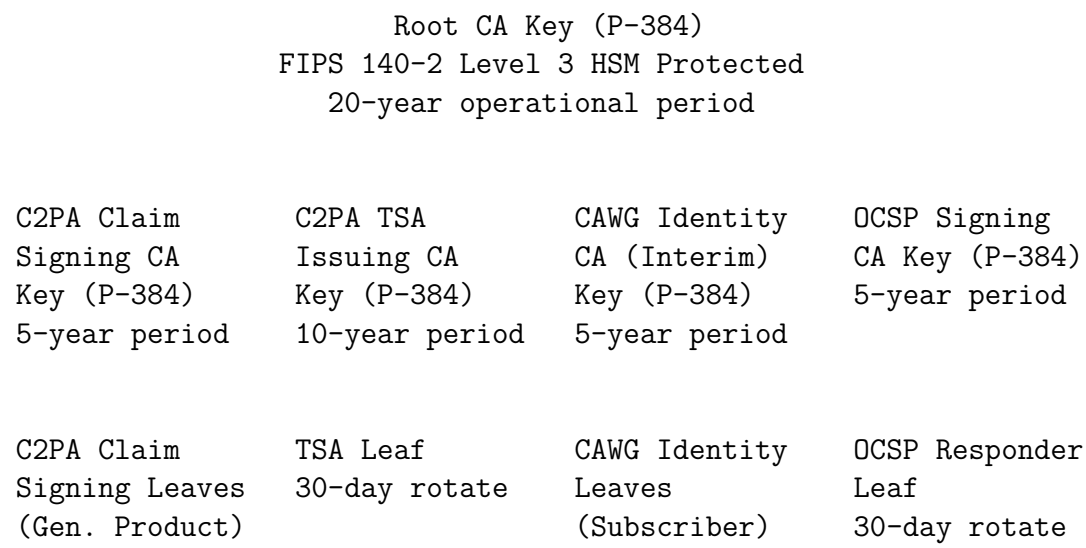
If OCSP service is terminated, TCA provides transition guidance for relying parties and replacement status service instructions as applicable. This PKI does not publish CRLs.

6 Technical Security Controls

This section details the technical measures and safeguards implemented to protect cryptographic keys and ensure the security of CA infrastructure, subscriber implementations, and TSA operations. TCA uses FIPS 140-2 Level 3 Hardware Security Modules (HSMs) for CA and TSA key operations.

6.1 Key Pair Generation and Installation

The following diagram provides a high-level overview of the PKI key hierarchy operated under this CP/CPS:



6.1.1 CA Key Pair Generation

CA key pairs are generated directly on FIPS 140-2 Level 3 Hardware Security Modules (HSMs). Root CA key generation is performed as a documented key generation ceremony using a written script with appropriate witnessing, evidence collection (including video recording), and approvals.

All CA keys use ECC P-384. Key generation events and related administrative actions are recorded in auditable logs. Issuance of any CA certificate follows a two-person approval process.

6.1.2 Subscriber Key Pair Generation

The TCA does not generate C2PA claim signing keys on behalf of subscribers. Subscribers are responsible for generating and protecting their claim signing keys. The TCA may provide a key management service; where used, such service is operated to support subscriber key management requirements.

Each subscriber key is used for a single purpose and is bound to a single certificate (or a sequence of renewals for that certificate) in accordance with applicable program requirements.

C2PA For C2PA Conforming Generator Products, claim signing key protection requirements vary by assurance level:

- Level 1 Server: software keystore with encryption at rest.
- Level 1 Distributed: software keystore with encryption at rest.
- Level 1 Edge: use of a secure enclave or Trusted Execution Environment (TEE) is recommended.
- Level 2 Server: FIPS 140-2 Level 2 HSM required.
- Level 2 Distributed: FIPS 140-2 Level 2 or a secure enclave required.
- Level 2 Edge: secure enclave or TEE with attestation required.

CAWG For CAWG interim requirements, subscriber keys are encrypted at rest or stored in secure hardware (aligning with C2PA Level 1 expectations).

6.1.3 Public Key Delivery to Certificate Issuer

Subscriber public keys are delivered to the certificate issuer via Certificate Signing Request (CSR), either through manual submission or via the applicable EST endpoint. Requests include proof of possession (PoP) for the corresponding private key and any required authentication material (for example, provisioning secrets, JWTs, or derived values) used to authorize the issuance request.

6.1.4 CA Public Key Delivery to Relying Parties

CA public keys are delivered to relying parties through publication of CA certificates (including the root CA certificate and any issuing CA certificates) in The TCA's certificate repository and other applicable trust lists or stores. Issuing CA certificates may also be provided via certificate chains and through AIA caIssuers references, as applicable.

6.1.5 Key Sizes and Algorithms

The TCA uses ECC P-384 for root and issuing CA key pairs with the corresponding SHA-384 signature algorithm. End-entity (leaf) certificates use ECC P-256 or P-384, with P-256 recommended, and the corresponding SHA-256 or SHA-384 signature algorithm.

OCSP responder certificates use ECC P-384 with ECDSA SHA-384 in this PKI, as summarized in Appendix A.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

All CA private keys are generated, stored, and used within cryptographic modules validated to FIPS 140-2 Level 3 (or higher), and the key material does not exist outside the module boundary in plaintext. TSA key protection requirements are described in §6.8.

For subscriber environments where assurance levels are defined (for example, "Level 2 Server"), FIPS 140-2 Level 2 HSMs are required where specified, and distributed or edge deployments follow the applicable program recommendations.

6.2.2 Multi-Person Control (n out of m)

TCA enforces multi-person control for sensitive CA key operations. The following activities require 2-of-2 multi-person control:

- Root CA key generation (key ceremony).
- Root CA certificate signing (approval workflow with distinct initiator and approver roles).
- Key deletion or destruction.

Issuing CA leaf certificate signing may be performed by a single authorized service account, with an auditable trail of all signing operations.

Trusted role definitions and separation of duties requirements are described in §5.

6.2.3 Private Key Escrow

Private key escrow is not supported.

6.2.4 Private Key Backup

TCA relies on the underlying redundancy and durability mechanisms of its managed HSM service for key material protection and availability. CA private keys remain non-exportable and are not backed up by exporting key material; instead, key material remains protected within cryptographic module boundaries and is preserved through the service's internal replication and recovery mechanisms. Administrative actions related to key lifecycle and access are subject to approval controls and are recorded in audit logs.

6.2.5 Private Key Archival

CA private keys are not archived. Upon retirement, CA keys are scheduled for deletion in accordance with key lifecycle procedures.

6.2.6 Private Key Transfer into or from Cryptographic Module

Private key transfer into or out of the cryptographic module is not supported or permitted. CA and TSA private keys are generated within cryptographic modules and are non-exportable.

6.2.7 Private Key Storage on Cryptographic Module

CA private keys are stored on FIPS 140-2 Level 3 cryptographic modules. Access to key management operations is protected by strong authentication, including multi-factor authentication (MFA), and is constrained by least-privilege authorization policies.

C2PA Where C2PA requirements call for higher assurance key storage (for example, Level 2 requirements for certain product classes), claim signing keys are stored in an appropriate hardware-protected environment (such as an HSM or equivalent) meeting the applicable assurance and protection requirements.

6.2.8 Method of Activating Private Key

The root CA private key is activated for signing only through a procedural, permissioned signing process that enforces multi-party approval.

Issuing CA private keys are activated through tightly controlled signing operations performed by authorized services. These services authenticate and authorize certificate requests, including verifying CSRs and proof of possession, prior to invoking any signing operation.

Subscribers are responsible for activation and protection of their own private keys.

6.2.9 Method of Deactivating Private Key

No stipulation.

6.2.10 Method of Destroying Private Key

CA private keys are destroyed by scheduling deletion through the managed cryptographic key service. Deletion is subject to approval controls (including multi-person control where required), is recorded in audit logs, and uses a configurable waiting period to mitigate accidental deletion. Once destroyed, the key material is irrecoverable.

6.2.11 Cryptographic Module Rating

Cryptographic modules used for CA and TSA key operations meet the requirements described in §6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

CA certificates (which contain CA public keys) are retained in the certificate repository to support relying party validation, including for certificates issued prior to CA retirement.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Certificate operational periods are set by the applicable certificate profiles (see §7 and Appendix A). In this PKI, the operational certificate validity periods are:

- Root CA: 20 years.
- C2PA Claim Signing Issuing CA: 5 years (1827 days).
- C2PA Timestamping Issuing CA: 10 years (3650 days).
- OCSP Signing CA: 5 years (1827 days).
- C2PA Claim Signing Leaf: Level 1 = up to 366 days; Level 2 = up to 90 days.
- CAWG Identity Leaf (Interim): up to 366 days.
- OCSP Responder: 30 days.
- TSA Leaf: up to 4110 days.

OCSP responder certificates are issued with a short validity period to reduce exposure if

an OCSP responder signing key is compromised. To avoid requiring frequent Root CA signing operations, OCSP responder certificates are issued by a dedicated OCSP Signing CA subordinate to the Root CA.

OCSP is not used for the Root CA certificate; relying parties treat the Root CA as a trust anchor and any Root CA trust status updates are distributed out-of-band.

Key pair usage periods do not exceed the corresponding certificate operational periods.

6.4 Activation Data

Administrative access to CA systems and key management functions requires multi-factor authentication (MFA). Allowable MFA methods include passkey and TOTP in addition to primary credentials.

Operational controls for granting and reviewing privileged access are described in §5.3.

6.5 Computer Security Controls

CA infrastructure is deployed in cloud environments using managed cryptographic services (HSM-backed key management), strong secrets management, and standard hardening practices appropriate for Internet-facing services.

Developer workstations used for sensitive development and operational tasks run up-to-date operating systems.

6.6 Life Cycle Technical Controls

TCA applies technical controls throughout the certificate lifecycle to protect the confidentiality, integrity, and availability of CA systems and certificate operations. Certificate issuance, renewal, and revocation operations require authenticated and authorized requests, and all security-relevant events are recorded in audit logs.

Certificate status information is made available through status services as described in this CP/CPS. Incident response procedures, monitoring, and recovery activities are coordinated with the operational controls described in §5.

6.7 Network Security Controls

All CA and TSA endpoints use HTTPS. Production systems do not permit direct SSH access. When sensitive functions are performed from developer devices (for example, administrative actions), those functions are performed over trusted networks with appropriate authentication and access controls.

6.8 Time-Stamping

TCA operates a Timestamping Authority (TSA) that is accessible through both public and gated endpoints.

TCA may issue TSA certificates to third-party TSAs. Where TSA operations are dele-

gated, TCA requires that delegated TSA operators meet the same technical key protection requirements, including the use of cryptographic modules meeting the applicable HSM assurance requirements.

TCA's TSA implementation follows RFC 3161 and uses FIPS 140-2 Level 3 cryptographic modules for TSA signing operations.

6.8.1 TSA Request Handling (RFC 3161)

TCA processes RFC 3161 timestamp requests by validating request structure and supported hash algorithms, applying abuse controls at the service boundary, and returning RFC 3161-compliant responses.

TCA only accepts timestamp requests using approved hash algorithms (SHA-256, SHA-384, and SHA-512). Requests may include a nonce, which is returned in the response when present. Timestamp responses are signed using TSA keys reserved exclusively for timestamping.

Timestamp requests are accepted over HTTPS using HTTP POST. The request content type is `application/timestamp-query` and the response content type is `application/timestamp-reply`.

Where the request indicates `certReq`, TCA includes the TSA certificate chain in the response as permitted by the protocol.

6.8.2 TSA Time Source and Accuracy Management

TCA maintains time values that are traceable to UTC, declares an intended accuracy, and monitors time synchronization quality. If detected drift exceeds the declared accuracy threshold, timestamp issuance is halted until the time source is restored to within acceptable bounds.

TCA maintains synchronization through reliable time synchronization mechanisms (for example, NTP-based synchronization), including appropriate handling of leap seconds.

6.8.3 TSA Key Management and Rotation

TCA TSA signing keys are reserved exclusively for timestamping operations, and TSA signing is performed using a controlled signing environment and keys protected by FIPS 140-2 Level 3 cryptographic modules.

TCA rotates TSA leaf keys in accordance with applicable key lifecycle, security, and operational requirements. Rotation is performed through controlled procedures executed from a secured operational environment with appropriate access controls and auditing. Prior TSA certificates and chains remain available to support verification of previously issued timestamps.

6.8.4 Delegated TSA Operator Requirements

Where TSA operations are delegated, delegated TSA operators are required to meet the same technical requirements described in this section, including at minimum:

- RFC 3161-compliant request handling and response generation.

- Approved hash algorithm support (SHA-256, SHA-384, SHA-512).
- Time source traceability to UTC and declared accuracy monitoring.
- Use of cryptographic modules meeting the required assurance level for TSA signing keys.
- Exclusive use of TSA signing keys for timestamping, with controlled access and auditable key usage.
- Security monitoring, incident response, and operational logging.

Delegated operators are also required to meet the baseline delegated operator security requirements in §6.9.

6.9 Delegated Operator Security Requirements

Where CA, RA, or TSA functions are delegated, delegated operators are required to meet equivalent security controls and compliance obligations as required by this CP/CPS. At minimum, delegated operators are required to maintain:

- Equivalent cryptographic module assurance levels for key generation, storage, and signing.
- Strong access controls (including MFA where applicable), least-privilege authorization, and separation of duties.
- Audit logging and record retention sufficient to support compliance and incident investigations.
- Security monitoring and incident response procedures aligned to this CP/CPS.
- Controls ensuring the confidentiality and integrity of subscriber and operational data.

These baseline requirements are supplemented by the applicable operational controls in §5, by the relevant technical controls in §6, and by the applicable certificate profiles in §7.

TCA may allow third-party TSA operators in accordance with the requirements in §6.8.4.

7 Certificate, CRL, and OCSP Profiles

This section defines the technical structure of all certificates, CRLs, and OCSP responses issued within this PKI hierarchy. It specifies the X.509 v3 extensions, key usages, policy OIDs, and other fields required for each certificate type.

7.1 Certificate Profile Overview

This PKI uses a single Root CA to sign one or more Issuing CAs (including C2PA Claim Signing, C2PA Timestamping, and CAWG Identity Issuing CAs). Issuing CAs issue end-entity (leaf) certificates for their intended purposes.

All certificates are X.509 v3. Certificate signing uses ECDSA, with CA certificates using stronger CA-level key sizes (for example, P-384) and leaf certificates permitting leaf-appropriate curves (for example, P-256 where applicable).

Appendix A provides a consolidated profile matrix.

7.2 Root CA Certificate Profile

Root CA certificates are self-signed, with the Subject matching the Issuer. Root CA Distinguished Names (DNs) include, at minimum, Country (C), Organization (O), and Common Name (CN).

Root CA certificates have an operational validity of approximately twenty (20) years. Root CA keys use ECDSA P-384. Root CA certificates assert `keyCertSign` and `cRLSign` key usages (critical) and include a Basic Constraints extension with cA=TRUE and a constrained path length (critical).

Root CA certificates include Subject Key Identifier (SKI) and Authority Key Identifier (AKI) in accordance with RFC 5280 conventions (with AKI corresponding to SKI). Root CA certificates do not include AIA or CDP extensions. Certificate Policies may be present as applicable.

7.3 Issuing CA Certificate Profiles

7.3.1 C2PA Claim Signing Issuing CA Profile

C2PA Claim Signing Issuing CA certificates are constrained intermediates used to issue C2PA claim signing leaf certificates. Issuing CA certificates have an operational validity of up to five (5) years.

Issuing CA keys use ECDSA P-384. Issuing CA certificates assert `keyCertSign` and `cRLSign` key usages (critical) and include Basic Constraints with cA=TRUE and pathLenConstraint=0 (critical).

Issuing CA certificates include the C2PA claim signing EKU and include the applicable Certificate Policies OID required for this hierarchy.

Issuing CA certificates include AIA with an OCSP responder URL and a CA Issuers URL, as described in this CP/CPS.

7.3.2 C2PA Timestamping Issuing CA Profile

C2PA Timestamping Issuing CA certificates are constrained intermediates used to issue TSA leaf certificates. Operational validity is configured for up to ten (10) years.

Timestamping Issuing CA keys use ECDSA P-384. Timestamping Issuing CA certificates assert `keyCertSign` and `cRLSign` key usages (critical) and include Basic Constraints with cA=TRUE and pathLenConstraint=0 (critical).

Timestamping Issuing CA certificates include an EKU constrained to `id-kp-timeStamping` and include the applicable Certificate Policies OID required for this hierarchy.

Timestamping Issuing CA certificates include AIA with an OCSP responder URL and a CA Issuers URL, as described in this CP/CPS.

7.3.3 CAWG Identity Issuing CA Profile (if applicable)

CAWG Identity Issuing CA certificates are an interim constrained profile used to issue CAWG identity leaf certificates until formal CAWG CA requirements are finalized. Operational validity is up to five (5) years.

The CAWG Identity Issuing CA certificate profile is based on C2PA conventions and uses EKU and policy constraints appropriate to CAWG identity usage.

7.4 End-Entity Certificate Profiles

7.4.1 C2PA Claim Signing Leaf Profile(s)

C2PA claim signing leaf certificates are end-entity certificates used for signing C2PA claims. Operational validity periods follow the applicable profiles (Level 1: up to 366 days; Level 2: up to 90 days).

Leaf certificate keys use ECDSA P-256 or P-384. Leaf certificates assert `digitalSignature` and `nonRepudiation` key usages (critical).

Leaf certificates include the C2PA claim signing EKU and the applicable Certificate Policies OID required for this hierarchy. Where applicable, leaf certificates include required C2PA extensions conveying CPL record and assurance level.

Leaf certificates include AIA with an OCSP responder URL and a CA Issuers URL, as described in this CP/CPS.

7.4.2 TSA Leaf Profile

TSA leaf certificates are end-entity certificates used exclusively for RFC 3161 timestamping. TSA leaf certificates have a maximum operational validity of up to 4110 days, as described in §6.

TSA leaf keys use ECDSA P-256 or P-384. TSA leaf certificates assert `digitalSignature` and `nonRepudiation` key usages (critical).

TSA leaf certificates include an EKU constrained to `id-kp-timeStamping` (critical) and include the applicable Certificate Policies OID required for this hierarchy.

TSA leaf certificates include AIA with an OCSP responder URL and a CA Issuers URL,

as described in this CP/CPS.

7.4.3 OCSP Responder Certificate Profile

OCSP responder certificates are used to sign OCSP responses. OCSP responder certificates include `id-kp-OCSPSigning` EKU and assert `digitalSignature` key usage.

OCSP responder certificates are issued by an OCSP Signing CA subordinate to the Root CA.

OCSP responder certificates have short operational validity and are used to support timely revocation status information.

7.4.4 CAWG Identity Leaf Profile

CAWG identity leaf certificates are end-entity certificates used for signing CAWG identity assertions. CAWG identity leaf certificates include `id-kp-documentSigning` EKU and are used with a COSE signature format where `sig_type` indicates the CAWG X.509 COSE signing mode.

Where supported by the applicable profile, CAWG identity leaf certificates may include logotype information (e.g., per RFC 9399) to support relying party display decisions.

7.5 Certificate Extensions (Common Requirements)

7.5.1 Subject / SAN / Name Constraints

All certificates include a Subject DN with, at minimum, Country (C), Organization (O), and Common Name (CN). Subject Alternative Name (SAN) entries may be included where required by the applicable certificate profile.

Issuing CAs MAY include `nameConstraints` to restrict the scope of names that can appear in certificates issued under that Issuing CA.

7.5.2 Key Usage / EKU

Key Usage and Extended Key Usage (EKU) are constrained by certificate type:

- CA certificates assert `keyCertSign` and `cRLSign` (critical).
- C2PA claim signing leaf certificates assert `digitalSignature` and `nonRepudiation` (critical) and include the C2PA claim signing EKU together with the applicable supporting EKU.
- TSA leaf certificates assert `digitalSignature` and `nonRepudiation` (critical) and include `id-kp-timeStamping` EKU (critical).
- OCSP responder certificates assert `digitalSignature` and include `id-kp-OCSPSigning` EKU.
- CAWG identity certificates assert `digitalSignature` and include `id-kp-documentSigning` EKU.

7.5.3 Certificate Policies

Certificates issued under this hierarchy include the applicable certificate policy identifier(s). The C2PA certificate policy OID is `1.3.6.1.4.1.62558.1.1`.

This CP/CPS is identified by policy OID `1.3.6.1.4.1.62524.1.1` and is published at https://trufo.ai/cpcps.

7.5.4 AIA / CDP Requirements

Root CA certificates do not include Authority Information Access (AIA) or CRL Distribution Points (CDP/CRLDP) extensions.

Issuing CA certificates and leaf certificates include AIA information sufficient for relying parties to locate (i) the OCSP responder and (ii) the issuing CA certificate(s) (via a CA Issuers URL). CRL Distribution Points (CDP/CRLDP) are not used in this PKI.

7.6 CRL Profile (if applicable)

Not applicable. This PKI does not publish Certificate Revocation Lists (CRLs). Revocation status information is provided via OCSP.

7.7 OCSP Profile

OCSP responses are provided in accordance with RFC 6960. Where applicable, a lightweight OCSP profile may be supported.

OCSP responses are signed by an OCSP responder certificate (or delegated responder, where used). Nonce handling is optional. OCSP responses are issued with a defined freshness window appropriate for relying party validation.

7.8 Delegated Operator Profile Constraints

Currently, certificates issued to delegated operators are limited to leaf certificates only. Issuing CA certificates are not delegated.

8 Compliance Audit and Other Assessments

This section covers the audit and assessment requirements for the CA, TSA, and any delegated operators. Compliance audits ensure ongoing adherence to this CP/CPS and applicable program requirements.

8.1 Frequency and Circumstances of Assessment

TCA may perform or commission assessments from time to time. No stipulation.

Assessments may be triggered in response to events such as security incidents, suspected compromise of key material, significant changes to infrastructure or controls, or onboarding of a new delegated operator.

8.2 Self-Audits

TCA may conduct internal reviews from time to time. No stipulation.

8.3 Delegated Operator Assessments

Delegated operators may be required to demonstrate compliance with applicable requirements prior to receiving certificates, and may be subject to ongoing assessment as specified in the applicable agreement. Non-compliance may result in certificate revocation or termination of the delegated operator relationship.

Currently, certificates issued to delegated operators are limited to leaf certificates.

C2PA Where delegated operators receive C2PA claim signing leaf certificates, delegated operators may be assessed against the applicable C2PA assurance-level security requirements for subscriber key generation and protection (including Level 1 and Level 2 requirements), as described in §6.1.2.

8.4 Topics Covered by Assessment

No stipulation.

8.5 Actions Taken as a Result of Deficiency

No stipulation.

8.6 Communications of Results

No stipulation.

9 Other Business and Legal Matters

This section covers the business, legal, and administrative framework governing the PKI. It addresses fees, liability, confidentiality, privacy, and the legal relationship between TCA and all PKI participants.

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Subscribers may be charged a fee for the issuance, management, renewal, and related administration of certificates under this CP/CPS, as specified in the applicable subscriber agreement.

9.1.2 Certificate Access Fees

TCA must not charge a fee as a condition of making a certificate available in a repository or otherwise making certificates available to relying parties.

9.1.3 Revocation or Status Information Access Fees

TCA must not charge a fee as a condition of providing access to certificate status information (including OCSP responses).

9.1.4 Fees for Other Services (if Applicable)

TCA may offer optional services subject to additional fees as specified by agreement. Such services may include access to gated (authenticated) OCSP and/or TSA endpoints and professional services or consultation related to integration, conformance preparation, or operational support.

9.1.5 Refund Policy

Refund policies, if any, are stipulated in the applicable subscriber agreement.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

PKI participants should maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or through a self-insured retention, as applicable.

9.2.2 Other Assets

TCA must maintain sufficient financial resources to maintain its operations and perform its duties, and must be reasonably able to bear the risk of liability to subscribers and relying parties.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following subscriber information is considered confidential:

- Certificate application records.
- Personal or other non-public information about subscribers.
- Transactional records (including full records and audit trails of transactions).
- Security measures controlling the operations of CA hardware and software.

9.3.2 Information Not within the Scope of Confidential Information

Certificates, certificate revocation and other status information, and repositories and information contained within them, are not considered confidential.

9.3.3 Responsibility to Protect Confidential Information

PKI participants receiving confidential information must secure it from compromise and disclosure to third parties.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

No stipulation.

9.4.2 Information Treated as Private

TCA protects subscribers' personally identifying information from unauthorized disclosure. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archives maintained by TCA must not be released except as required by law.

9.4.3 Information Not Deemed Private

Information included in certificates is public information and is not afforded privacy protections.

9.4.4 Responsibility to Protect Private Information

Sensitive information is stored securely and may be released only as required by law.

9.4.5 Notice and Consent to Use Private Information

The policy authority and/or TCA is not required to provide notice or obtain consent of the subscriber to release private information.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The policy authority and/or TCA must not disclose private information to any third party unless authorized by this CP/CPS, required by law, required by government rule or regulation, or required by order of a court of competent jurisdiction.

9.4.7 Other Information Disclosure Circumstances

Not applicable.

9.5 Intellectual Property Rights

TCA retains all intellectual property rights in and to the certificates and revocation/status information that it issues.

A certificate applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any certificate application and in any Distinguished Name (DN) within any certificate issued to that applicant.

Private keys corresponding to certificates of CAs and subscribers are the property of the CAs and subscribers that are the respective Subjects of those certificates.

Without limiting the generality of the foregoing, root public keys and certificates containing them, including CA and subscriber public keys and certificates containing them, are the property of TCA. TCA may license software and hardware manufacturers to reproduce such public key certificates for placement in compliant devices or software.

9.6 Representations and Warranties

The policy authority must:

- Approve the CPS for each CA that issues certificates under this CP/CPS.
- Review periodic audits to ensure that CAs are operating in compliance with their approved CP/CPS.
- Review name space control procedures to ensure that DNs are uniquely assigned for all certificates issued under this CP/CPS.
- Revise this CP/CPS to maintain the level of assurance and operational practicality and publicly distribute this CP/CPS.
- Coordinate modifications to this CP/CPS to ensure continued compliance by entities operating under approved practices.

9.6.1 CA Representations and Warranties

TCA warrants that:

- CA procedures are implemented in accordance with this CP/CPS.
- Certificates issued are issued in accordance with the stipulations of this CP/CPS.
- There are no material misrepresentations of fact in a certificate known to or originating from the entities approving the certificate application or issuing the certificate.
- There are no errors in the information in a certificate introduced by entities approving the certificate application due to failure to exercise reasonable care in managing the application.
- Revocation services (when applicable) and use of a repository conform to all material requirements of this CP/CPS in all material respects.

9.6.2 RA Representations and Warranties

To the extent permitted by applicable law, TCA disclaims any warranties, including any warranty of merchantability or fitness for a particular purpose.

9.6.3 Subscriber (and Related Parties) Representations and Warranties

Subscribers must sign an agreement containing the requirements the subscriber must meet, including protection of private keys and use of certificates, before certificates are issued. In addition, subscribers warrant that:

- The subscriber will abide by all terms, conditions, and restrictions levied on the use of private keys and certificates.
- Each digital signature created using the private key corresponding to the public key listed in the certificate is the digital signature of the subscriber and the certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created.
- Subscriber private keys are protected from unauthorized use or disclosure.
- All representations made by the subscriber in the certificate application are true.
- All information supplied by the subscriber and contained in the certificate is true.
- Certificates are used exclusively for authorized and legal purposes, consistent with all material requirements of this CP/CPS.
- The subscriber will promptly notify TCA upon suspicion of loss or compromise of private key(s).
- The subscriber is an end-entity subscriber and is not using the private key corresponding to any public key listed in a certificate for purposes of digitally signing any certificate (or any other certified public key) or revocation status object as a CA.

Where a subscriber operates or controls C2PA Conforming Generator Products and/or is associated with CAWG identity profiles that rely on certificates issued under this CP/CPS, the subscriber warrants that such products and related implementations are operated and used in a manner consistent with the requirements outlined in this CP/CPS and any applicable program requirements.

Subscriber agreements may include additional representations and warranties.

9.6.4 Relying Party Representations and Warranties

This CP/CPS does not specify the steps a relying party must take to determine whether to rely upon a certificate. The relying party determines, pursuant to its own policies, what steps to take. TCA provides certificates and status information needed to support path construction, validation, and any CP mappings that the relying party may choose to employ.

Relying parties acknowledge that they have sufficient information to make their own reliance decisions, that reliance decisions are made at their discretion, and that they bear responsibility for the consequences of reliance decisions, including any failure to perform relying party obligations.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, subscriber agreements disclaim TCA's and the applicable subscriber's possible implied warranties, including any warranty of merchantability or fitness for a particular purpose.

9.8 Limitations of Liability

Liability (and any limitation of liability) of subscribers is as set forth in the applicable subscriber agreements.

9.9 Indemnities

To the extent permitted by applicable law, subscribers are required to indemnify TCA for:

- Falsehood or misrepresentation of fact by the subscriber on a certificate application.
- Failure by the subscriber to disclose a material fact on a certificate application, if the misrepresentation or omission was made negligently or with intent to deceive any party.
- Failure by the subscriber to take precautions necessary to prevent compromise, loss, disclosure, modification, or unauthorized use of the subscriber's private key(s) or a certificate.

Subscriber shall: (i) promptly remediate any product that does not conform to the requirements outlined in this CP/CPS upon notice from TCA; and (ii) indemnify TCA for actual damages arising from Subscriber's failure to timely remediate. TCA may revoke certificates for non-conforming products.

- The subscriber's use of a name, including any use that infringes upon the intellectual property rights of a third party.

9.10 Term and Termination

9.10.1 Term

This CP/CPS becomes effective when approved by the policy authority. Amendments to this CP/CPS become effective upon publication. This CP/CPS has no specified term.

9.10.2 Termination

This CP/CPS, as amended from time to time, remains in force until it is replaced by a new version. Termination of this CP/CPS is at the discretion of the policy authority.

9.10.3 Effect of Termination and Survival

Upon termination of this CP/CPS, PKI participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, PKI participants use commercially reasonable methods to communicate with each other, considering the criticality and subject matter of the communication.

9.12 Amendments

The policy authority reviews this CP/CPS at least annually.

Amendments are categorized per Appendix D.3 (Editorial, Minor, Major, Critical) with corresponding review and notification requirements:

- Editorial and Minor changes may be made without subscriber notification.
- Major changes require review by the policy authority and the applicable C2PA conformance administrator, and notice is posted to the repository.
- Critical changes require full governance review and direct notification to subscribers.

An OID change is required only if the policy authority determines that a policy change requires a new OID. Otherwise, amendments do not require changes to policy OIDs.

A Certificate Profile Quick Reference

This appendix provides a quick-reference summary of certificate profiles and OIDs. For detailed profile specifications including all field requirements, constraints, and extensions, refer to §7.

A.1 Summary Table

A.1.1 C2PA Certificates

Certificate Type	Key Usage	EKU	Policy OIDs	Max Validity	Algorithm
Root CA	keyCertSign, cRLSign	—	`1.3.6.1.4.1.62524.1.1` (optional)	20 years	ECDSA P-384, SHA-384
C2PA Claim Signing Issuing CA	keyCertSign, cRLSign	c2pa-kp-claimSigning, id-kp-documentSigning	`1.3.6.1.4.1.62558.1.1`	5 years	ECDSA P-384, SHA-384
C2PA Claim Signing Leaf (L1)	digitalSignature, nonRepudiation	c2pa-kp-claimSigning, id-kp-documentSigning	`1.3.6.1.4.1.62558.1.1`	366 days	ECDSA P-256/P-384, SHA-256/384
C2PA Claim Signing Leaf (L2)	digitalSignature, nonRepudiation	c2pa-kp-claimSigning, id-kp-documentSigning	`1.3.6.1.4.1.62558.1.1`	90 days	ECDSA P-256/P-384, SHA-256/384

A.1.2 CAWG Certificates

Certificate Type	Key Usage	EKU	Policy OIDs	Max Validity	Algorithm
CAWG Identity CA (Interim)	keyCertSign, cRLSign	id-kp-documentSigning	`1.3.6.1.4.1.62558.1.1`	5 years	ECDSA P-384, SHA-384
CAWG Identity Leaf (Interim)	digitalSignature	id-kp-documentSigning	`1.3.6.1.4.1.62558.1.1`	366 days	ECDSA P-256/P-384, SHA-256/384

A.1.3 TSA Certificates

Certificate Type	Key Usage	EKU	Policy OIDs	Max Validity	Algorithm
C2PA Timestamping CA	keyCertSign, cRLSign	id-kp-timeStamping	1.3.6.1.4.1.62558.1.1	10 years	ECDSA P-384, SHA-384
TSA Leaf	digitalSignature, nonRepudiation	id-kp-timeStamping (critical)	1.3.6.1.4.1.62558.1.1	4110 days	ECDSA P-256/P-384, SHA-256/384

A.1.4 OCSP Certificates

Certificate Type	Key Usage	EKU	Policy OIDs	Max Validity	Algorithm
OCSP Signing CA	keyCertSign, cRLSign	—	1.3.6.1.4.1.62524.1.1 (optional)	5 years	ECDSA P-384, SHA-384
OCSP Responder	digitalSignature	id-kp-OCSPSigning	—	30 days	ECDSA P-384, SHA-384

A.2 OID Reference

OID	Name	Usage
1.3.6.1.4.1.62524.1.1	CP/CPS policy OID	CP/CPS identification
1.3.6.1.4.1.62558.1.1	C2PA Certificate Policy	C2PA ecosystem policy
1.3.6.1.4.1.62558.2.1	c2pa-kp-claimSigning	C2PA Claim Signing EKU
1.3.6.1.4.1.62558.3	c2pa-assurance-level	C2PA Assurance Level extension
1.3.6.1.4.1.62558.4	c2pa-cpl-record	C2PA CPL UUID extension
1.3.6.1.5.5.7.3.8	id-kp-timeStamping	Timestamping EKU
1.3.6.1.5.5.7.3.9	id-kp-OCSPSigning	OCSP Signing EKU
1.3.6.1.5.5.7.3.36	id-kp-documentSigning	Document Signing EKU

B Endpoint Quick Reference

This appendix provides a consolidated quick reference for key public endpoints and download URLs. Detailed operational and protocol requirements are specified in §2, §4, §6, and §7.

B.1 Endpoint Summary

Category	Endpoint	URL	Notes
Repository	Central Repository	https://trufo.ai/tca/repository	CA artifacts and related materials
Services	TSA Services	https://tsa.trufo.ai	RFC 3161 timestamping
Services	OCSP Services	https://ocsp.trufo.ai	Certificate status checking
Services	CA Services	https://ca.trufo.ai	EST-style lifecycle endpoints
Services	RA Services	/ra/c2pa/csr-jwt	Canonical CSR JWT issuance path for C2PA enrollment
EST	CA Certificates	https://ca.trufo.ai/.well-known/est/{leaf_type}/cacerts	GET (type-specific path)
EST	Enrollment	https://ca.trufo.ai/.well-known/est/{leaf_type}/simpleenroll	POST (type-specific path)
OCSP	OCSP Responder	https://ocsp.trufo.ai	GET/POST
TSA	Public TSA	https://tsa.trufo.ai	POST
CA Certs	Root CA	https://ca.trufo.ai/root-ca.crt	DER
CA Certs	C2PA Claim Signing Issuing CA	https://ca.trufo.ai/c2pa-ca.crt	DER
CA Certs	C2PA Timestamping CA	https://ca.trufo.ai/ctsa-ca.crt	DER
CA Certs	CAWG Identity CA (Interim)	https://ca.trufo.ai/temp-cawg-ca.crt	DER
CA Certs	OCSP Signing CA	https://ca.trufo.ai/ocsp-signing-ca.crt	DER
Docs	CP/CPS (current)	https://trufo.ai/cpcps	The most recent version
Docs	CP/CPS (archive)	https://trufo.ai/tca/repository/cpcps	Historical versions
Docs	C2PA Certificate Policy	https://trufo.ai/tca/repository/c2pa/certificate-policy	C2PA CP reference
Docs	C2PA Trust List	https://trufo.ai/tca/repository/c2pa/trust-list	C2PA Trust List
Docs	C2PA TSA Trust List	https://trufo.ai/tca/repository/c2pa/tsa-trust-list	C2PA TSA Trust List
Docs	Terms of Service	https://trufo.ai/terms-of-service	Subscriber agreement
Docs	Privacy Policy	https://trufo.ai/privacy-policy	Data handling practices

C Appendix C. Key Management Quick Reference

This appendix provides quick-reference tables for key management. For detailed technical security controls and a key hierarchy overview, refer to §6.

C.1 Key Storage Summary

Key Type	HSM Required	FIPS Level	See §
Root CA	Yes	Level 3	§6.2.1, §6.2.7
Issuing CAs	Yes	Level 3	§6.2.1, §6.2.7
TSA Leaf (TCA)	Yes	Level 3	§6.8.3
TSA Leaf (Delegated)	Yes	Level 3	§6.8.4
Subscriber (C2PA L1)	No	—	§6.1.2
Subscriber (C2PA L2)	Yes	Level 2 Rec.	§6.1.2
Subscriber (CAWG)	No	—	§6.1.2

C.2 Key Validity Summary

Key Type	Maximum Validity	See §
Root CA	20 years	§6.3.2
C2PA Claim Signing Issuing CA	5 years	§6.3.2
C2PA Timestamping CA	10 years	§6.3.2
CAWG Identity CA	5 years	§6.3.2
OCSP Signing CA	5 years	§6.3.2
C2PA Claim Signing Leaf (L1)	366 days	§6.3.2
C2PA Claim Signing Leaf (L2)	90 days	§6.3.2
TSA Leaf	4110 days	§6.3.2
OCSP Responder	30 days	§6.3.2
CAWG Identity Leaf	366 days	§6.3.2

C.3 Multi-Person Control Summary

Operation	Required Approvals	See §
Root CA key generation	2 of 2 (ceremony)	§6.1.1
Root CA certificate signing	2 of 2 (workflow)	§6.2.2
Issuing CA operations	1 of 1 (with audit)	§6.2.2
Key deletion/destruction	2 of 2	§6.2.10

D Appendix D. Change Log

This appendix documents all revisions to this CP/CPS, including the nature of changes and their effective dates.

D.1 Version History

Version	Date	Summary
1.0	2024-10-23	Initial publication of Trufo CP/CPS
2.0	2026-01-31	C2PA and CAWG conformance update
2.1	2026-03-21	Operational updates from web-based RA platform.

D.2 Detailed Change Log

D.2.1 Version 2.1 (2026-03-21)

Major Changes:

- Updated §1 document revision identifiers and wording for RA enrollment flow presentation.
- Updated §2 publication references and repository links.
- Updated §3 identification and authentication language, including RA/OV/PV gating terminology and MFA context.
- Updated §4 lifecycle operations text to align with RA-issued CSR JWT authorization and EST `simpleenroll` flow.
- Updated §5 service-termination wording to remain consistent with OCSP-only status architecture.
- Updated §6 technical security values and algorithm references (including leaf validity limits and OCSP responder algorithm profile).
- Updated §7 certificate profile constraints for currently supported key algorithms and validity limits.
- Updated Appendix A, Appendix B, and Appendix C quick-reference tables to match current profile and endpoint behavior.
- Updated Appendix D version history and detailed entries for revision 2.1 consistency.

D.2.2 Version 2.0 (2026-01-31)

Major Changes:

This version represents a comprehensive update to align with C2PA Certificate Policy v0.1 (2025-06-02) and to introduce support for CAWG Identity certificates.

§1 – Introduction:

- Added conformance statements for C2PA Certificate Policy v0.1 and C2PA Generator Product Security v0.1.
- Added interim conformance statements for CAWG Identity Assertion v1.3.

- Updated PKI participant definitions to include C2PA-specific roles (Generator Products, Validator Products).
- Added CAWG-specific participant definitions (Identity Holders, Relying Parties).
- Defined constraints for delegated/third-party services (TSA delegation requirements).

§2 – Publication and Repository Responsibilities:

- Established central repository at https://trufo.ai/tca/repository.
- Defined publication requirements for C2PA CP and Trust List references.
- Specified OCSP-only revocation status (no CRL publication).
- Documented AIA extension content for chain building.

§3 – Identification and Authentication:

- Added C2PA-specific identity proofing requirements per assurance level.
- Added CAWG-specific identity proofing requirements (interim).
- Defined Conforming Products List (CPL) verification procedures.
- Specified authentication requirements for EST-style enrollment.

§4 – Certificate Life Cycle Operational Requirements:

- Added EST endpoint specifications for certificate lifecycle operations.
- Defined processing timelines for C2PA and CAWG certificate applications.
- Specified certificate acceptance procedures for manual and automated workflows.
- Added OCSP freshness requirements (1 hour update after revocation).

§5 – Facility, Management, and Operational Controls:

- Updated personnel controls for multi-person control requirements.
- Added incident response procedures aligned with C2PA CP requirements.
- Specified business continuity requirements for CA and TSA services.

§6 – Technical Security Controls:

- Updated cryptographic module requirements to FIPS 140-2 Level 3 for all CA keys.
- Added detailed TSA key management and rotation procedures.
- Specified key storage requirements by assurance level (C2PA L1/L2).
- Added delegated TSA operator security requirements.

§7 – Certificate, CRL, and OCSP Profiles:

- Added complete certificate profiles for C2PA Claim Signing (L1 and L2).
- Added certificate profile for C2PA TSA Leaf.
- Added interim certificate profile for CAWG Identity.
- Defined mandatory C2PA extensions (c2pa-cpl-record, c2pa-assurance-level).
- Specified OCSP profile and response behavior.
- Removed CRL profile requirements (OCSP-only).

§8 – Compliance Audit and Other Assessments:

- Added audit requirements aligned with C2PA CP.
- Specified self-assessment procedures for delegated operators.

§9 – Other Business and Legal Matters:

- Updated warranty and liability provisions for the C2PA/CAWG ecosystem.
- Added provisions for program authority relationships.

Appendices:

- Added Appendix A: Certificate Profile Quick Reference.
- Added Appendix B: Endpoint Quick Reference.
- Added Appendix C: Key Management Quick Reference.
- Added Appendix D: Change Log.

D.2.3 Version 1.0 (2024-10-23)

Initial Publication:

- Established Trufo Certificate Authority CP/CPS framework.
- Defined Root CA and Issuing CA structure.
- Specified basic operational controls and security requirements.
- Established baseline certificate profiles.

D.3 Change Categories

Changes to this CP/CPS are categorized as follows:

Category	Description	Review Requirement
Editorial	Typo corrections, formatting, clarifications that do not change requirements	TPA review
Minor	Non-material changes to operational procedures	TPA review + notification
Major	Changes to security requirements, certificate profiles, or policy statements	TPA + C2PA conformance admin review
Critical	Changes affecting trust anchor, key management, or ecosystem conformance	Full governance review + Subscriber notification