TrustAsia Certification Practice Statement for C2PA Trusted Service

V1.0.0

TrustAsia Technologies, Inc.

2026-05-09

Table of Contents

1. General Provisions

1.1 Overview

1.1.1 Company Introduction

TrustAsia Technologies, Inc. (abbreviated as "TrustAsia") was established in April 2013. In December 2020, TrustAsia CA passed the qualification review by the State Cryptography Administration Office of Security Commercial Code Administration (abbreviated as OSCCA) and was granted the "Electronic Authentication Service License" by OSCCA (License number: 0060). In November 2021, TrustAsia CA obtained the "License for Electronic Certification Service Provider" issued by the Ministry of Industry and Information Technology (License number: ECP31010421056).

TrustAsia CA was granted "ISO9001 quality management system certification", "ISO 27001 information security management system certification", and "ISO22301 business continuity management system certification" by China Quality Certification Centre (CQC), all of which were accredited by China National Accreditation Service for Conformity Assessment (CNAS) and the International Accreditation Forum (IAF).

TrustAsia CA is an outstanding domestic cyber security digital certificate and security monitoring solution provider. Its brand, TrustAsia, located in the field of information security, specializes in providing internationally renowned brand digital certificates and cyber security management solutions, which is recognized and trusted by the field of cyber security.

With the internationally standardized operational management and service level capability, we will provide globalized electronic authentication services for users with requirements on telecommunication and information security aspects in a variety of industries.

1.1.2 Service Hierarchy

The CA certificate hierarchy of TrustAsia CA for C2PA, organized by algorithm, is as follows:

TrustAsia C2PA RSA Root CA (Root Certificate)

—TrustAsia C2PA Claim Signing RSA CA 2026 (C2PA Claim Signing Intermediate CA Certificate)

—TrustAsia C2PA TSA RSA CA 2026 (C2PA Timestamp Intermediate CA Certificate)

TrustAsia C2PA ECC Root CA (Root Certificate)

—TrustAsia C2PA Claim Signing ECC CA 2026 (C2PA Claim Signing Intermediate CA Certificate)

—TrustAsia C2PA TSA ECC CA 2026 (C2PA Timestamp Intermediate CA Certificate)

1.1.3 Certification Practice Statement (CPS)

This TrustAsia C2PA Trusted Service Certification Practice Statement (hereinafter referred to as the "CPS") is compiled in compliance with applicable local laws and regulations.

This CPS describes how TrustAsia CA carries out C2PA electronic certification services, including the business methods and processes of applying, approving, issuing, managing, and revoking certificates, as well as the corresponding service, legal, and technical measures and safeguards, for electronic certification participants to understand and follow. A Subscriber's Generator Product instance uses a certificate to cryptographically sign C2PA Claims, attaching C2PA Content Credentials to assets. Based on the Assurance Level of certificates issued under this policy, Relying Parties may use them as part of the trust evaluation of assets containing Content Credentials.

The contents described in this CPS follow these policies, guidelines, and requirements:

1. The RFC 3647 standard issued by the Internet Engineering Task Force (IETF)
2. The most recent version of the C2PA Certificate Policy published prior to this CPS

TrustAsia CA will periodically review updates and will continuously revise this CPS. If there is any inconsistency between this CPS and the above-referenced standards, the officially issued standards shall prevail.

1.2 Document Name and Identification

This document is the TrustAsia C2PA Trusted Service Certification Practice Statement.

1.2.1 Object Identifiers

This section records the policy identifiers, extension identifiers, and extended key usage identifiers used in C2PA certificates.

Object Identifier (OID)	Object Represented
1.3.6.1.4.1.62558.1.1	C2PA Certificate Policy
1.3.6.1.4.1.62558.3	C2PA Assurance Level Extension
1.3.6.1.4.1.62558.3.10	Assurance Level 1
1.3.6.1.4.1.62558.3.20	Assurance Level 2
1.3.6.1.4.1.62558.4	C2PA Compliant Product List Record ID Extension
1.3.6.1.4.1.62558.2.1	C2PA Claim Signing Key Usage

1.2.2 Revision History

Release Date	Update Content	Version
2026-05-09	Initial release	V1.0.0

1.3 PKI Participants

1.3.1 Certification Authorities

TrustAsia CA is responsible for issuing, signing, and revoking digital certificates that bind public

keys to Subscriber identities. Generator Products may use digital certificates issued by TrustAsia CA to sign C2PA Manifests.

As an operator of multiple CAs, TrustAsia CA performs functions related to public key operations, including receiving certificate requests, issuing, revoking, and renewing digital certificates, and maintaining, issuing, and publishing CRLs and OCSP responses. For information about TrustAsia CA's products and services, please visit www.trustasia.com.

1.3.2 Registration Authorities

An entity authorized by TrustAsia CA to collect, verify, and submit Applicant and/or Subscriber information for inclusion in public key certificates. The RA shall operate under the authority of TrustAsia CA and comply with this CPS.

TrustAsia CA will act as the RA itself in addition to assuming the role of CA, and will not establish a separate RA.

1.3.3 Subscribers

An Applicant that has become a customer of a CA in the C2PA Trust List and is eligible to receive certificates for its Compliant Generator Product instances.

1.3.4 Relying Parties

An entity that evaluates the trustworthiness of assertions made by a signer in a C2PA asset, based on the signer's identity and the Assurance Level encoded in the certificate.

1.3.5 Other Participants

Human or non-human (hardware or software) entities participating in the C2PA ecosystem. Examples include cameras (capture devices), image editing software, cloud services, or personnel using such tools.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates are restricted to use by the Generator Product instance identified as the certificate Subject, for digitally signing C2PA Claims at the Assurance Level indicated in the certificate. Timestamp certificates are for use in timestamping services, and OCSP signing response certificates are for use in OCSP responses.

1.4.2 Prohibited Certificate Uses

Use of certificates issued under this policy outside the scope of the C2PA Content Credentials Specification or C2PA Compliance Program is not permitted.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The governing body of this CPS is the TrustAsia CA Security Policy Committee, which is responsible for formulating, approving, issuing, implementing, updating, and revoking this CPS. The TrustAsia CA Security Policy Committee is composed of appropriate representatives from company management responsible for operational security, technical security, customer service, and personnel security.

The daily work of the external consulting service of this policy document is handled by the Policy Department.

1.5.2 Contact Information

1.5.2.1 CPS Contact

TrustAsia CA will maintain strict version control over the CPS and designate a dedicated department to handle related matters. Any questions, suggestions, or inquiries regarding the CPS may be directed as follows:

Contact Department: Policy Department

Contact email address: cps@trustasia.com

Address: 32/F, Building B, No. 391, Guiping Road, Xuhui District, Shanghai, China (200233)

Tel.: 0086-021-58895880

Fax No.: 0086-021-51861130

Official website: https://www.trustasia.com

1.5.2.2 Certificate Revocation Contact

Certificate problem reports and certificate revocation requests must be submitted in one of the following ways, and certificate revocation requests must be submitted in written form:

- Email: revoke@trustasia.com
- Tel.: 400-880-8600 (Domestic) or 86-21-58895880 (International)

1.5.3 Person Determining CPS Suitability for the Policy

The TrustAsia CA Security Policy Committee is the primary body for policy formulation and is the highest authority to review and approve this CPS.

1.5.4 CPS Approval Procedures

This CPS is compiled by a CPS drafting team organized by the TrustAsia CA Security Policy Committee. Upon completion, the draft is submitted to the Security Policy Committee for review.

After approval by the Committee, the CPS is officially published on the TrustAsia CA official website.

1.6 Definitions and Acronyms

1.6.1 Definitions

Term	Definition
Administration Authority	An entity authorized by the Governing Body to operate the Compliance Program on its behalf. It is responsible for recognizing and certifying key compliance roles that agree to participate in the program. The C2PA Technical Working Group Conformance Task Force operates in this capacity.
Applicant	An entity that has created a Generator Product or Validator Product and wishes to have it recognized as a "Compliant Product" and added to the C2PA Compliant Product List (CPL) under the governance framework of the C2PA Compliance Program.
Applicant Representative	A natural person who is an employee or agent formally authorized by the Applicant.
Assertion	A data structure used to represent a statement made (or "created") by a signer, or collected at Claim Generation time, about an Asset. This data is part of a C2PA Manifest.
Asset	A file or data stream containing digital content, asset metadata, and an optional C2PA Manifest.
Assurance Level	An indication to a Relying Party of the degree of confidence that assertions and claims signed using a given C2PA Claim Signing Certificate reflect the intended behavior of the Generator Product instance. A higher Assurance Level means a higher degree of confidence a Relying Party may have.
Attestation	The process of providing a digital signature over a set of measurements securely stored in hardware, which is then verified by a requesting party along with the set of measurements.
C2PA Certificate Policy	A document specifying the requirements that a Certification Authority (CA) MUST satisfy when issuing digital certificates to Subscribers implementing C2PA-compliant products (used to create assets with digital content and C2PA Manifests), and the requirements that Subscribers MUST satisfy when using such certificates.
C2PA Claim	A digitally signed, tamper-evident data structure that references a set of assertions about an Asset and the information needed to characterize content binding. If any assertion has been redacted, a corresponding claim description is included. This data is part of a C2PA Manifest.

Term	Definition
C2PA Claim Signing Certificate	An X.509 certificate issued by a CA in the C2PA Trust List to a Compliant Generator Product instance of a Conformance Implementer, where the certificate Subject name identifies the Generator Product.
C2PA Compliance Program	A risk-based governance program designed to allow Applicants to demonstrate conformance and obtain C2PA recognition by satisfying procedural requirements. The program includes evaluating C2PA-relevant functionality of the Applicant's products, assessing security attributes to assign a maximum Assurance Level, evaluating the CA's processes and technical capabilities, and signing legal agreements to join the program.
C2PA Compliant Product List	The authoritative record of all Compliant Products recognized as compliant under the C2PA Compliance Program.
C2PA Content Credentials	The preferred non-technical term for a C2PA Manifest. Accordingly, a C2PA Manifest store represents the Content Credentials of an Asset. Content Credentials also refers to the overall C2PA technology and is therefore essentially treated as a plural noun. If a C2PA Manifest is Content Credentials, then multiple C2PA Manifests or the broader, general concept constitute Content Credentials.
C2PA Content Credentials Specification	A globally recognized standard providing content provenance and authenticity for digital assets, designed to enable individuals and organizations to adopt digital provenance technology through a rich ecosystem while satisfying security requirements.
C2PA Governance Framework	A set of governance documents defining the C2PA trust ecosystem, including roles, requirements, and processes.
C2PA Manifest	A collection of provenance information about an Asset formed from a combination of one or more Assertions (including content binding), a Claim, and a Claim signature. A C2PA Manifest is part of a C2PA Manifest Store.
C2PA Trust List	In the context of the Compliance Program, a list of X.509 certificate trust anchors (Root CAs or Subordinate CAs) managed by C2PA, where these CAs issue certificates to Compliant Generator Products in accordance with this C2PA Certificate Policy.
C2PA TSA Trust List	A list of trust anchors managed by C2PA from which CAs issue Timestamp signing certificates to Timestamp Authorities (TSAs).
Certification Authority (CA)	A trusted entity responsible for issuing, signing, and revoking digital certificates that bind public keys to Subscriber identities. Generator Products use digital certificates issued by a CA to sign C2PA Manifests.
Compliance Criteria	A set of normative requirements that C2PA requires Governed Parties to demonstrate compliance with under the Compliance Program, including requirements from the specification itself, the Generator Product Security Requirements document, and the C2PA Certificate Policy.

Term	Definition
Conformance Implementer	An Applicant that has become a member of the C2PA Compliance Program and has at least one product in good standing in the CPL.
Compliant Product	A Generator or Validator Product that has been recognized as compliant by the program and added to the CPL with a status of "conformant." A Compliant Generator Product is assigned a maximum Assurance Level.
Dynamic Evidence	Attributes evaluated by the CA during automated certificate enrollment for a Generator Product instance, typically forwarded in the form of verifiable hardware-backed artifacts (e.g., key or platform attestation reports).
Generator Product	A collection of software, hardware, and platform configurations created by an Applicant that work together as a system to produce digital assets with C2PA Manifests. The product, acting as the signer, is responsible for whether the assets produced conform to normative requirements.
Generator Product Security Requirements	Security-related implementation requirements that a Generator Product must meet in order to achieve a particular maximum Assurance Level.
Governed Party	An organization wishing to assume a recognized role in the C2PA Compliance Program. The program requires it to sign legal agreements and undergo review before its products are included in the C2PA Trust List or Compliant Product List. Governed Parties in the C2PA ecosystem include Certification Authorities and Applicants that choose to apply for and comply with the requirements of the C2PA Compliance Program.
Governance Body	The organization responsible for the trustworthiness of the ecosystem. It authorizes the Administration Authority to manage the ecosystem and authorizes certification entities to convey trust. C2PA serves as the Governance Body of the Compliance Program, driven by its Steering Committee.
Hosted Environment	A server-side environment hosting a subset of the mechanisms and functions of a Generator Product or Validator Product.
Implementation Category – Back-end	An implementation architecture for a target of evaluation where assets, assertions, claims, and claim signatures are generated in one or more hosted environments, including instances hosted on-premises or by commercial cloud service providers.
Implementation Category – Distributed	An implementation architecture for a target of evaluation consisting of an edge subsystem and a back-end subsystem, where the generation of assets, assertions, claims, and claim signatures is distributed across both types of subsystems.
Implementation Category – Edge	An implementation architecture for a target of evaluation where assets, assertions, claims, and claim signatures are generated on network edge endpoints.
Maximum Assurance Level	A numeric designation determined at the sole discretion of the C2PA Compliance Program, based on its evaluation of the security functions and attributes of an Applicant’s Generator Product.

Term	Definition
Registration Authority (RA)	An entity authorized by a CA to collect, verify, and submit Applicant and/or Subscriber information for inclusion in public key certificates. The RA operates under the authority of the CA and complies with the CA's CPS.
Reliable Communication Method	A communication method verified through a source other than the Applicant's Representative, such as a postal/courier address, telephone number, or email address.
Manifest Consumer	A diverse and numerous population of consumers relying on Content Credentials to ensure provenance and authenticity of digital objects. To consume C2PA-supported Content Credentials, Manifest Consumers must use C2PA-approved service providers.
Relying Party	An entity that evaluates the trustworthiness of assertions made by a signer in a C2PA asset, based on the signer's identity and the Assurance Level encoded in the certificate.
Security Incident	An actual or potential event that compromises the confidentiality, integrity, or availability of an information system and the information the system processes, stores, or transmits, or constitutes a violation (or imminent threat of violation) of security policies, security procedures, or acceptable use policies.
Signer	In the context of the Compliance Program, a Compliant Generator Product instance in the CPL is always the signer.
Static Evidence	Attributes of the Generator Product target of evaluation documented in the Generator Product Security Requirements document, reviewed by the Administration Authority when evaluating an Applicant's Generator Product to determine the maximum Assurance Level.
Subscriber	An Applicant that has become a customer of a CA in the C2PA Trust List and is eligible to receive certificates for its Compliant Generator Product instances.
Target of Evaluation	A system whose functional correctness and implementation security are evaluated by the Compliance Program, comprising the Generator Product or Validator Product and the subsystems it relies upon.
Timestamp Authority (TSA)	A server providing electronic authentication and trust services by creating hash values to verify the date and time a file was created or modified, serving as an independent witness that a file has not changed since it was signed.
Trusted Execution Environment (TEE)	See NIST definition.
Validator	A Manifest Consumer that performs the operations described in the validation process.

Term	Definition
Validator Product	A collection of software, hardware, and platform configurations created by an Applicant that work together as a system to verify digital assets with C2PA Manifests. A Validator Product may integrate validator functionality monolithically or rely on a separate validator service locally (e.g., on-device) or remotely (e.g., cloud-hosted). Because the Validator Product is always the entity listed on the C2PA Compliant Product List (CPL), it is responsible for producing correct validation results in accordance with normative requirements, whether it directly integrates or relies on a separate service.

1.6.2 Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document shall be interpreted in accordance with RFC 2119.

Unless otherwise specified, dates stated in this document omit time and time zones; the associated time shall be 00:00:00 UTC+8 (Beijing Time).

2. Publication and Repository Responsibilities

2.1 Repositories

The TrustAsia CA repository is a publicly accessible repository that provides information services to Subscribers and Relying Parties. The repository includes, but is not limited to, the following: CPS, Subscriber Agreement, Relying Party Agreement, Root CA certificates, Intermediate CA certificates, and other information published by TrustAsia CA as necessary.

2.2 Publication of Certification Information

2.2.1 Repository Publication

The TrustAsia CA repository is published on the official website (https://www.trustasia.com/cps) in a timely manner, or in other appropriate forms as needed. Published content includes CA certificates, CPS amendments, and other materials, all of which must remain consistent with this CPS and applicable laws and regulations.

In addition, TrustAsia CA establishes and maintains a non-public secure repository containing records of all certificates issued under this C2PA Root CA. Records of issued certificates are retained for at least one year after expiration. Repository records include: certificate serial number, subject name, validity period, X.509v3 extensions and their values, and revocation status. The repository is subject to strict access controls and periodic audits to ensure its integrity and confidentiality.

2.2.2 CRL Publication

TrustAsia CA publishes certificate revocation lists (CRLs) via HTTP. Subscribers and Relying Parties may obtain the CRL from the CRL Distribution Point address in certificates issued by TrustAsia CA. Each CRL published by TrustAsia CA contains an incrementing serial number.

2.2.3 OCSP Publication

TrustAsia CA provides an Online Certificate Status Protocol (OCSP) service, allowing Subscribers and Relying Parties to query certificate status information in real time.

2.3 Time or Frequency of Publication

2.3.1 CPS Publication Frequency

TrustAsia CA will periodically follow changes to the C2PA Certificate Policy and adjust this CPS in a timely manner to maintain conformance.

2.3.2 CRL Publication Frequency

TrustAsia CA publishes CRLs for Subscriber certificates once per day; CRLs for Subordinate CA certificates are published at least once every 12 months. If a Subordinate CA certificate is revoked, the CA certificate CRL shall be updated and published within 24 hours.

2.4 Access Controls on Repositories

Information in the TrustAsia CA repository is provided for public query and access in a read-only manner.

Through network security protection, secure system design, and security management policies, TrustAsia CA ensures that only authorized personnel may add, delete, modify, or publish content in the repository.

All versions of the CPS, including historical versions, will be publicly available in the repository. == 3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Digital certificates issued by TrustAsia CA comply with the X.501 standard.

3.1.2 Need for Names to Be Meaningful

TrustAsia CA uses Distinguished Names (DNs) to identify the certificate Subject and the certificate Issuer. Under the C2PA trust model, names in the DN have specific representative meaning and may be related to the identity or unique attributes of the end entity using the certificate.

The Subject of a certificate MUST be a specific Generator Product created by the Subscriber and used to sign C2PA Claims. The identification requirements for the DN fields are as follows:

1. The values of DN fields MUST exactly match the corresponding record for the Generator Product listed in the C2PA Compliant Product List.
2. All field values in the DN MUST be written in pure ASCII text.

3.1.3 Anonymity or Pseudonymity of Subscribers

TrustAsia CA will not issue anonymous or pseudonymous certificates.

Certificates issued by TrustAsia CA do not uniquely identify the specific instance of the Generator Product to which they are issued. For example, an issued certificate does not contain the unique serial number of the specific device that obtained the certificate.

3.1.4 Rules for Interpreting Various Name Forms

C2PA Claim Signing Certificates issued by TrustAsia CA comply with the X.509 V3 standard. The

unique Distinguished Name assigned to the certificate holder follows the X.501 naming convention.

3.1.5 Uniqueness of Names

Issued certificates MUST ensure name uniqueness. TrustAsia CA enforces name uniqueness within its domain. Issuing multiple certificates to the same entity is not considered a violation of name uniqueness. For example, TrustAsia CA may issue certificates with the same Subject DN to multiple devices of the same model or multiple instances of the same application.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate Applicants SHALL NOT use names that may infringe upon others' intellectual property rights in their certificate applications. TrustAsia CA does not verify the Subscriber’s right to use a trademark when issuing certificates, nor is it responsible for resolving trademark-related disputes. TrustAsia CA may reject or revoke certificates that are subject to trademark disputes.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in the certificate generates its own key pair, that party shall be required to prove possession of the private key corresponding to the public key in the certificate request. TrustAsia CA verifies the Subscriber’s possession of the private key by verifying the Subscriber’s digital signature on the PKCS#10 Certificate Signing Request (CSR) using the public key contained in the CSR.

3.2.2 Authentication of Organization Identity

If a certificate request contains an organization identity, TrustAsia CA will verify whether the entity submitting the certificate request for signing C2PA-compliant claims controls the application associated with the name referenced in the certificate, or has been authorized by the application owner to act on its behalf.

TrustAsia CA will verify that the operational status of the Applicant organization is not marked as "ceased," "inactive," "invalid," "non-current," or equivalent, and will verify the identity and address information of the Applicant organization through one or more of the following:

1. A government agency in the jurisdiction in which the Applicant organization is legally established, exists, or is recognized.
2. A third-party database that is regularly updated and considered a "reliable data source," such as the Global LEI (Legal Entity Identifier) data source.
3. Valid registration documents issued by a government agency, including but not limited to business licenses, public institution legal person certificates, and unified social credit code certificates.
4. Verification through opinion letters issued by qualified lawyers, accountants, or similar professionals.
5. Confirmation of the organization’s address through property bills, bank statements,

government-issued tax bills, or other verification methods recognized by TrustAsia CA.

6. Engagement of a third party to investigate the organization, or requiring the Applicant to provide additional information and documentary evidence.

In addition to the above identity and address verification, TrustAsia CA will also obtain the organization's address and contact information through third-party databases that are regularly updated and considered reliable data sources, and will contact the organization by telephone, email, postal mail, or other means to confirm the accuracy of the information provided by the Applicant Representative.

For certificate renewal requests, TrustAsia CA will re-validate the Subscriber's identity using the procedures described in Section 3.2 "Initial Identity Validation" no more than 398 days after the previous identity validation.

3.2.3 Authentication of Individual Identity

TrustAsia CA's certificate issuance targets must be Applicants that are organizational entities. However, TrustAsia CA will verify the personal identity of the Applicant Representative during the certificate issuance process. The Applicant Representative must be a natural person and may be an authorized employee or authorized agent of the Applicant organization. TrustAsia CA will use the verification methods in Section 3.2.2 to confirm the Applicant's request intent with the Applicant Representative.

3.2.4 Non-Verified Subscriber Information

In general, except for identity information that is explicitly required to be clearly and reliably verified for the type of certificate in question, TrustAsia CA makes no representations regarding the accuracy of Subscriber information that has not been required to be verified, and assumes no related legal liability. Information in the certificate MUST be verified from trusted third-party data sources; unverified information SHALL NOT be included in the certificate.

3.2.5 Validation of Authority

TrustAsia CA will verify that the Applicant Representative has the authority to submit a C2PA Claim Signing Certificate application for the Applicant's Generator Product on behalf of the Applicant, to sign the Subscriber Agreement on behalf of the Applicant, and to bind the Applicant to the terms and conditions of the agreement.

TrustAsia CA may verify the authenticity of the certificate application directly with the Applicant Representative, or with an authoritative department within the Applicant's organization, such as the Applicant's primary business office, corporate office, human resources office, information technology office, or another department deemed appropriate by TrustAsia CA.

3.2.6 Criteria for Interoperation

Not applicable.

3.2.7 Proof of Compliance

TrustAsia CA will verify whether the Generator Product for which the Applicant is requesting a certificate already exists in the C2PA Compliant Product List and whether its current status is clearly marked as "conformant."

TrustAsia CA will obtain the maximum Assurance Level for which the Generator Product is eligible based on the value of the Maximum Assurance Level field in the corresponding entry for that Generator Product in the C2PA Compliant Product List.

TrustAsia CA will not issue certificates with an Assurance Level higher than the value of the Maximum Assurance Level field.

3.3 Identification and Authentication for Re-key Requests

TrustAsia CA does not support re-key operations.

3.3.1 Identification and Authentication for Routine Re-key

This scenario is not supported.

3.3.2 Identification and Authentication for Re-key After Revocation

This scenario is not supported.

3.4 Identification and Authentication for Revocation Requests

In TrustAsia CA’s certificate services, certificate revocation requests may be initiated by the Subscriber, the C2PA Administration Authority, TrustAsia CA, or judicial personnel authorized by a judicial authority. When a revocation request is initiated by a Subscriber, TrustAsia CA will verify the authenticity of the revocation request and revoke the relevant certificate within 72 hours.

3.5 Identification and Authentication for Certificate Issuance and Renewal

For renewal requests, TrustAsia CA will re-validate the Subscriber’s identity using the procedures described in Section 3.2 "Initial Identity Validation" no more than 398 days after the previous identity validation.

4. Certificate Life Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

An Applicant initiates the certificate request process by submitting a formal application to TrustAsia CA through the designated method to become a Subscriber. The Applicant shall provide the following information and documents:

1. Information about the Generator Product for which the certificate is being requested, including its record ID in the C2PA Compliant Product List.
2. The Assurance Level requested by the Applicant for its Generator Product, which SHALL NOT exceed the Maximum Assurance Level recorded for that product in the C2PA Compliant Product List.
3. If the Assurance Level indicated in the CPL record for the Applicant's Generator Product so requires, evidence that the product is capable of producing verifiable artifacts using one of the attestation methods listed in that product's CPL record.

4.1.2 Enrollment Process and Responsibilities

1. The enrollment process includes:
    - Submitting a certificate application;
    - Generating a key pair;
    - Providing the public key of the key pair (a signed CSR) to TrustAsia CA;
    - Agreeing to the applicable Subscriber Agreement;
    - Paying any applicable fees.
2. Responsibilities:
    - The Applicant shall familiarize itself with the matters stipulated in the Subscriber Agreement, this CPS, and other applicable documents, in particular the provisions regarding the scope of certificate use, rights, obligations, and warranties.
    - The Subscriber is responsible for providing truthful, complete, and accurate certificate application information and materials to TrustAsia CA.
    - The Registration Authority is responsible for examining and reviewing the certificate application information and identity verification materials provided by the Subscriber.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Upon receiving a Subscriber's certificate application, TrustAsia CA's validation team will review the information and documents submitted by the Subscriber for completeness and accuracy, and will perform identification and authentication of the Subscriber's identity in accordance with Section 3.2 of this CPS.

When the Assurance Level indicated in the Subscriber's Generator Product entry in the C2PA Compliant Product List has specific requirements, TrustAsia CA will confirm that the Applicant has the capability to obtain and submit Platform Attestation Reports to TrustAsia CA.

4.2.2 Approval or Rejection of Certificate Applications

4.2.2.1 Approval of Certificate Applications

TrustAsia CA approves a certificate application by issuing the certificate after successfully completing all required verification steps.

TrustAsia CA may approve a certificate application if the following conditions are met:

1. The application fully satisfies the identification and authentication requirements for Subscriber identity set forth in Section 3.2 of this CPS.
2. The Subscriber has accepted or has not objected to the content and requirements of the Subscriber Agreement.
3. The Subscriber has paid the applicable fees as required.

4.2.2.2 Rejection of Certificate Applications

TrustAsia CA has the right to reject a certificate application if any of the following circumstances occur:

1. The application does not comply with the Subscriber identity identification and authentication requirements set forth in Section 3.2 of this CPS.
2. The Subscriber cannot provide the required identity verification materials as requested.
3. The Subscriber objects to or cannot accept the relevant content and requirements of the Subscriber Agreement.
4. The Subscriber has not or cannot pay the applicable fees as required.
5. The intended use of the Subscriber's certificate does not comply with the laws and regulations of the Subscriber's jurisdiction.
6. TrustAsia CA determines that approving the application would expose TrustAsia CA to disputes, legal proceedings, or losses.
7. The public key length, algorithm, or other aspects of the submitted application present security concerns.

For rejected certificate applications, TrustAsia CA will notify the Subscriber of the application failure via email.

4.2.3 Time to Process Certificate Applications

Under normal circumstances, TrustAsia CA will verify Subscriber information and issue certificates within a reasonable timeframe. Unless otherwise agreed with the relevant Subscriber or specified in another agreement, no specific processing time for completing a certificate application is stipulated.

Certificate processing time depends largely on when the Subscriber provides the information and documents required to complete validation and whether the Subscriber responds to TrustAsia CA's administrative requests in a timely manner. Certificate application requests remain valid until rejected.

4.2.4 CA Credentials

Upon successful completion of the application process, the CA associates the newly approved Subscriber with new or existing secure access credentials (e.g., username and password, client certificate, or bearer token) used to authenticate the Subscriber when submitting certificate enrollment requests.

4.3 Certificate Issuance

Certificate issuance complies with the identification and authentication of Subscriber identity as specified in Section 3.2 of this CPS.

If the Maximum Assurance Level indicated in the Subscriber's product entry in the CPL so requires, TrustAsia CA requests and verifies the Dynamic Evidence required for that Assurance Level, satisfying the following:

1. Dynamic Evidence may include key attestation reports, application attestation reports, platform attestation reports, or other verifiable artifacts backed by a hardware root of trust.
2. When verifying key and platform attestation reports, TrustAsia CA follows the "Requirements for Verifying Dynamic Evidence" defined in Appendix A of the C2PA Certificate Policy.

After successfully verifying the above Dynamic Evidence, TrustAsia CA issues a C2PA Claim Signing Certificate complying with the specifications in Chapter 7 of this CPS to the Subscriber's specific device or application instance.

4.3.1 CA Actions During Certificate Issuance

For Subscriber certificates, TrustAsia CA confirms the source of the certificate request prior to issuance.

During issuance, the RA administrator is responsible for approving certificate applications and submitting the certificate issuance request to the CA's certificate issuance system by operating the RA system. The certificate issuance request sent from the RA to the CA must be protected by authentication and confidentiality measures for the RA's identity and information, and must ensure the request is sent to the correct CA certificate issuance system. Upon receiving the issuance request, the CA certificate issuance system authenticates and decrypts the information from the RA.

Database storage and CA processes occurring during certificate issuance are protected against unauthorized modification.

For valid certificate issuance requests, the CA certificate issuance system delivers the certificate to the Subscriber.

TrustAsia CA has deployed multi-factor authentication for all accounts that can directly issue certificates.

4.3.1.1 Manual Authorization for Root CA Certificate Issuance

The Root CA certificate issuance process requires individuals authorized by TrustAsia CA (CA system operators, system administrators, or PKI administrators) to manually issue an explicit instruction so that the Root CA performs the certificate signing operation.

4.3.2 Notification to Subscriber of Certificate Issuance

TrustAsia CA delivers the certificate to the Subscriber within a reasonable time after publication through any secure means. Typically, TrustAsia CA sends the certificate to the Subscriber's designated email address via email during the application process.

4.4 Certificate Acceptance

A Subscriber's acceptance of a certificate signifies the Subscriber's acceptance of the necessary terms of the user agreement in the C2PA Certificate Policy and constitutes compliance with this CPS.

4.4.1 Conduct Constituting Certificate Acceptance

Certificates issued under this CPS are restricted to use by C2PA Compliant Products identified as the certificate Subject, implemented by the designated Subscriber and listed in the C2PA Compliant Product List, for digitally signing C2PA Claims at the Assurance Level indicated in the certificate. Use for any other purpose is strictly prohibited.

The Subscriber is solely responsible for installing the issued certificate on the Subscriber's computer or Hardware Security Module (HSM).

Conduct by which a Subscriber is deemed to have accepted an issued certificate includes, but is not limited to:

1. The Subscriber accesses the TrustAsia CA certificate service website, downloads the certificate to the digital certificate carrier, and completes the download.
2. TrustAsia CA, with the Subscriber's permission, downloads the certificate on behalf of the Subscriber and delivers the certificate to the Subscriber via a secure carrier.
3. The Subscriber downloads the certificate through a certificate receipt notification sent to the Subscriber.
4. The Subscriber accepts the method of obtaining the certificate and does not object to the certificate or its contents.
5. The Subscriber successfully installs and uses the certificate through a Generator Product

instance.

4.4.2 Publication of the Certificate by the CA

TrustAsia CA's delivery of the certificate to the Subscriber constitutes publication of the certificate.

4.4.3 Notification to Other Entities by the CA

TrustAsia CA will not notify other entities.

4.5 Key Pair and Certificate Usage

See Section 6.1.7 of this CPS.

4.5.1 Subscriber Private Key and Certificate Usage

Key usage scenarios shall be determined by the Key Usage extension in the X.509 certificate. Private keys corresponding to public keys in certificates issued under this CPS SHALL be under the sole control of the Generator Product instance and SHALL NOT be exported or shared with other devices, application instances, or third parties, unless permitted by the Generator Product Security Requirements. Certificates issued under this CPS are restricted to use by the Generator Product identified as the Subject, for signing C2PA Claims at the indicated Assurance Level; all other uses are strictly prohibited.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties should consider the overall circumstances and the risk of loss before relying on a certificate.

When a Relying Party receives information bearing a digital signature, it has an obligation to perform the following confirmations:

1. Obtain the certificate corresponding to the digital signature and its certificate chain;
2. Verify the certificate's validity period to ensure the certificate is used within its validity period;
3. Confirm that the certificate corresponding to the signature is trusted by the Relying Party;
4. Verify whether the certificate corresponding to the signature has been revoked by querying the CRL or OCSP;
5. Confirm that the intended use of the certificate is appropriate for the corresponding signature;
6. Verify the signature using the public key on the certificate;
7. Consider other information specified in this CPS or elsewhere.

If the above conditions are not satisfied, the Relying Party has the responsibility to reject the signed information.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

This scenario is not supported.

4.6.2 Who May Request Renewal

This scenario is not supported.

4.6.3 Processing Certificate Renewal Requests

If certificate renewal is required, the Subscriber must re-apply following the validation procedures in Chapter 3 of this CPS.

4.6.4 Notification of New Certificate Issuance to Subscriber

This scenario is not supported.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

This scenario is not supported.

4.6.6 Publication of the Renewal Certificate by the CA

This scenario is not supported.

4.6.7 Notification to Other Entities by the CA

This scenario is not supported.

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

This scenario is not supported.

4.7.2 Who May Request Certification of a New Public Key

This scenario is not supported.

4.7.3 Processing Certificate Re-keying Requests

If re-keying is required, the Subscriber must re-apply following the validation procedures in Chapter 3 of this CPS.

4.7.4 Notification of New Certificate Issuance to Subscriber

This scenario is not supported.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

This scenario is not supported.

4.7.6 Publication of the Re-keyed Certificate by the CA

This scenario is not supported.

4.7.7 Notification to Other Entities by the CA

This scenario is not supported.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

This scenario is not supported.

4.8.2 Who May Request Certificate Modification

This scenario is not supported.

4.8.3 Processing Certificate Modification Requests

If certificate modification is required, the Subscriber must re-apply following the validation procedures in Chapter 3 of this CPS.

4.8.4 Notification of New Certificate Issuance to Subscriber

This scenario is not supported.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

This scenario is not supported.

4.8.6 Publication of the Modified Certificate by the CA

This scenario is not supported.

4.8.7 Notification to Other Entities by the CA

This scenario is not supported.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

1. TrustAsia CA MUST revoke a certificate within 72 hours if one or more of the following circumstances occur:

a. The Subscriber requests revocation;

b. TrustAsia CA obtains evidence that the certificate has been misused;

c. TrustAsia CA is notified that the Subscriber has violated one or more material obligations under the Subscriber Agreement or this CPS;

d. TrustAsia CA has reason to believe or confirms that the Generator Product has been compromised, or that attestation has failed;

e. TrustAsia CA is notified of a material change to information contained in the certificate;

f. TrustAsia CA is notified that certificate issuance did not comply with the C2PA Certificate Policy or TrustAsia CA's CPS;

g. TrustAsia CA determines that any information appearing in the certificate is inaccurate, untrue, or misleading;

h. Revocation of the Subscriber certificate is required by TrustAsia CA's CPS for reasons other than those described in this Section 4.9.1.1;

i. TrustAsia CA is notified through a demonstrated method that the Subscriber's private key has been compromised or that there is clear evidence of a defect in the method used by the Subscriber to generate the private key;

j. TrustAsia CA ceases operations for any reason and has not arranged with another CA to provide certificate revocation services;

k. Performance of obligations under the CPS is delayed or prevented by force majeure; natural disaster; computer or communications failure; change of law, regulation, or other legislation; governmental action; or other causes beyond individual control that pose a threat to the information of others;

l. The Subscriber has not paid applicable service fees after TrustAsia CA has fulfilled its collection obligations;

m. The Generator Product's status in the CPL changes to any status beginning with "revoked";

n. The C2PA Governing Body requests revocation.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

TrustAsia CA SHALL revoke a Subordinate CA certificate within 72 hours if one or more of the following circumstances occur:

1. The Subordinate CA formally requests revocation in writing;
2. The Subordinate CA identifies and notifies TrustAsia CA that the initial certificate request was

not authorized and cannot be traced to an authorized action;

3. TrustAsia CA obtains evidence that the Subordinate CA's private key corresponding to the certificate's public key has been compromised, or no longer meets the requirements of Sections 6.1.5 and 6.1.6 of the Baseline Requirements;
4. TrustAsia CA obtains evidence that the certificate has been misused;
5. TrustAsia CA is notified that issuance of the Subordinate CA certificate did not comply with the Baseline Requirements, or that the Subordinate CA has failed to comply with this CPS;
6. TrustAsia CA determines that any information in the Subordinate CA certificate is inaccurate, untrue, or misleading;
7. TrustAsia CA ceases operations for any reason and has not arranged with another CA to provide certificate revocation services;
8. TrustAsia CA's authority to issue certificates under the Baseline Requirements has expired, been revoked, or been terminated, unless it continues to maintain CRL/OCSP repositories;
9. This CPS requires revocation of the Subordinate CA certificate.

4.9.2 Who Can Request Revocation

Entities that may request revocation include the Subscriber, the C2PA Administration Authority, TrustAsia CA, or judicial personnel authorized by a judicial authority.

4.9.3 Procedure for Revocation Request

4.9.3.1 Voluntary Revocation Request by Subscriber

1. The Subscriber submits a certificate revocation application form and relevant identity verification materials to TrustAsia CA, stating the reason for revocation in the application;
2. TrustAsia CA performs identification and authentication of the revocation request in accordance with Section 3.4 of this CPS;
3. Upon completing the revocation, TrustAsia CA shall promptly publish the revocation to the Certificate Revocation List;
4. After the certificate is revoked, TrustAsia CA will notify the Subscriber by email or other appropriate means. If the Subscriber cannot be reached, TrustAsia CA may, where necessary, announce the revoked certificate on its website;
5. TrustAsia CA provides 7*24-hour certificate revocation application service. Subscribers may apply for certificate revocation through the contact methods provided in Section 1.5.2 of this CPS.

4.9.3.2 Involuntary Revocation of Subscriber Certificate

1. When TrustAsia CA has sufficient reason to believe that a circumstance described in Section 4.9.1.1 of this CPS requiring mandatory revocation has occurred, TrustAsia CA will apply for revocation through its internal process;
2. When a security risk arises with respect to the private key corresponding to TrustAsia CA's Root CA or Subordinate CA certificate, Subscriber certificate revocation may be performed directly

upon approval by the national competent authority for electronic certification services;

3. When a third party such as a Relying Party, judicial authority, application software provider, or anti-virus organization submits a certificate problem report, TrustAsia CA shall conduct an investigation and determine whether to revoke the certificate based on the investigation results;
4. After the certificate has been revoked, TrustAsia CA will notify the Subscriber of the revocation and the reason for it through appropriate means including email and telephone. If the Subscriber cannot be reached, TrustAsia CA may, where necessary, announce the revoked certificate on its website;
5. TrustAsia CA provides 7*24-hour certificate problem reporting and handling service. Parties may submit problem reports through the contact methods provided in Section 1.5.2 of this CPS.

4.9.4 Revocation Request Grace Period

TrustAsia CA does not support a revocation request grace period.

4.9.5 Time Within Which CA Must Process the Revocation Request

Within 72 hours of receiving a revocation request, TrustAsia CA will investigate the facts and circumstances related to the revocation request and provide an initial report to the Subscriber and the entity that submitted the revocation request.

After reviewing the facts and circumstances, the CA will assist the Subscriber and the entities that submitted the problem report or other revocation-related notifications to determine whether to revoke the certificate or take other reasonable remedial action. If revocation is determined, the CA will publish the revocation within the timeframe specified in Section 4.9.1.1, measured from receipt of the revocation request or revocation-related notification.

When determining the timing of revocation, the CA will consider the following criteria:

1. The nature of the problem (scope, context, severity, seriousness, risk of harm);
2. The consequences of revocation (direct and collateral impacts on Subscribers and Relying Parties);
3. The number of revocation requests received regarding a specific certificate or Subscriber;
4. The entity making the complaint (e.g., a law enforcement complaint about a website engaged in illegal activity is more significant than a consumer complaint about not receiving an ordered product); and
5. Applicable legislation.

4.9.6 Revocation Checking Requirements for Relying Parties

The CRL is publicly available information with no read-access security restrictions. Relying Parties may freely query CRLs as needed, including querying the Certificate Revocation List, checking certificate status through TrustAsia CA's designated website, or using the Online Certificate Status Protocol (OCSP).

Before relying on a certificate, Relying Parties shall proactively check the certificate's status against the most recently published CRL from TrustAsia CA and shall verify the reliability and integrity of the CRL to confirm the certificate's validity.

4.9.7 CRL Issuance Frequency

CRLs are accessible via a publicly accessible HTTP URL. Within 24 hours of issuing the first certificate, TrustAsia CA will generate and publish either:

1. A complete CRL, or
2. CRL partitions that, when aggregated, reconstitute the complete CRL.

For CAs that issue Subscriber certificates:

1. Update and publish a new CRL at least every 4 days
2. Update and publish a new CRL within 24 hours of revoking a certificate

For CAs that issue CA certificates:

1. Update and publish a new CRL at least every 12 months
2. Update and publish a new CRL within 24 hours of revoking a certificate

The CA will continue to publish CRLs until:

1. All CA certificates sharing the same Subject public key have expired or been revoked; or
2. The corresponding CA private key has been destroyed.

4.9.8 Maximum Latency for CRLs

TrustAsia CA CRLs are automatically published to the public network after generation. Under normal circumstances, CRLs take effect within 1 hour and at most within 24 hours.

4.9.9 On-line Revocation/Status Checking Availability

TrustAsia CA provides OCSP responses indicating the revocation status of Generator Claim Signing certificates as described in Section 2.2.1 of this CPS.

4.9.10 On-line Revocation Checking Requirements

Consistent with RFC 6960.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Related to Key Compromise

If a Subscriber or TrustAsia CA discovers or suspects private key compromise, immediate action must be taken to revoke the compromised certificate in accordance with this CPS and to re-issue the

certificate.

Any Relying Party that discovers private key compromise may report it to TrustAsia CA via email (revoke@trustasia.com). The report must include evidence of the private key compromise:

1. The private key itself.
2. A CSR signed with the compromised private key, where the CSR Common Name is "Proof of Private Key Compromise for TrustAsia."

4.9.13 Circumstances for Certificate Suspension

TrustAsia CA does not support certificate suspension.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Certificate status information is available through CRL and OCSP responses.

For revoked certificates, TrustAsia CA will not delete their revocation records from CRLs and OCSP until the certificate has expired.

4.10.2 Service Availability

Certificate status services are available around the clock. TrustAsia CA operates and maintains its CRL and OCSP functions with sufficient resources to provide response times of 10 seconds or less under normal operating conditions.

Under normal network conditions, the CRL for the C2PA certificate chain is downloadable over a simulated telephone line in no more than 3 seconds.

TrustAsia CA responds to high-priority certificate problems around the clock. Where appropriate, TrustAsia CA refers such issues to law enforcement agencies and revokes the Subject certificate associated with such issues.

4.10.3 Optional Features

OCSP responders may not be available for all certificate types.

4.11 End of Subscription

Upon termination of a subscription or cessation of relevant activities, the Subscriber shall destroy the private key.

The following circumstances shall be deemed as the Subscriber terminating the use of certificate services provided by TrustAsia CA:

1. Failure to pay service fees on time after certificate expiration;
2. Failure to perform certificate renewal or re-key after certificate expiration;
3. Certificate revocation prior to expiration.

Once a Subscriber terminates TrustAsia CA's certificate authentication service during the certificate's validity period, TrustAsia CA will immediately revoke the Subscriber's certificate upon approving the termination request and will publish the revocation in accordance with the CRL publication policy.

TrustAsia CA maintains detailed records of the certificate revocation process and periodically archives certificates and corresponding Subscriber data following termination of a subscription.

4.12 Key Escrow and Recovery

TrustAsia CA does not host private keys for any digital certificate Subscribers and therefore does not provide key recovery services.

4.12.1 Key Escrow and Recovery Policy and Practices for Signing Keys

Not applicable.

4.12.2 Key Encapsulation and Recovery Policy and Practices for Session Keys

Not applicable.

5. Management, Operational, and Physical Controls

This section describes the physical, procedural, and personnel controls, publication, and certificate management required by TrustAsia CA to operate and maintain the integrity of the PKI system. The focus is on logical and procedural controls reflecting the nature of the environment in which certificates will be used.

5.1 Physical Controls

5.1.1 Site Location and Construction

TrustAsia CA's data center and systems are constructed in accordance with the following standards:

1. Computer Site Technical Requirements (GB 2887-89)
2. Code for Design of Electronic Information System Room (GB 50174-2008)
3. Code for Fire Protection Design of Interior Decoration of Buildings (GB50222-95)
4. Code for Design of Low Voltage Distribution (GBJ50054-95)
5. Technical Requirements and Test Methods for Electromagnetic Shielded Room Processing Classified Information, Class C (BMB3-1999)
6. General Specification for Computer Sites (GB/T 2887-2011)
7. Code for Design of Protection of Structures against Lightning (GB/50057-2010)

TrustAsia CA's data center has an access control system with the following functions:

1. Access to each door is controlled by access card and fingerprint authentication;
2. Logs are maintained for entry and exit through each door;
3. Doors in the management service area and core area are equipped with forced-open alarms and overtime alarms;
4. The entire access control system is connected to a UPS to provide emergency power in the event of a power outage.

The entire facility has a video surveillance system with no blind spots, providing uninterrupted 7*24-hour recording of important passageways inside and outside the facility. All recordings are retained for at least 3 months; video recordings of significant events are separately archived for reference. Illegal intrusion detection alarms, environmental monitoring alarms, and audible/visual alarms are installed, with simultaneous notification to operations personnel.

5.1.2 Physical Access

5.1.2.1 Public Area

The entrance and power distribution areas of TrustAsia CA's facility are access-controlled,

requiring an access card or fingerprint authentication to enter.

5.1.2.2 Management Service Area

The service area is the working area for TrustAsia CA operations and management personnel. Two trusted personnel are required to simultaneously use an access card and fingerprint authentication to enter. Personnel entry and exit from the service area are logged.

5.1.2.3 Core Area

The core area is the CA operations management zone. Entry requires an access card and fingerprint authentication.

The certificate authentication system, cryptographic equipment, and other related cryptographic materials are stored in this area. CA servers, database systems, and cryptographic equipment are located within the shielded server room inside the core area. The shielded server room requires two trusted personnel to simultaneously use an access card and fingerprint authentication to enter, ensuring that no single individual can perform sensitive operations inside the shielded area.

A separate buffer zone exists within the shielded area to prevent electromagnetic leakage when the shielded door is opened.

5.1.3 Power and Air Conditioning

TrustAsia CA has a reliable and secure dual-feed power supply system with an emergency power backup system to ensure 7*24-hour normal power supply and to provide normal service in the event of a power supply interruption. In addition, a dedicated diesel generator is used, capable of sustaining full load for all racks in the new data center for more than 12 hours.

The data center is equipped with an air conditioning system to control temperature and humidity in the operations facility, with capacity configured based on the number of cabinets and the full load of equipment in each server room.

5.1.4 Water Exposures

TrustAsia CA’s server room is elevated 1.45 meters above the ground and is equipped with a water leakage alarm system. In the event of a water hazard, the system will immediately trigger an alarm and notify relevant personnel to take emergency measures.

5.1.5 Fire Prevention and Protection

TrustAsia CA’s server room fire alarm system uses a cabinet-type heptafluoropropane automatic fire suppression device. The system collects fire data through temperature and smoke sensors installed in the server room, simultaneously processing alarm data and system operating status data from users' automatic fire alarm terminals in real time.

The system has two management modes: manual and automatic, enabling real-time monitoring and detection of the network system and configuring manual or automatic control modes, and completing the various interlinked actions specified in the system design.

5.1.6 Media Storage

TrustAsia CA stores audit, archive, and backup information media in secure facilities, protected by physical access controls. Only authorized personnel may access the media with at least 2 trusted personnel present. A media usage log is maintained to record media status and to prevent accidental damage to media.

5.1.7 Waste Disposal

TrustAsia CA shreds paper documents and data discs no longer in use so that the information cannot be recovered. Cryptographic equipment is initialized using the method provided by the equipment manufacturer and physically destroyed before being disposed of.

At least 2 trusted personnel must be present when disposing of waste materials.

5.1.8 Off-site Backup

TrustAsia CA backs up critical data and audit log data to offline media and transports them to an off-site location for storage. The storage facility meets the media storage requirements described in Section 5.1.6.

5.2 Procedural Controls

5.2.1 Trusted Roles

During the provision of electronic certification services, TrustAsia CA designates as trusted roles all positions that can materially affect the issuance, use, management, and revocation of certificates and related key operations, adhering to the principle of separation of trusted roles. These roles include but are not limited to:

1. Authentication and Customer Service Personnel: responsible for Subscriber information entry, review of digital certificate application information, completion of authentication, approval, and revocation operations, and provision of related support services;
2. Key and Cryptographic Device Management Personnel: responsible for maintaining the CA key and certificate lifecycle and managing cryptographic equipment;
3. System Maintenance Personnel: responsible for daily maintenance of CA system hardware and software, and monitoring and troubleshooting;
4. Security Management Personnel: responsible for physical security and routine security management;
5. Security Audit Personnel: responsible for auditing business operations;
6. Human Resources Management Personnel: responsible for background checks on personnel in critical positions and security management.

Trusted roles are appointed by management. The list of persons appointed to trusted roles is maintained and reviewed annually.

5.2.2 Number of Persons Required per Task

TrustAsia CA strictly controls critical tasks in its specific business procedures. The following sensitive operations require multiple trusted roles to complete jointly, for example:

1. Access to the shielded server room: configured for 2-person entry/exit mode;
2. Authentication, review, and certificate issuance: requires 2 trusted personnel to complete jointly;
3. Safe storing root key activation data: configured for 2-person opening mode;
4. Key and cryptographic device operations and storage: requires 3 of 5 trusted personnel to complete jointly;
5. CA system back-end operations: requires 2 trusted personnel to complete jointly;
6. Critical system data operations and maintenance: requires at least 1 person to operate and 1 person to supervise and record.

5.2.3 Identification and Authentication for Each Role

Before allowing any personnel to access and perform operations in the systems necessary for their trusted role, TrustAsia CA requires authentication to the CA and RA systems. For example:

1. For physical access by trusted personnel, authentication is performed via access card and fingerprint recognition to determine corresponding access rights.
2. For trusted personnel performing Subscriber certificate lifecycle management, they access the system using their respective digital certificates to perform certificate management tasks.
3. For system maintenance personnel, they log into the system for maintenance through a bastion host using their individual accounts and passwords.

5.2.4 Roles Requiring Separation of Duties

To ensure system security and adhere to the principle of separation of trusted roles, trusted roles at TrustAsia CA are held by different individuals.

5.2.5 Documentation of Operational Procedures

TrustAsia CA maintains detailed operational documentation to ensure the integrity, security, and compliance of the PKI system. These documents include but are not limited to the following five core areas:

1. Certificate lifecycle management procedures, including certificate issuance, renewal, and revocation processes;
2. Key generation and management specifications within equipment or applications;
3. Authentication and verification procedures for specific Assurance Levels;
4. Incident response and disaster recovery plans;
5. Security policies, guidelines, and access control measures.

5.2.6 Change Management

TrustAsia CA has established a formal change management process to strictly control, document, and review all changes to C2PA certification service infrastructure, software, and operational procedures.

5.2.6.1 Formal Change Process and Records

TrustAsia CA implements an internal system change management policy. Any adjustment to C2PA production systems, security architecture, core software, or business processes must be submitted through a change request that details the change content and affected scope. All change activities fall within the scope of audit.

5.2.6.2 Testing and Approval Mechanism

Before deploying changes to the production environment, rigorous validation is performed in an independent development or test environment to ensure the changes do not affect system stability or compliance with C2PA specifications. Changes must be approved by a trusted role and may only be implemented upon authorization.

5.2.6.3 Rollback and Recovery Plan

To address unforeseen issues that may arise during change implementation, TrustAsia CA prepares a rollback plan for each change. If a change fails to achieve the expected results or causes system anomalies, TrustAsia CA will immediately initiate the rollback procedure to restore the infrastructure, software, or operating environment to a safe and stable state.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

TrustAsia CA's qualification requirements for personnel in trusted roles are as follows:

1. Good social and professional background.
2. Compliance with national laws and regulations, with no criminal record.
3. Compliance with TrustAsia CA's security management standards, regulations, and policies.
4. A conscientious and responsible work attitude and a good professional background.
5. Good team cooperation spirit.
6. Personnel in critical and core positions must have relevant work experience or pass training and assessments organized by TrustAsia CA before assuming their roles.

5.3.2 Background Check Procedures

TrustAsia CA, in cooperation with relevant government departments and investigative agencies, conducts background checks on trusted employees. All trusted employees and employees applying for transfer to trusted positions must agree in writing to a background check. Background checks must comply with the requirements of laws and regulations; the content, methods, and persons

conducting the investigation must not violate laws and regulations. Background checks shall use lawful means and verify personnel background information through relevant organizations and departments to the greatest extent possible.

Background checks are divided into basic checks and comprehensive checks. Basic checks cover employment history, professional references, education, and social relations. Comprehensive checks, in addition to all basic check items, also cover criminal records, social relations, and social security. Personnel in critical positions for public trust certificate services must undergo comprehensive checks.

Human resources department investigation procedures include:

1. Confirming the personal information of candidates; providing the following documents: resume, highest degree certificate, degree certificate, qualification certificates, identification card, and other relevant valid documents.
2. Verifying the authenticity of submitted materials via telephone, online means, etc.
3. During background checks, candidates found to have the following may be directly disqualified from becoming trusted personnel:
    - Fabricating facts or materials;
    - Relying on unreliable references;
    - Using illegal identification or education/qualification certificates;
    - Serious dishonest conduct at work.
4. Upon completion of the investigation, reporting the results to the management responsible for the relevant work for approval.
5. TrustAsia CA signs a confidentiality agreement with employees to restrict them from disclosing any confidential or sensitive information about CA certificate services. All personnel currently in trusted roles are also evaluated on the job to continuously verify their trustworthiness and work competence.

5.3.3 Training Requirements

TrustAsia CA provides position-specific pre-job training based on the needs of trusted roles, and maintains records of employee training participation. These training programs include:

1. Basic Public Key Infrastructure (PKI) knowledge;
2. This CPS and related standards and procedures;
3. Identity authentication and verification policies and procedures;
4. Security management policies and mechanisms;
5. Disaster recovery and business continuity procedures;
6. Data protection related to C2PA services;
7. Unified requirements for role responsibilities;
8. National laws, regulations, standards, and procedures for electronic certification services;
9. Other training as required.

Reviewers performing identity verification duties must complete all of the above training before assuming their positions to ensure they can satisfactorily fulfil their duties. Reviewers must pass periodic knowledge assessments organized by TrustAsia CA to ensure they possess the skills required to fulfil their duties.

5.3.4 Retraining Frequency and Requirements

Personnel serving in trusted roles or other important roles must receive at least one training session organized by TrustAsia CA within any 5-year period. Personnel involved in the operation of certification systems shall receive at least one relevant skills and knowledge training session every 5 years. In addition, TrustAsia CA will require personnel to undergo continuing training on an as-needed basis in response to system upgrades, policy adjustments, and other requirements.

5.3.5 Job Rotation Frequency and Sequence

The frequency and sequence of job rotation for TrustAsia CA employees will be determined in accordance with the institution's security management policies.

5.3.6 Sanctions for Unauthorized Actions

When an employee is confirmed to have used TrustAsia CA systems for certification operations without authorization or beyond the scope of their authority, TrustAsia CA will immediately revoke that person's login credentials, simultaneously terminate their system access, and, depending on the severity of the unauthorized conduct, impose measures including job transfer, public criticism, fines, dismissal, and referral to judicial authorities.

5.3.7 Independent Contractor Requirements

TrustAsia CA currently does not employ external independent contractors for certification-related work.

5.3.8 Documentation Supplied to Personnel

Documents provided to personnel by TrustAsia CA typically include but are not limited to the following:

1. This CPS and related standards and specifications;
2. Employee handbook;
3. Job descriptions, workflows, and specifications;
4. Internal operational documents, including business continuity management and disaster recovery plans;
5. Security management policies, etc.

5.3.9 Access Control

TrustAsia CA implements strict access control management for C2PA certification systems, related data, and infrastructure to ensure the confidentiality, integrity, and availability of systems.

1. Principle of Least Privilege: All access to CA systems, databases, and sensitive data is granted based on a "need-to-know" basis. System access rights are strictly assigned on a "least privilege" basis, ensuring that trusted personnel only have the operational permissions necessary to fulfil their role responsibilities.
2. Identity Authentication and Strong Password Policy: Authentication is required before accessing CA systems or performing trusted role tasks. TrustAsia CA implements a strict strong password policy; passwords must meet specified length and complexity requirements.
3. Multi-Factor Authentication: TrustAsia CA mandates multi-factor authentication on critical access paths. Accounts capable of directly issuing certificates, and remote system administration access through a bastion host, must use multi-factor authentication.
4. Access rights are reviewed on a regular basis.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

TrustAsia CA will record details of actions taken to process certificate applications and issue certificates, including all information generated and documents received related to certificate applications, the time and date, and the personnel involved.

If TrustAsia CA's applications cannot automatically log events, manual procedures will be implemented to meet the requirements.

These events include but are not limited to:

1. CA certificate and key lifecycle management events, including:

a. Key generation, backup, storage, recovery, archival, and destruction;
b. Certificate requests, renewal, and re-key requests, and revocation;
c. Approval and rejection of certificate applications, including successful and failed certificate operations;
d. Cryptographic device lifecycle management events, including: device receipt, installation, uninstallation, activation, use, and maintenance;
e. Generation of CRL entries;
f. Signing of OCSP responses;
g. Records of introducing new certificate profiles and retiring existing ones.

2. Subscriber lifecycle management events:

a. Certificate requests, renewal, re-key requests, and revocation;
b. Acceptance and rejection of certificate requests, including acceptance of Subscriber Agreements, validation of application materials, and storage of application and validation materials;
c. Certificate issuance;

d. Generation of CRL entries;
e. Signing of OCSP responses;

3. Security events:

a. Successful and unsuccessful attempts to access PKI systems;
b. Actions performed on PKI and security systems;
c. Changes to security configuration profiles;
d. Installation, updates, and deletion of software on certificate systems;
e. System crashes, hardware failures, and other anomalies;
f. Firewall and router activity; and
g. Entry and exit from CA facilities, including authorized and unauthorized personnel access and access to secure storage facilities.

4. System operations events, including:

a. System startup and shutdown;
b. Creation and deletion of system privileges, setting or modifying passwords;
c. Unauthorized access and access attempts to CA system networks;
d. Unauthorized access and access attempts to system files;
e. Reading, writing, or deletion of security and sensitive files or records;

5. Trusted personnel management records, including:

a. Account application records for network access;
b. Application, modification, and creation request records for system privileges;
c. Changes in personnel status.

Log records generally shall include:

1. Date and time of the record;
2. Sequence number of the record;
3. Identity of the entity making the log entry;
4. Description of the record content.

5.4.1.1 Router and Firewall Activity Logs

TrustAsia CA router and firewall logs shall include at least:

1. Successful and unsuccessful login attempts on routers and firewalls;
2. Records of all administrative operations performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications;
3. Records of all changes made to firewall rules, including additions, modifications, and deletions;

4. Records of all system events and errors, including hardware failures, software crashes, and system restarts.

5.4.2 Frequency of Processing Log

For automated system logs and manual records maintained by operators, TrustAsia CA performs one annual review and summary.

For system security logs, one annual follow-up review is performed to check for significant events that violate policies and specifications.

5.4.3 Retention Period for Audit Log

TrustAsia CA and its Timestamp Authority retain the following logs for at least one year:

1. CA certificate and key lifecycle management event records after any of the following occurs:

a. The CA private key is destroyed; or

b. The CA field in the X.509v3 Basic Constraints extension of the certificate is set to "TRUE," and the final CA certificate that shares the CA private key's public key has been revoked or has expired.

2. Subscriber certificate lifecycle management event records after Subscriber certificate revocation or expiration.
3. Timestamp Authority data records after the Timestamp certificate private key is revoked or renewed.
4. Any security event records after an event occurs.

Note: Although these requirements establish minimum retention periods, TrustAsia CA and its Timestamp Authority may choose longer periods to facilitate investigation of security incidents or other types of events that may require retrospective review.

5.4.4 Protection of Audit Log

TrustAsia CA's audit logs are stored in databases and backed up, including audit information and event records in relevant documents.

TrustAsia CA implements strict physical and logical access controls to ensure that only authorized personnel may access these records. Unauthorized access, reading, modification, and deletion are strictly prohibited.

5.4.5 Audit Log Backup Procedures

TrustAsia CA's system logs are synchronized in real time to log servers and backed up weekly. Manual paper records are periodically archived and stored in dedicated filing cabinets.

5.4.6 Audit Collection System

For electronic audit information, TrustAsia CA's audit log collection system encompasses:

1. Certificate management systems;
2. Certificate issuance systems;
3. Certificate directory systems;
4. Remote communication systems;
5. Certificate processing systems;
6. Access control systems;
7. Website and database security management systems;
8. Other systems requiring audit.

For paper-based audit information, dedicated filing cabinets are used for collection and archiving.

5.4.7 Notification to Event-Causing Subject

When TrustAsia CA discovers an attack, it will log the attacker's behavior, trace the attacker within the limits permitted by law, and reserve the right to take corresponding countermeasures. TrustAsia CA has the right to determine whether to notify entities associated with the incident.

5.4.8 Vulnerability Assessments

TrustAsia CA performs an annual risk assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, and any process for the disclosure, misuse, alteration, or destruction of certificate data or certificate management;
2. Assesses the likelihood and potential harm of such threats, taking into account the sensitivity of certificate data and certificate management processes; and
3. Evaluates the adequacy of policies, procedures, information systems, technology, and other arrangements that TrustAsia CA has put in place to counter such threats. Based on the risk assessment, a security plan is developed, implemented, and maintained, including security procedures, measures, and product controls to manage the risks identified in the risk assessment. The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of certificate data and certificate management processes. The security plan also considers the technologies available at the time and the cost of implementing specific measures, and implements an appropriate level of reasonable security given potential damage from security vulnerabilities and the nature of the data to be protected.

5.5 Records Archival

5.5.1 Types of Records Archived

In addition to archiving matters described in Section 5.4.1, TrustAsia CA also archives the following categories of events, including but not limited to:

1. Documents related to the security of its certificate systems, certificate management systems, Root CA systems, and authorized third-party systems; and

2. Documents related to the validation, issuance, and revocation of certificate applications and certificates.

5.5.2 Retention Period for Archive

Archived audit logs (as described in Section 5.5.1) are retained for at least 1 year from the time stamp of their creation, or for the period required by Section 5.4.3, whichever is longer.

Records retained by TrustAsia CA for at least 1 year include:

1. All archived documents related to the security of certificate systems, certificate management systems, and Root CA systems as specified in Section 5.5.1; and
2. All archived documents related to the validation, issuance, and revocation of certificate applications and certificates (as specified in Section 5.5.1) after the occurrence of any of the following:

a. Such records and documents are last relied upon for the validation, issuance, or revocation of certificate requests and certificates; or

b. Expiration of Subscriber certificates that relied upon such records and documents.

5.5.3 Protection of Archive

TrustAsia CA provides secure physical and logical protection for archived documents in both electronic and paper form, along with strict management procedures, to ensure archived documents are not damaged and to prevent unauthorized access, modification, and deletion.

5.5.4 Archive Backup Procedures

Electronic records generated by systems are periodically backed up and stored off-site in offline media. Electronic records generated manually are collected and backed up in internal storage servers.

Paper documents do not require backup but are protected by strict security measures to prevent unauthorized access, modification, and deletion.

5.5.5 Requirements for Time-stamping of Records

When creating archived records, TrustAsia CA automatically time-stamps them using system time (non-cryptographic method). TrustAsia CA's time source servers are synchronized with a Coordinated Universal Time (UTC) time source recognized by a national metrology institute.

TrustAsia CA's Timestamp Authority (TSA) will record the following information and make these records available to qualified auditors as evidence that the Timestamp Authority complies with these requirements:

1. Physical or remote access to the timestamp server, including the time of access and the identity of the individual accessing the server;
2. History of timestamp server configuration;

3. Any attempt to delete or modify timestamp logs;
4. Security events, including:

a. Successful and unsuccessful timestamp authority access attempts.

b. Actions performed by the Timestamp Authority server.

c. Changes to security configuration profiles.

d. System crashes and other anomalies; and

e. Firewall and router activity.

5. Revocation of a timestamp certificate;
6. Significant changes to the timestamp server's time; and
7. System startup and shutdown.

5.5.6 Archive Collection System

For electronic records generated by systems, they are synchronized in real time to log servers and backed up off-site weekly.

For electronic records generated manually, they are collected and backed up in internal storage servers.

For paper-based archival materials, they are collected and archived in filing cabinets.

5.5.7 Procedures to Obtain and Verify Archive Information

TrustAsia CA implements physical and logical access control methods to ensure that only authorized personnel may access these archived records. Unauthorized access, reading, modification, and deletion are strictly prohibited.

5.6 CA Key Changeover

5.6.1 Key Changeover Procedure

TrustAsia CA's ICA certificates have a maximum validity period of 5 years. The expiry time of any Subscriber certificate issued by an ICA SHALL NOT exceed the ICA certificate's expiry time.

For the key pair corresponding to an ICA certificate, TrustAsia CA will initiate the key changeover process 2 years before the ICA certificate expires to replace the soon-to-expire ICA key pair. Key changeover is performed as follows:

1. Two years before the ICA certificate expires, a new key pair is generated and a new ICA certificate is issued.
2. After generating the new key pair, approved Subscriber certificate requests will progressively be issued using the new ICA key.

3. One year before the original ICA certificate expires, the use of its private key to issue new ICA certificates shall cease.

5.6.2 Notification to Subscriber

TrustAsia CA will comply with the following provisions to notify Subscribers of any planned key changeover event:

1. Advance Notification Obligation: For all planned CA key changeovers, TrustAsia CA will notify Subscribers in advance. This notification is intended to ensure that Subscribers have sufficient time to perform necessary configuration updates to their Generator Products or system environments to maintain the integrity and continuity of the C2PA trust chain.
2. Notification Timeframe: TrustAsia CA will issue notifications within a reasonable time prior to the official implementation of a key changeover. The notification timeframe will take into full account the time required for Subscribers to update their systems, perform compatibility testing, and deploy new trust anchors, ensuring that the impact on Subscriber operations is minimized.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

TrustAsia CA develops and documents business continuity plans and disaster recovery plans to notify software vendors, Subscribers, and Relying Parties in the event of a disaster, security incident, or business disruption. TrustAsia CA does not publicly disclose business continuity plans, but they are subject to audit by auditors and are tested, reviewed, and updated annually. Business continuity plans include:

1. Conditions for activating the plan;
2. Emergency procedures;
3. Fallback procedures;
4. Recovery procedures;
5. Plan maintenance schedule;
6. Awareness and training requirements;
7. Individual responsibilities;
8. Recovery Time Objectives (RTO);
9. Periodic testing of the contingency plan;
10. Plans for TrustAsia CA to promptly maintain or restore CA operations after interruption or failure of a critical business process;
11. Requirements to store critical cryptographic materials (i.e., secure cryptographic devices and activation materials) at an alternative location;
12. What constitutes an acceptable system interruption and recovery time;
13. Frequency of backup copies of important business information and software;

14. Distance of the recovery facility from the CA's primary site; and
15. Procedures to protect its facilities as far as practicable for the period following a disaster and prior to restoration of a secure environment at the primary or remote site.

5.7.2 Computing Resources, Software, and/or Data Corruption

TrustAsia CA backs up the resources, software, and data of business systems and other critical systems, and has developed corresponding contingency handling procedures. In the event of destruction of network communication resources, inability of computer equipment to provide normal service, software corruption, database tampering, or other such events or disasters caused by force majeure, TrustAsia CA will implement recovery in accordance with the disaster recovery plan.

5.7.2.1 Backup Storage

TrustAsia CA backs up critical business data, configuration files, archived records, and audit log data and transports them to a secure off-site location for storage. The backup media storage facility meets the physical access control standards described in Section 5.1.6 of this CPS and requires at least 2 trusted personnel to be present for access. To ensure the effectiveness of backup data under extreme circumstances, TrustAsia CA regularly conducts recoverability tests of backup data in accordance with policy requirements, verifying the integrity of backup media and the accuracy of data restoration procedures, to ensure rapid restoration of business operations when needed.

2. **Recovery Plan**

TrustAsia CA develops and maintains a detailed, formally documented business continuity plan and disaster recovery plan. This plan specifies detailed procedures for restoring operations following natural disasters, security incidents, computing resource destruction, or large-scale system failures.

5.7.3 Private Key Compromise Handling Procedures

1. When a Subscriber discovers that a certificate private key has been compromised, the Subscriber must immediately cease use of the private key and immediately access the TrustAsia CA certificate service website to revoke the certificate, or immediately notify TrustAsia CA by telephone, email, or other means to revoke the certificate, and re-apply for a new certificate following the relevant procedures. TrustAsia CA will publish certificate revocation information in accordance with Section 4.9 of this CPS.
2. When a Subscriber's certificate private key is compromised, TrustAsia CA will immediately revoke the certificate and notify the Subscriber. The Subscriber must immediately cease use of the private key and re-apply for a new certificate following the relevant procedures. TrustAsia CA will publish certificate revocation information in accordance with Section 4.9 of this CPS.
3. When TrustAsia CA's Root CA or Subordinate CA private key is compromised, TrustAsia CA will implement emergency handling in accordance with the key emergency plan and promptly notify Relying Parties through various channels.

5.7.4 Business Continuity Capabilities After a Disaster

In the event of a significant disaster at the physical site, TrustAsia CA will restore partial service within 48 hours in accordance with the business continuity plan.

5.8 CA or RA Termination

When TrustAsia CA needs to cease its operations, it will strictly comply with the requirements for the suspension of certification authority operations set forth in the Electronic Signature Law of the People's Republic of China and related regulations.

Before TrustAsia CA terminates, it must:

1. Identify a successor entity to assume operations;
2. Draft a TrustAsia CA termination statement;
3. Notify relevant Subscribers of the cessation of operations at least 90 days in advance;
4. Handle archived documentary records;
5. Cease certification center services;
6. Archive relevant system logs;
7. Handle and store sensitive documents.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

CA key pairs are generated in a secure physical environment using cryptographic equipment compliant with FIPS 140-2 Level 3. Key generation, management, storage, backup, and recovery comply with the relevant provisions of the FIPS 140-2 standard.

The CA key pair generation process is performed in TrustAsia CA's shielded server room, witnessed by multiple TrustAsia CA key administrators, a number of trusted personnel, and qualified independent third-party auditors, following a pre-prepared key generation script. The entire CA key pair generation process and operations must be video-recorded. A qualified independent third-party auditor shall produce a report demonstrating that the processes and controls during the CA key pair generation can ensure the integrity and confidentiality of the CA key pair.

The key generation ceremony script includes:

a. Definition of roles and participant responsibilities;
b. Authorization or approval for the key generation ceremony;
c. Cryptographic hardware and activation materials required for the ceremony;
d. Specific steps to be performed during the key generation ceremony;
e. Physical security requirements for the ceremony site;
f. Secure post-ceremony storage of cryptographic hardware and activation materials;
g. Signatures of participants and witnesses confirming the ceremony was conducted in accordance with the script; and
h. Any anomalies or deviations from the script during the key generation ceremony.

6.1.1.2 RA Key Pair Generation

Not applicable.

6.1.1.3 Subscriber Key Pair Generation

Subscriber key pairs are generated by the Subscriber. TrustAsia CA does not generate certificate key pairs on behalf of Subscribers.

Requirements for Subscriber key pair generation are defined in the C2PA Compliance Program's Implementation Security Requirements document and may vary depending on the Assurance Level being implemented.

TrustAsia CA only issues certificates for Claim Signing keys that comply with applicable requirements of the C2PA Content Credentials Specification and the certificate profile requirements

of this CPS.

Regardless of Assurance Level, Subscribers may only use keys for which certificates have been issued under this CPS to sign C2PA Claims generated by the device or application identified as the certificate Subject.

6.1.2 Private Key Delivery to Subscriber

TrustAsia CA does not generate or deliver private keys to Subscribers.

6.1.3 Public Key Delivery to Certificate Issuer

As part of the certificate application process, the Subscriber generates a key pair and submits the public key to TrustAsia CA in a CSR.

6.1.4 CA Public Key Delivery to Relying Parties

TrustAsia CA public keys are contained in TrustAsia CA's self-signed Root CA certificates and Intermediate CA certificates. Subscribers and Relying Parties may obtain Root CA and Intermediate CA certificates from the C2PA official website.

6.1.5 Key Sizes

To ensure sufficient key security strength, TrustAsia CA certificates of different types comply with the following standards:

Certificate Type	**Root CA**	**Intermediate CA**	**Subscriber Certificate**
Digest Algorithm	SHA-384	SHA-384	SHA-256 or SHA-384
RSA Key Size	4096	4096	2048 or 3072 or 4096
ECC Curve	P-384	P-384	P-256 or P-384 or P-521
EdDSA Curve	-	-	Ed25519

6.1.6 Public Key Parameters Generation and Quality Checking

TrustAsia CA and Subscribers shall both generate public keys in accordance with Section 6.1.1 of this CPS. Public key parameters are generated by compliant devices/platforms to ensure the quality of public key parameters. Public keys must meet the requirements of Section 6.1.5 of this CPS.

TrustAsia CA performs public key parameter checks prior to issuing a certificate to ensure public key parameters satisfy the following:

- For RSA public keys:
  1. The public exponent is an odd number greater than or equal to 3.
  2. The public exponent shall be in the range 2^16+1 to 2^256-1.
  3. The modulus is odd.

4. The modulus is at least 2048 bits in length and is a multiple of 8.
5. The modulus is not a perfect power of a prime.
6. The modulus has no factor smaller than 752.

- For ECDSA public keys:

The validity of all keys is confirmed through a full ECC public key validation procedure or a partial ECC public key validation procedure.

6.1.7 Key Usage Purposes

X.509 v3 certificates issued by TrustAsia CA include the Key Usage extension, whose usage is consistent with the RFC 5280 standard. Certificate Subscribers must use keys in accordance with the purposes indicated in the Key Usage extension of the certificate issued by TrustAsia CA.

Root CA keys are generally used to issue the following certificates and CRLs:

1. Self-signed certificates representing the Root CA;
2. Intermediate CA certificates and cross-certificates;
3. OCSP signing certificates;
4. Infrastructure certificates (management role certificates, CA internal operations device certificates).

Intermediate CA keys are generally used to issue the following certificates and CRLs:

1. Subscriber certificates;
2. Timestamp signing certificates;
3. OCSP signing certificates.

The permitted key usage of a Subscriber’s key is determined by the Key Usage and Extended Key Usage extensions in the certificate issued under the applicable Intermediate CA.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

TrustAsia CA implements physical and logical protections to prevent unauthorized certificate issuance. For private key backups outside the designated verified systems or devices described above, TrustAsia CA stores encrypted key shares in physical devices held by different entities to prevent private key disclosure. The algorithm and key length used to encrypt private key shares are, based on current technology, capable of resisting cryptanalysis attacks for the remaining lifetime of the encrypted key or key share.

6.2.1 Cryptographic Module Standards and Controls

Cryptographic modules used by TrustAsia CA for CA key pairs and timestamp key pairs comply with the FIPS 140-2 Level 3 standard.

Cryptographic modules used for Assurance Level 2 comply with or exceed the following standards:

- FIPS 140-2 Level 2, or
- CC EAL 4+ or higher.

Cryptographic modules used for timestamp certificates comply with or exceed the following standards:

- FIPS 140-2 Level 3, or
- CC EAL 4 or higher.

6.2.2 Private Key Multi-Party Control (m-of-n)

TrustAsia CA implements multi-party control for operations such as CA private key generation, renewal, revocation, backup, and recovery. Management of the private key is distributed among 5 key administrators; operations on the private key require at least 3 key administrators to be present and to provide approval by inserting their administrator IC cards or USB keys and entering PIN codes.

6.2.3 Private Key Escrow

TrustAsia CA will not escrow private keys.

6.2.4 Private Key Backup

TrustAsia CA backs up Root CA private keys and CA private keys. In accordance with the operating procedures provided by the cryptographic equipment manufacturer, multi-party controlled backup ciphertext files and backup recovery privilege IC cards or USB keys are generated and stored in the company's safe (or bank safe deposit box or other facility with security standards no lower than the local backup). TrustAsia CA has established a CA key backup and recovery plan, and conducts annual reviews and recovery drills of this plan.

6.2.5 Private Key Archival

TrustAsia CA does not archive private keys for Subscriber certificates, nor does it archive any CA certificate private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

TrustAsia CA key pairs are generated, stored, and used on hardware cryptographic modules. For recovery purposes, TrustAsia CA backs up CA keys under multi-party control in accordance with the operating procedures provided by the cryptographic equipment manufacturer.

In addition, TrustAsia CA has strict key management processes to control the copying of CA key pairs. All of these measures effectively prevent CA private key loss, theft, modification, unauthorized disclosure, and unauthorized use.

6.2.7 Private Key Storage on Cryptographic Module

6.2.7.1 CA Private Key Storage

TrustAsia CA private keys are stored in encrypted form in hardware cryptographic modules compliant with the FIPS 140-2 Level 3 standard, and private key usage also occurs within the hardware cryptographic module.

6.2.7.2 Timestamp Service Private Key Storage

TrustAsia CA private keys used for timestamp services comply with the requirements of Section 6.2.7.1 of this CPS.

6.2.8 Method of Activating Private Key

TrustAsia CA private keys are stored in hardware cryptographic modules. Activation requires compliance with Section 6.2.2 of this CPS: at least a majority of key administrators must be present and provide approval, and operator privileges on the cryptographic device are used for activation. When CA private key usage is required (online or offline), key administrators must provide their operator IC card or USB key and enter a PIN code to complete the operation.

6.2.9 Method of Deactivating Private Key

For TrustAsia CA private keys, the private key enters a deactivated state when the CA system issues a logout instruction to the cryptographic module, the cryptographic management software issues a shutdown instruction to the cryptographic module, or the hardware cryptographic module storing the private key loses power.

The operation to deactivate a private key is performed by key administrators using their administrator cards to log into the server cryptographic module and entering a PIN code, with at least a majority of key administrators present and providing approval.

6.2.10 Method of Destroying Private Key

At the end of the CA private key's lifecycle, TrustAsia CA retains the CA private key in one backup hardware cryptographic module; all other CA private key backups are securely destroyed. At the same time, all PIN codes, IC cards, USB keys, and other materials used to activate the private key must also be destroyed.

The CA SHALL NOT destroy its private key before its commercial purpose has expired or its legal liability has ended.

Archived CA private keys shall be securely destroyed upon the conclusion of their archival period, or when the CA private key backup or copy is no longer needed for a valid commercial purpose, with multiple trusted personnel participating. Destruction of a CA private key shall ensure the CA private key is completely deleted from the hardware cryptographic module, leaving no residual information.

6.2.11 Cryptographic Module Rating

See Section 6.2.1 of this CPS.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

For TrustAsia CA public key archival, see Chapter 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The maximum validity periods for TrustAsia CA certificates are:

Type	Private Key Usage Period	Certificate Validity Period
C2PA Root CA	Not stipulated	25 years
C2PA Claim Signing Intermediate CA	Not stipulated	5 years
C2PA Timestamp CA	Not stipulated	15 years
Assurance Level 1 Certificate	Not stipulated	Not to exceed 366 days
Assurance Level 2 Certificate	Not stipulated	Not to exceed 90 days
Timestamp Certificate	Not stipulated	Not to exceed 4,110 days

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

TrustAsia CA private key activation data is generated by the cryptographic device in accordance with the operating procedures provided by the cryptographic equipment manufacturer, with at least a majority of key administrators present and providing approval.

Subscriber private key activation data, including passwords for downloading certificates (provided in the form of a secure envelope), login passwords for USB keys and IC cards, etc., must all be generated in a secure and reliable environment. Such activation data is delivered to Subscribers through secure and reliable means, such as offline face-to-face delivery or registered post. For activation data that is not for one-time use, TrustAsia CA recommends that Subscribers change it themselves.

If Subscriber certificate private key activation data is a password, such passwords must:

1. Be at least 8 characters;
2. Contain at least one lowercase letter;
3. Not contain many identical characters;
4. Not be the same as the operator’s name;
5. Not use birthdays, telephone numbers, or other numeric sequences;

6. Not contain a long substring from the username information.

6.4.2 Activation Data Protection

For CA private key activation data (smart IC cards, PIN codes), TrustAsia CA ensures trusted personnel hold such data by reliable means. All trusted personnel are required to memorize, rather than write down, their passwords and not share them with others.

Subscriber activation data must be generated in a secure and reliable environment and must be kept safe, or memorized and then destroyed, and must not be made known to others. If a Subscriber uses a password or PIN code to protect the private key, the Subscriber shall keep it safe to prevent disclosure or theft. If a Subscriber uses biometric features to protect the private key, the Subscriber shall take care to prevent unlawful theft of their biometric features.

6.4.3 Other Aspects of Activation Data

When private key activation data is transmitted, it shall be protected from loss, theft, modification, unauthorized disclosure, or unauthorized use during transmission.

When private key activation data is no longer needed, it shall be destroyed, and it shall be protected from theft, disclosure, or unauthorized use in the process. Destruction results in the inability to obtain any part or all of the activation data, directly or indirectly, from residual information or media; for example, paper recording a password must be shredded.

Taking security factors into account, the lifecycle of activation data for Subscribers applying for certificates is specified as follows:

1. Passwords used by Subscribers to apply for certificates become invalid upon successful application.
2. For passwords protecting private keys or IC cards and USB keys, Subscribers are recommended to change them as needed based on business requirements; passwords in use for more than 3 months should be changed.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Subscriber Generator Products shall comply with platform-specific security guidelines and best practices to prevent unauthorized access, malware, and other cybersecurity threats.

Security measures such as secure coding practices, code signing, and regular security updates shall be employed.

Access to sensitive data or functions within Generator Products shall be restricted and protected by appropriate authentication and authorization mechanisms.

6.5.2 Computer Security Rating

TrustAsia CA's CA systems and their operating environments have undergone third-party security assessments and penetration testing, and the corresponding test reports have been obtained.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

TrustAsia CA's software design and development process follows these principles:

1. Establishing an internal system change and upgrade request procedure, requiring staff to strictly follow the process;
2. Establishing an internal procurement process and management policy;
3. Development programs must undergo rigorous testing in a development environment before an application for deployment to the production environment is submitted;
4. Effective online backup is performed before a change is deployed;
5. Third-party verification and review;
6. Security risk analysis and reliability design.

6.6.2 Security Management Controls

TrustAsia CA has established various security policies, management policies, and processes for the security management of certification systems.

Information security management of the certification system is operated in strict compliance with the relevant operational management standards of the State Cryptography Administration.

The use of the certification system is strictly controlled. All systems undergo rigorous testing and validation before secure use, and any modification or upgrade is documented.

TrustAsia CA regularly performs security checks on the system to identify whether devices have been compromised and whether security vulnerabilities exist.

6.6.3 Life Cycle Security Controls

Throughout the entire certificate lifecycle from issuance to revocation, TrustAsia CA implements security controls to ensure the confidentiality, integrity, and availability of certificates and their associated data.

The certificate issuance and revocation processes are protected against unauthorized operations and tampering.

Certificate status information is available to Relying Parties at all times via mechanisms such as OCSP or CRL.

6.7 Network Security Controls

TrustAsia CA implements the following network security controls:

1. Secure communication protocols and practices are used when Generator Product instances interact with the CA or RA during certificate operations;
2. Network traffic is protected against eavesdropping, tampering, and unauthorized access;
3. Identity authentication is required when trusted personnel access CA systems remotely;
4. Authentication is performed when trusted personnel or CA systems establish connections with remote computers.
5. The principle of minimum open access is applied, with restrictions on access to unopened ports.
6. Firewalls are used to protect the CA's internal network from unauthorized access from other zones.
7. The principle of minimum open access is applied; only authorized users are given access to available network services such as SSH and HTTPS.
8. All network security configurations are recorded.
9. Routing controls are implemented to ensure computer connections and information flow comply with access control policies.
10. Local network components in the physical security environment are regularly maintained, and their configurations are regularly reviewed for compliance with configuration requirements.
11. Sensitive data exchanged over public or untrusted networks is encrypted.

6.8 Time-stamping

TrustAsia CA's C2PA Timestamp Authority (TSA) is operational, providing timestamping services compliant with RFC 3161.

System time on TrustAsia CA computers shall be updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every 24 hours.

TrustAsia CA maintains an internal NTP server that is synchronized with an external UTC(k) laboratory, maintaining clock accuracy to within one second or less. TrustAsia CA monitors the timestamp application service; if accuracy exceeds the allowed range, the timestamp application service will cease signing timestamps.

The timestamp application service signs using a dedicated reserved private key. A timestamp application service has only one valid signing key at any given time.

TSA key generation complies with Section 6.1.1 of this CPS, and TSA key storage complies with Section 6.2.7 of this CPS.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

TrustAsia CA issues certificates in accordance with the following specifications, in addition to the technical requirements of Sections 2.2, 6.1.5, and 6.1.6. See Chapter 11 of this CPS.

TrustAsia CA issues certificates based on RFC 5280 requirements. The following configurations apply to all issued certificates.

7.1.1 Version Number

Certificates conform to the X.509 V3 certificate format. Version information is stored in the certificate version field.

7.1.2 Certificate Extensions and Content

TrustAsia CA issues certificates based on RFC 5280 requirements. The configurations below apply to all issued certificates. See Chapter 11 of this CPS.

7.1.3 Algorithm Object Identifiers

7.1.3.1 Subject Public Key Information

The following requirements apply to the subjectPublicKeyInfo field in certificates; no other encodings are used.

RSA

TrustAsia CA uses the rsaEncryption algorithm identifier (OID: 1.2.840.113549.1.1.1) to indicate RSA keys, displaying NULL. When encoded, the RSA key algorithm identifier in hexadecimal is 300d06092a864886f70d0101010500.

ECDSA

TrustAsia CA uses the id-ecPublicKey algorithm identifier (OID: 1.2.840.10045.2.1) to indicate ECDSA keys.

Parameters are encoded using the curve name:

- For P-256 keys, the curve is secp256r1 (OID: 1.2.840.10045.3.1.7).
- For P-384 keys, the curve is secp384r1 (OID: 1.3.132.0.34).

When encoded, the ECDSA key identifiers are the following hexadecimal encodings:

- P-256 key: 301306072a8648ce3d020106082a8648ce3d030107
- P-384 key: 301006072a8648ce3d020106052b81040022

7.1.3.2 Signature Algorithm Identifier

Objects signed by TrustAsia CA private keys and signatures derived therefrom are consistent with the algorithm used in the context.

Specifically, all of the following objects and fields:

1. The signatureAlgorithm field of the certificate.
2. The signature field of the TBSCertificate.
3. The signatureAlgorithm field of the certificate list.
4. The signature field of the TBSCertificate.
5. The signatureAlgorithm field of the OCSP response.

RSA

TrustAsia CA uses two RSA signature algorithms and encodings, as follows:

Signature Algorithm	OID	Hex Encoding
SHA-256 with RSA	1.2.840.113549.1.1.11	300d06092a864886f70d01010b0500
SHA-384 with RSA	1.2.840.113549.1.1.12	300d06092a864886f70d01010c0500

ECDSA

TrustAsia CA uses two ECDSA signature algorithms and encodings, as follows:

Signature Algorithm	OID	Hex Encoding
SHA-256 with ECDSA	1.2.840.10045.4.3.2	300a06082a8648ce3d040302
SHA-384 with ECDSA	1.2.840.10045.4.3.3	300a06082a8648ce3d040303

7.1.4 Name Forms

This section describes the encoding rules applicable to all certificates issued by the CA. Section 7.1.2 may specify further restrictions, but these do not supersede the requirements herein.

7.1.4.1 Name Encoding

For each valid certification path (as defined by RFC 5280, Section 6), TrustAsia CA ensures:

- For each certificate in the certification path, the encoding of the issuer distinguished name field is byte-for-byte identical to the encoding of the subject distinguished name field of the issuing CA's certificate.
- For each CA certificate in the certification path, the encoding of the subject distinguished name field is byte-for-byte identical across all certificates whose subject distinguished names can be compared under RFC 5280, Section 7.1, including expired and revoked certificates.

When encoding names:

- Each Name contains one RDNSequence.
- Each RelativeDistinguishedName contains exactly one AttributeTypeAndValue.
- No Name contains more than one instance of a given AttributeTypeAndValue across all RelativeDistinguishedNames.

7.1.5 Name Constraints

Not applicable.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Reserved Certificate Policy Identifiers

As specified in Section 1.2 of this CPS.

7.1.7 Usage of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

Not applicable.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

7.2 CRL Profile

TrustAsia CA generates and publishes CRLs in accordance with the following configuration.

CRLs cover all certificates issued by that CA. If CRL partitions are used, the aggregate of those partitions is equivalent to the full CRL. The CA does not issue indirect CRLs.

Field		Present	Description
tbsCertList			
	version	Present	v2
	signature	Present	
	issuer	Present	Byte-for-byte match with issuing CA Subject
	thisUpdate	Present	CRL issuance date
	nextUpdate	Present	7 days for Subscriber certificates; 12 months for Intermediate CA certificates
	revokedCertificate	Not used	
	extensions	Present	See table below

Field	Present	Description
signature	Present	

7.2.1 Version Number

TrustAsia CA Certificate Revocation Lists comply with the version and format requirements of X.509 v2.

7.2.2 CRL and CRL Entry Extensions

CRL extensions:

Extension	Present	Critical	Description
authorityKeyIdentifier	Yes	Non-critical	Byte-for-byte match with the issuing CA's SubjectKeyIdentifier
CRLNumber	Yes	Non-critical	A monotonically increasing non-negative integer not exceeding 2^159
IssuingDistributionPoint	*	-	See Section 7.2.2.1 of this CPS

Revoked certificate components:

Component	Present	Description
serialNumber	Yes	Byte-for-byte match with the serial number of the revoked certificate
revocationDate	Yes	Normally the revocation date; if TrustAsia CA has sufficient evidence that the private key compromise occurred before the revocation date, this date shall be back-dated to the compromise date.
crlEntryExtensions	Possibly	See crlEntryExtensions components table below

crlEntryExtensions components:

CRL Entry Extension	Present	Description
reasonCode	Possibly	When the reason code is 0 (unspecified), it is absent; this reason code is the default option specified in the Subscriber Agreement. When the reason code is any other value, it is present and non-critical.

7.2.2.1 CRL Distribution Points

TrustAsia CA does not use this extension when using a complete CRL. This extension is enabled when using CRL partitions.

7.3 OCSP Profile

If an OCSP response is for a Root CA or Subordinate CA certificate (including cross-certified Subordinate CA certificates) and that certificate has been revoked, the revocationReason field MUST be present in the RevokedInfo of CertStatus.

The indicated CRLReason contains the values permitted for CRLs as specified in Section 7.2.2.

7.3.1 Version Number

OCSP V1 as defined by RFC 6960.

7.3.2 OCSP Extensions

Consistent with RFC 6960. The singleExtensions of OCSP responses do not include the reasonCode (OID 2.5.29.21) CRL entry extension.

8. Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

TrustAsia CA performs the following audits and assessments:

1. An annual security vulnerability assessment and penetration test covering systems, physical facilities, and operational management, with measures taken based on the assessment report to reduce operational risk.
2. An annual operational quality assessment to ensure the reliability, security, and controllability of operational services.
3. An annual audit of physical controls, key management, operational controls, and authentication execution to determine whether actual practices are consistent with established standards and requirements, and to take action based on the review results.
4. An annual operational risk assessment to identify internal and external threats, evaluate the likelihood and potential damage of threat events, and develop and implement remediation plans based on the risk assessment results.
5. In addition to internal audits and assessments, TrustAsia CA engages an independent auditing firm to conduct an annual external audit and assessment in accordance with the WebTrust for CAs audit criteria.

8.2 Identity/Qualifications of Assessor

Internal audits and assessments are performed by TrustAsia CA’s internal audit and assessment team.

External audits are performed by entities with the following qualifications:

1. An independent audit entity;
2. Must be a licensed, qualified assessment body with a good reputation in the industry;
3. Familiarity with computer information security systems, communication network security requirements, PKI technology, standards, and operations;
4. Professional technical skills and tools for examining system operational performance;
5. Qualified to perform WebTrust audits.

8.3 Assessor’s Relationship to Assessed Entity

Internal auditors' positions shall not overlap with those of system administrators, business administrators, or business operators within the institution.

External assessors and TrustAsia CA have a mutually independent relationship, with no interests between the parties sufficient to affect the objectivity of the assessment.

8.4 Topics Covered by Assessment

Audit work covers the following areas:

1. Certificate lifecycle management procedures: reviewing certificate issuance, renewal, and revocation processes. The focus is on verifying whether TrustAsia strictly validates the compliance status of Generator Products through the Compliant Product List during operations, and whether the policy requirement prohibiting re-use of old keys is satisfied.
2. Authentication validation: assessing the accuracy of the CA's verification of Dynamic Evidence provided by Generator Product instances when processing automated certificate enrollment requests. The audit shall confirm whether the CA correctly parses hardware root-of-trust-backed endorsement reports and verifies platform security attributes against the corresponding Assurance Level.
3. Key management practices: the audit scope covers key lifecycle management within TrustAsia CA's infrastructure, as well as oversight and verification practices for key generation environments and protection measures within Subscriber Generator Products.
4. Logical and procedural security controls: verifying whether logical access controls for the CA certification system adhere to the "need-to-know" and "least privilege" principles. The audit shall also cover the implementation of separation of duties to ensure that critical functions such as authentication validation and certificate issuance are performed by different trusted roles.
5. Personnel security and training: verifying the background checks and qualifications of personnel involved in attestation validation and certificate management positions. The focus is on evaluating the completeness of pre-job training, periodic retraining, and assessment records for the technical processes specific to C2PA services.
6. Incident response and disaster recovery procedures: verifying the effectiveness of business continuity plans and disaster recovery plans. The audit shall focus on: notification mechanisms following private key compromise or security incidents, the integrity of off-site backups for critical data, and records of business continuity plan drills.

The independent auditing firm conducts an independent audit of TrustAsia CA in accordance with the requirements of the WebTrust for CAs criteria.

8.5 Actions Taken as a Result of Deficiency

For issues identified in internal audit results, the audit and assessment team is responsible for monitoring the improvement progress of the relevant responsible departments.

Audit report management for C2PA services follows the specifications below to ensure transparency of the assessment process and effectiveness of corrective actions:

1. Clear identification of non-conformities: audit reports shall be issued by the independent audit body, and any non-conformities, security deficiencies, or areas recommended for improvement shall be clearly and accurately identified in the report, enabling relevant parties to assess the operational risk and compliance level of TrustAsia's PKI systems.
2. Corrective actions and continuous improvement: for issues and deficiencies identified in internal or third-party audits, TrustAsia will take the following measures:

a. The audit and assessment team is responsible for overseeing the relevant responsible departments in developing and implementing corrective actions for identified deficiencies.

b. After completing the rectification within the specified timeframe, TrustAsia shall, at the request of the third-party audit body, undergo a re-audit or verification assessment to confirm that the deficiencies have been effectively remediated.

TrustAsia commits to documenting and retaining the results of audit rectifications and their handling as an important reference for subsequent compliance assessments. After the third-party auditing firm completes its assessment, TrustAsia CA will implement rectifications in accordance with its work report and undergo re-audit and assessment.

8.6 Communication of Results

TrustAsia CA publicly discloses audit reports within three months of the end of the audit period. Upon formal request from the C2PA Steering Committee or other authorized parties, TrustAsia shall provide them with complete compliance audit reports and related explanatory documents. If the delay exceeds three months, TrustAsia CA provides an explanatory letter signed by a qualified auditor.

Audit reports satisfy the requirements of the remainder of this Section 8.6 and contain the following clearly identified information:

1. Name of the audited organization;
2. Name and address of the organization performing the audit;
3. SHA-256 fingerprints of all Root and Subordinate CA certificates (including cross-certificates) within the scope of the audit;
4. Audit criteria, with version numbers, used to audit each certificate (and associated key);
5. List of CA policy documents referenced during the audit, with version numbers;
6. Whether the audit covers a period of time or a point in time;
7. Start date and end date of the audit period, for audits covering a period of time;
8. The date for point-in-time audits;
9. Date the report was issued, after the end date or point-in-time date.

TrustAsia CA ensures that a qualified auditor provides an authoritative English-language version of the audit report that is publicly available. The report is provided in PDF format and all required information is searchable as text. Each SHA-256 fingerprint in the audit report is in uppercase letters and does not contain colons, spaces, or line breaks.

8.7 Self-Assessments

In accordance with this CPS, TrustAsia CA's self-assessment framework for C2PA service security specifically incorporates the following security incident review mechanism:

1. Security incident review:

a. In-depth investigation: if a security incident occurs, TrustAsia must conduct a thorough review to accurately identify the root cause, the scope of impact, and lessons learned.

b. Preventive mechanisms: the review process must produce actionable remediation recommendations aimed at effectively preventing future recurrence of similar events that compromise confidentiality, integrity, or availability, through technical or procedural improvements.

2. Information sharing and compliance transparency: relevant security incident review reports must be shared with the C2PA Steering Committee and the C2PA Technical Working Group Conformance Task Force to ensure ecosystem governance parties can promptly understand potential risks and respond collaboratively.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

TrustAsia CA may charge fees to Subscribers for electronic certification-related services provided. Specific fee schedules are determined at its own discretion in accordance with market conditions and regulatory requirements.

If the price specified in an agreement signed by TrustAsia CA differs from the price published by TrustAsia CA, the agreement price shall prevail. Subscribers shall bear all fees incurred in obtaining electronic certification services under this CPS.

9.1.2 Certificate Access Fees

TrustAsia CA does not charge a separate fee for certificate queries during the certificate validity period. If a user has special requirements, additional fees may be charged, to be negotiated with TrustAsia CA.

9.1.3 Revocation or Status Information Access Fees

TrustAsia CA shall not charge fees for access to the Certificate Revocation List (CRL).

9.1.4 Fees for Other Services

If TrustAsia CA provides Subscribers with certificate storage media and related services, TrustAsia CA will specify the price for such items in the agreement signed with the Subscriber or other entity.

Fees for other services that TrustAsia CA will or may provide will be communicated to users in a timely manner.

9.1.5 Refund Policy

If a Subscriber’s contract cannot be fulfilled or the Subscriber’s certificate cannot be used due to reasons attributable to TrustAsia CA, TrustAsia CA will refund the relevant fees to the Subscriber. If the refund is sought for reasons not attributable to TrustAsia CA, the Subscriber Agreement shall govern.

9.1.6 Fee Changes

TrustAsia CA reserves the right to modify its fee structure (including certificate issuance, renewal, and related technical service rates) based on market conditions, technical costs, or governance requirements. Before implementing any fee adjustment, TrustAsia will notify affected Subscribers in accordance with Section 9.12.2 of this CPS. Such advance notice is intended to ensure transparency and predictability of fee management so that Subscribers have sufficient time for budget planning or system configuration adjustments.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

TrustAsia CA has purchased commercial general liability insurance with a policy limit of at least USD 2,000,000 and professional liability/errors and omissions insurance with a policy limit of at least USD 5,000,000.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

If TrustAsia CA breaches its obligations as specified in this CPS, Subscribers may request that TrustAsia CA assume indemnification liability (except where exempted by law or agreement). Upon confirmation by TrustAsia CA, the entity may be indemnified. Indemnification limitations are as follows:

1. All indemnification obligations of TrustAsia CA shall not exceed the insurance coverage specified in Section 9.2.1 of this CPS. The cap on indemnification amounts may be revised by TrustAsia CA depending on the circumstances, and TrustAsia CA will immediately notify the relevant parties upon any such revision.
2. TrustAsia CA assumes indemnification liability for losses only within the certificate validity period.

9.2.4 Subscriber Financial Responsibility

Subscribers bear all fees incurred throughout the full certificate lifecycle, including but not limited to certificate issuance, renewal, revocation, and related technical service fees. Subscribers shall make timely and full payment in accordance with the Subscriber Agreement signed with TrustAsia CA or the officially published price schedule. If a Subscriber fails to fulfil payment obligations on time, TrustAsia has the right to revoke the Subscriber's certificate and terminate services in accordance with this CPS.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

In TrustAsia CA's electronic certification services, the following information is considered confidential:

1. Materials submitted or agreements signed by TrustAsia CA Subscribers when applying for certificates, where the content is not disclosed in the certificate.
2. Audit records including: local logs, server logs, and archived log information, which TrustAsia CA treats as confidential. Only security auditors and business administrators may view such records. They shall not be published outside the company except as required by law.

3. Other personal and corporate information retained by TrustAsia CA and its RA shall be treated as confidential and shall not be disclosed except as required by law.

Except as required by applicable laws, administrative regulations, or mandatory requirements of competent government authorities, or as necessary for independent compliance audits such as WebTrust, TrustAsia commits not to disclose Subscriber Agreements, audit records, or other non-public business information to any third party without the Subscriber’s explicit written consent. TrustAsia will disclose relevant information to law enforcement or administrative authorities when required by law and administrative procedure.

9.3.2 Information Not Within the Scope of Confidential Information

TrustAsia CA treats the following as non-confidential information:

1. Information in certificates and CRLs issued by TrustAsia CA.
2. Information in certificate policies supported by TrustAsia CA and identified in the CPS.
3. Information published on the TrustAsia CA website that is authorized by TrustAsia CA and for use by TrustAsia CA Subscribers only.
4. The confidentiality of other TrustAsia CA information depends on the specific data item and application.

9.3.3 Responsibility to Protect Confidential Information

TrustAsia CA has the responsibility and obligation to appropriately retain and protect the confidential information specified in Section 9.3.1 of this CPS.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

TrustAsia CA respects the privacy rights of Subscribers' personal information and commits to full compliance with national regulations and laws on personal information privacy protection. TrustAsia CA will also ensure that all employees strictly adhere to security and confidentiality standards to protect personal privacy.

9.4.2 Information Treated as Private

TrustAsia CA treats as private all personal information related to certificates or CRLs that is not publicly available in their content. TrustAsia CA uses appropriate safeguards and reasonable care to protect privacy.

9.4.3 Information Not Deemed Private

Certificate information held by the Subscriber, and certificate status information, are not treated as private.

9.4.4 Responsibility to Protect Private Information

TrustAsia CA has the responsibility and obligation to appropriately retain and protect the personal privacy of certificate applicants as specified in Section 9.4.2 of this CPS.

9.4.5 Notice and Consent to Use Private Information

TrustAsia CA will take appropriate steps to protect the personal privacy of Subscribers and will use reliable security measures to protect stored personal privacy information. Unless required by law or mandatory government requirements, TrustAsia CA commits not to provide Subscribers' personal information to unrelated third parties (including companies or individuals) without the Subscriber’s consent.

9.4.5.1 Purpose Limitation

The collection and use of personal information is strictly limited to business purposes explicitly specified in this CPS, such as identity authentication, certificate issuance, and management. Without the Subscriber’s consent, TrustAsia CA commits not to provide personal information other than information embedded in the certificate to any third party, except as required by laws, regulations, or mandatory government requirements.

9.4.5.2 Data Subject Rights

Subscribers have the right to access, correct, or lawfully request deletion of their personal information retained by TrustAsia CA. TrustAsia CA respects and ensures Subscribers' control over their private data, on the premise of compliance with national laws and regulations and the regulatory constraints of electronic certification services.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Pursuant to applicable laws, administrative regulations, rules, decisions, orders, and other instruments, and where required by judicial enforcement or legally authorized administrative enforcement, TrustAsia CA may be required to provide relevant information to law enforcement or administrative enforcement authorities, with or without the knowledge of the Subscriber.

9.4.7 Other Information Disclosure Circumstances

If a Subscriber requests TrustAsia CA to provide specific customer support services, such as material mailing, TrustAsia CA may need to provide the Subscriber’s name, mailing address, and other information to third parties such as mailing companies.

Disclosure of other information is subject to applicable law and the Subscriber Agreement.

9.5 Intellectual Property Rights

1. TrustAsia CA holds and retains all intellectual property rights in the certificates and all software provided by TrustAsia CA.
2. TrustAsia CA has ownership, title, and beneficial interest rights in the digital certificate system

software.

3. TrustAsia CA has the right to determine which software system to adopt.
4. All information published on the TrustAsia CA website is the property of TrustAsia CA; without written permission from TrustAsia CA, others may not reproduce it for commercial purposes.
5. Certificates and CRLs issued by TrustAsia CA are property controlled by TrustAsia CA.
6. External operational management policies and specifications are the property of TrustAsia CA.
7. Distinguished Names (DNs) used to represent entities in TrustAsia CA's domain in the directory, and certificates issued to end entities within that domain, are the property of TrustAsia CA.
8. This CPS is licensed under a "Creative Commons Attribution-NoDerivatives (CC-BY-ND) 4.0 International License."

9.5.1 Subscriber Ownership

Subscribers hold complete and lawful ownership and control over all intellectual property rights relating to the "Claim Generation implementation" that uses certificates issued under this CPS for signing.

9.5.2 CA Ownership

TrustAsia makes no claims of ownership or rights over the Subscriber's technical implementation described above or the intellectual property rights relating thereto.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

TrustAsia CA's commitments to Subscribers in the course of providing electronic certification services are as follows:

1. Name Usage Warranty: TrustAsia CA warrants that it has implemented and strictly followed the procedures described in this CPS to verify that the Applicant has legitimate rights to or control over the product name and related identifiers included in the certificate.
2. Issuance Authorization Warranty: TrustAsia CA warrants that it has verified through formal procedures that the certificate Subject has authorized issuance, confirmed that the Applicant Representative has legitimate authority to request the certificate, and that the relevant verification process has been accurately disclosed in this document.
3. Information Accuracy Warranty: TrustAsia CA warrants that it has executed complete procedures to verify the accuracy of all information in the certificate and has strictly followed the verification logic disclosed in this CPS during the issuance process.
4. Agreement Compliance: TrustAsia CA confirms that a legally effective Subscriber Agreement has been signed with the Subscriber, or that the Subscriber's representative has expressly acknowledged the terms of use.
5. Status Service: TrustAsia CA maintains a publicly accessible repository available 7x24 hours that provides real-time valid or revoked certificate status.

6. Timely Revocation: TrustAsia CA commits to fulfilling revocation obligations within the established timeframes when revocation circumstances specified in this CPS occur.

Root CA Responsibility: TrustAsia's Root CA assumes full indemnification and joint and several liability for the compliance, performance, and warranty obligations of its Subordinate Issuing CAs, as if the Root CA had itself issued those certificates.

9.6.2 RA Representations and Warranties

TrustAsia CA's Registration Authority makes the following commitments in the course of participating in electronic certification services:

1. The registration process provided to Subscribers fully complies with all material requirements of TrustAsia CA's CPS.
2. Certificate information will not be inconsistent with the certificate applicant's information due to the RA's error when TrustAsia CA generates the certificate.
3. TrustAsia CA will submit revocation, renewal, and other service applications in a timely manner as required by the CPS.

9.6.3 Subscriber Representations and Warranties

By accepting a certificate issued by TrustAsia CA, a Subscriber is deemed to have made the following commitments to TrustAsia CA and relevant parties relying on the certificate:

1. Acceptance of a certificate signifies the Subscriber's acknowledgment and acceptance of all terms and conditions in this CPS and the applicable Subscriber Agreement.
2. Digital signatures will only be created during the certificate's validity period.
3. The information provided by the Subscriber to TrustAsia CA when applying for the certificate is truthful, complete, and accurate. The Subscriber agrees to assume any legal liability for providing false or fraudulent information. Where an agent is involved, the Subscriber and the agent bear joint and several liability. The Subscriber has a responsibility to notify TrustAsia CA or its authorized certificate services provider of any misrepresentation or omission made by the agent.
4. Each signature made using the private key corresponding to the public key in the Subscriber's certificate is the Subscriber's own signature; when the signature is made, the certificate is valid (not expired or revoked) and the certificate's private key is accessed and used by the Subscriber.
5. Unless expressly stipulated in a written agreement between the Subscriber and the CA, the Subscriber warrants not to engage in the business conducted by the CA (or similar entity).
6. Upon accepting the certificate, the Subscriber shall assume the following responsibilities: maintaining control over its private key at all times, using trusted systems, and taking reasonable precautions to prevent loss, disclosure, tampering, or unauthorized use of the private key.
7. The Subscriber shall not refuse any announcement, change, update, or upgrade published by TrustAsia CA, including but not limited to modifications to policies and specifications and additions to or removal of certificate services.

8. Certificates shall be used lawfully within the scope of use specified in this CPS; certificates shall only be used for authorized or other lawful purposes.
9. Reasonable and secure measures shall be taken to prevent events such as loss, disclosure, or tampering of certificate private keys.

9.6.4 Relying Party Representations and Warranties

1. Comply with all provisions of this CPS.
2. Confirm that the certificate is used within the specified scope and period.
3. Verify the certificate chain before relying on a certificate.
4. Verify whether the certificate has been revoked by querying the CRL or OCSP before relying on a certificate.
5. If a Relying Party fails to perform reasonable checks due to negligence or other reasons, the Relying Party is willing to compensate TrustAsia CA for any resulting losses, and shall bear any resulting losses to itself or others.
6. Relying Parties shall not refuse any announcement, change, update, or upgrade published by TrustAsia CA, including but not limited to modifications to policies and specifications and additions to or removal of certificate services.

9.6.5 Representations and Warranties of Other Participants

Other participants in electronic certification activities shall commit to complying with all provisions of this CPS.

9.7 Disclaimers of Warranties

Except for the express commitments in Section 9.6.1 of this CPS, TrustAsia CA assumes no other form of guarantee or obligation:

1. TrustAsia CA does not warrant the content of representations made by Subscribers, Relying Parties, or other participants.
2. TrustAsia CA makes no warranty regarding any software used in electronic certification activities.
3. TrustAsia CA assumes no liability for the use of certificates for purposes beyond the specified scope.
4. TrustAsia CA does not assume liability for service interruptions caused by force majeure, such as war or natural disasters, and any resulting customer losses.
5. TrustAsia CA's liability may be disclaimed when a Subscriber breaches the commitments in Section 9.6.3 of this CPS, or when a Relying Party breaches the commitments in Section 9.6.4 of this CPS.
6. TrustAsia CA assumes no liability for incorrect issuance, delay, interruption, or inability to issue digital certificates, or for the suspension or termination of all or part of certificate services, caused by technical failures such as equipment or network failures. Such "technical failures" include but are not limited to: failures caused by associated entities such as power,

telecommunications, or communications departments; hacker attacks; TrustAsia CA's equipment or network failures.

7. TrustAsia CA has carefully followed the digital certificate authentication business rules stipulated by national laws and regulations, yet losses still occur.

9.8 Limitations of Liability

Where a Subscriber suffers losses as a result of civil activities conducted using TrustAsia CA's electronic certification services, TrustAsia CA shall assume limited indemnification liability not exceeding the limits specified in Section 9.9 of this CPS.

9.9 Indemnities

9.9.1 Indemnification by CA

If TrustAsia CA breaches the representations in Section 9.6.1 of this CPS, Subscribers may request that TrustAsia CA assume indemnification liability (except where exempted by law or agreement). The cap on legal liability for direct losses is:

- Under no circumstances shall the indemnification amount per certificate exceed 10 times the market purchase price of that certificate.
- The indemnification amount per certificate per Subscriber or Relying Party shall not be less than USD 2,000.

TrustAsia CA assumes limited indemnification liability in the following circumstances:

1. TrustAsia CA incorrectly issues a certificate to a third party other than the Subscriber, causing the Subscriber to suffer losses;
2. When the information or materials submitted by the Subscriber are accurate and truthful, the certificate issued by TrustAsia CA contains erroneous information, causing the Subscriber to suffer losses;
3. Where TrustAsia CA knowingly issues a certificate to a Subscriber despite being aware of false or fraudulent information submitted by the Subscriber, causing the genuine entity to suffer losses;
4. Due to reasons attributable to TrustAsia CA, the certificate private key is deciphered, stolen, or disclosed, causing the Subscriber to suffer losses;
5. TrustAsia CA's failure to revoke a certificate in a timely manner causes the Subscriber to suffer losses.

In addition, TrustAsia CA's indemnification limitations are as follows:

1. All indemnification obligations of TrustAsia CA shall not exceed the amount specified in Section 9.2.1 of this CPS. This cap may be revised by TrustAsia CA depending on the circumstances, and TrustAsia CA will immediately notify the relevant parties upon any such revision.
2. TrustAsia CA is not liable for losses caused by reasons attributable to the Subscriber or Relying

Party; such losses shall be borne by the Subscriber or Relying Party.

3. TrustAsia CA assumes indemnification liability for losses only within the certificate validity period.

9.9.2 Indemnification by Subscribers

Subscribers shall assume indemnification liability if the following circumstances cause TrustAsia CA or Relying Parties to suffer losses:

1. When applying for certificate registration, the Subscriber intentionally, negligently, or maliciously provides untruthful information, causing TrustAsia CA or a third party to suffer harm;
2. The Subscriber's intentional or negligent private key disclosure or loss, the Subscriber's failure to notify TrustAsia CA despite knowing the private key has been disclosed or lost, or the improper delivery of the private key to another party for use, causing TrustAsia CA or a third party to suffer harm;
3. The Subscriber's use of the certificate violates this CPS and related operational specifications, or the certificate is used for purposes outside the scope of this CPS;
4. After the Subscriber or another entity entitled to request revocation of the certificate has submitted a revocation request, and before TrustAsia CA publishes the revocation information for the certificate, if the certificate is used to conduct illegal transactions or disputes arise from transactions, and if TrustAsia CA has performed the relevant operations in accordance with this CPS, the Subscriber must bear all indemnification liability;
5. Information or materials provided are untruthful, incomplete, or inaccurate;
6. Information in the certificate changes but the Subscriber continues using the certificate without timely notifying TrustAsia CA and Relying Parties;
7. Failure to implement effective protective measures for the private key, resulting in loss, compromise, theft, or disclosure of the private key;
8. Failure to stop using the certificate and notify TrustAsia CA and Relying Parties in a timely manner upon becoming aware of private key loss or risk;
9. Continued use of the certificate after it has expired;
10. Certificate information in the Subscriber's certificate infringes upon the intellectual property rights of a third party;
11. Use of the certificate outside the specified scope, such as engaging in illegal activities.

9.9.3 Indemnification by Relying Parties

Relying Parties shall assume indemnification liability if the following circumstances cause TrustAsia CA or Subscribers to suffer losses:

1. Failure to fulfil obligations specified in the agreement between TrustAsia CA and the Relying Party and in this CPS;
2. Failure to conduct reasonable review in accordance with this CPS, causing TrustAsia CA or a third party to suffer harm;

3. Reliance on a certificate under unreasonable circumstances, such as where the Relying Party is aware that the certificate is being used beyond its permitted scope or validity period, or that the certificate has been or may have been stolen, yet still relies on it;
4. Failure by the Relying Party to verify the certificate chain;
5. Failure by the Relying Party to confirm whether the certificate has been revoked by querying the CRL or OCSP.

9.10 Term and Termination

9.10.1 Term

Any revision to this CPS takes effect upon publication to TrustAsia CA's online repository and remains effective until replaced by a new version or until TrustAsia CA ceases operations.

9.10.2 Termination

This CPS terminates when TrustAsia CA ceases operations.

9.10.3 Effect of Termination and Survival

Upon termination of this CPS, its effect terminates simultaneously. However, with respect to legal facts that occurred prior to the date of termination, the provisions of this CPS regarding the responsibilities and exemptions of all parties shall continue to apply, including but not limited to provisions relating to audit, confidential information, privacy protection, intellectual property, indemnification, and limited liability clauses, which shall survive the termination of this CPS.

If any provisions of this CPS, Subscriber Agreement, Relying Party Agreement, or other agreements become invalid for any reason, such as content modification or conflict with applicable law, this shall not affect the legal validity of other provisions in the document.

9.11 Individual Notices and Communications with Participants

Where necessary, such as when proactively revoking a Subscriber's certificate, discovering that a Subscriber is using the certificate for unauthorized purposes, or other acts by the Subscriber that violate the Subscriber Agreement, TrustAsia CA will individually notify Subscribers and Relying Parties by email or other means. TrustAsia CA publicly discloses accurate and up-to-date contact information to facilitate effective communication.

9.12 Amendments

9.12.1 Amendment Procedures

Authorized by the TrustAsia CA Security Policy Committee, the CPS drafting team may amend this CPS from time to time to ensure that it complies with national laws and regulations, regulatory authority requirements, and relevant international standards, and meets the practical needs of

certification business operations.

Amendments and updates to this CPS are proposed by the CPS drafting team, approved by the TrustAsia CA Security Policy Committee, and completed by the CPS drafting team. The revised CPS is officially published externally after approval by the TrustAsia CA Security Policy Committee. Continued use of certificates issued by TrustAsia CA following any revision to this CPS constitutes acceptance by the Subscriber of the revised terms and conditions.

9.12.2 Notification Mechanism and Period

Revised versions of the CPS, once approved, will be published immediately on the TrustAsia CA official website. For amendments that require notification by email, letter, media, or other means, TrustAsia CA will notify the relevant parties within a reasonable time, where "reasonable time" is defined as sufficient to minimize the impact on the relevant parties.

9.12.3 Circumstances Under Which OID Must Be Changed

TrustAsia CA is solely responsible for determining whether a revision to the CPS requires a change to the OID.

9.12.4 Circumstances Under Which the CPS Must Be Revised

Circumstances in which TrustAsia CA must amend this CPS include: inconsistencies between the CPS and governing law, or explicit requirements for changes or adjustments to the institution’s certification business from national regulatory authorities.

9.13 Dispute Resolution Provisions

In the event of disputes arising among TrustAsia CA, Subscribers, Relying Parties, and other end entities in the course of electronic certification activities, the parties shall first attempt to resolve the dispute amicably through consultation pursuant to applicable agreements. If consultation fails, the parties may resolve the dispute through legal channels.

Any litigation brought against TrustAsia CA concerning any matter covered by this CPS shall be submitted to the jurisdiction of the People’s Court in the location of TrustAsia CA’s business registration.

9.14 Governing Law

The C2PA Certificate Policy and any agreements arising therefrom shall be governed by and construed in accordance with the laws of the State of Delaware, USA. For any disputes, litigation, or legal proceedings arising from related C2PA service agreements, the parties consent to the exclusive jurisdiction of the state or federal courts of the State of Delaware, USA.

9.15 Compliance with Applicable Law

This CPS is subject to applicable national, state, local, and foreign laws, regulations, ordinances, decrees, and orders, including but not limited to restrictions on the export or import of software,

hardware, or technical information.

All entities operating under TrustAsia CA pursuant to this CPS shall comply with applicable law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

The complete document structure of this CPS includes: the title, table of contents, and main body. Substitute content for revisions to the table of contents and main body shall completely supersede all previous sections and shall be placed on the TrustAsia CA website for reference and review.

9.16.1.1 CA and C2PA Governance Body

The rights and obligations between TrustAsia CA and the C2PA Governance Body are governed by the Electronic Certification Service Authority Agreement signed by both parties and by this CPS.

9.16.1.2 CA and Subscriber

The legal relationship between TrustAsia CA and Subscribers is governed by the Subscriber Agreement signed by both parties and the relevant provisions of this CPS.

9.16.2 Assignment

TrustAsia CA declares that, in accordance with the rights and obligations of the parties to the certification entity described in this CPS, no party may assign such rights and obligations by any means without the prior written consent of TrustAsia CA.

9.16.3 Severability

If any part of this CPS is determined to be incorrect or invalid, the other parts of this CPS shall remain valid until this CPS is updated.

If any provision or clause of this CPS is found to be unenforceable by a court or other body with authority, the remainder of this CPS shall remain valid.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

TrustAsia CA declares that if any entity such as a Subscriber or Relying Party fails to enforce a provision of this CPS, this shall not be construed as that entity waiving enforcement of that or any other provision in the future.

9.16.5 Force Majeure

If compliance with, delay in, or inability to fulfil the warranty obligations specified in this CPS is caused by force majeure such as war, epidemic, fire, earthquake, or natural disaster, TrustAsia CA shall not be liable for such events.

9.17 Other Provisions

TrustAsia CA retains the final right of interpretation of this CPS.

10. Appendix A – Validation Requirements

10.1 Validation Items and Requirements

TrustAsia CA's authentication requirements for Subscriber certificates are as follows:

Validation Item	Validation Requirement
CSR Validation	Verify the CSR signature data Verify the CSR public key length Verify whether the CSR public key is a weak key
Organization Validation	Verify that the Applicant's name is legitimate and compliant Verify that the Applicant is legally existing and operating Verify the country, province, city, and address of the Applicant's location Verify a telephone number, fax number, email address, or postal delivery address as a verified means of communication for the Applicant Comply with CPS Section 3.2.2
Individual Identity Validation	Verify the Applicant's application intent by contacting the Applicant Representative.
Lawyer Identity Validation	Verify the lawyer's relevant information, examine the lawyer's practicing certificate or inquire about its registration, and confirm the lawyer's practice status with the law firm where the lawyer is registered; Confirm the authenticity and accuracy of the signed legal opinion letter with the lawyer.

Validation Item	Validation Requirement
Compliance Validation	Compliance validation items for Assurance Level 1 and 2 baseline: • Verify the capability to automatically apply for certificates • Verify the recordID (UUID) in the CPL • Verify that the DN matches the information in the CPL record • Verify the Maximum Assurance Level recorded in the CPL • The Generator Product is present in the CPL with a status showing "conformant" Dynamic Evidence validation items for Assurance Level 2: • Attestation of the cryptographic hardware module used to generate the private key • Generator Product platform attestation report • Verification method for the Maximum Assurance Level

11. Appendix B – Certificate Profiles

11.1 Root CA Certificate

Note: Certificates are divided into RSA and ECC series; the template reflects where they differ.

Certificate Field		Critical	Content
Version			v3
Serial Number			Contains at least 64 bits from a CSPRNG
TBSCertificate Signature			TrustAsia C2PA RSA Root CA: sha384withRSA TrustAsia C2PA ECC Root CA: sha384withECDSA
Issuer			Byte-for-byte match with Subject
Validity: notBefore			No more than 24 hours before time of issuance
Validity: notAfter			25 years
Subject	Common Name (CN)		TrustAsia C2PA RSA Root CA or TrustAsia C2PA ECC Root CA
	Organization (O)		TrustAsia Technologies, Inc.
	Country (C)		CN
Subject Public Key Info			RSA 4096 ECDSA P-384
Signature Algorithm			Matches TBSCertificate
Extension: subjectKeyIdentifier		Non-critical	160-bit SHA-1 hash of subjectPublicKey, per RFC 5280
Extension: authorityKeyIdentifier		Non-critical	Matches subjectKeyIdentifier
Extension: basicConstraints		Critical	Subject Type=CA Path Length Constraint=2
Extension: keyUsage		Critical	keyCertSign, cRLSign

11.2 Intermediate CA Certificates

11.2.1 C2PA Claim Signing Intermediate CA Certificate

Certificate Field	Critical	Content
Version		v3

Certificate Field		Critical	Content
Serial Number			Contains at least 64 bits from a CSPRNG
TBSCertificate Signature			TrustAsia C2PA Claim Signing RSA CA 2026: sha384withRSA TrustAsia C2PA Claim Signing ECC CA 2026: sha384withECDSA
Issuer			Byte-for-byte match with issuing CA's Subject
Validity: notBefore			No more than 24 hours before time of issuance
Validity: notAfter			Not to exceed 1,827 days
Subject	Common Name (CN)		TrustAsia C2PA Claim Signing RSA CA 2026 or TrustAsia C2PA Claim Signing ECC CA 2026
	Organization (O)		TrustAsia Technologies, Inc.
	Country (C)		CN
Subject Public Key Info			RSA 4096 or ECDSA P-384
Signature Algorithm			Matches TBSCertificate
Extension: subjectKeyIdentifier		Non-critical	160-bit SHA-1 hash of subjectPublicKey, per RFC 5280
Extension: authorityKeyIdentifier		Non-critical	Matches issuing certificate's subjectKeyIdentifier
Extension: certificatePolicies		Non-critical	Policy Identifier=1.3.6.1.4.1.62558.1.1
Extension: basicConstraints		Critical	Subject Type=CA Path Length Constraint=0
Extension: keyUsage		Critical	keyCertSign, cRLSign
Extension: extKeyUsage		Non-critical	c2pa-kp-claimSigning(1.3.6.1.4.1.62558.2.1) id-kp-emailProtection(1.3.6.1.5.5.7.3.4) id-kp-documentSigning(1.3.6.1.5.5.7.3.36)
Extension: authorityInfoAccess		Non-critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.c2pa.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.c2pa.trustasia.com/<Issuername>

Certificate Field	Critical	Content
Extension: cRLDistributionPoints	Non-critical	CRL HTTP URL= http://crl.c2pa.trustasia.com/<Issuername>.crl

11.2.2 C2PA Timestamp Signing Intermediate CA Certificate

Certificate Field		Critical	Content
Version			v3
Serial Number			Contains at least 64 bits from a CSPRNG
TBSCertificate Signature			TrustAsia C2PA TSA RSA CA 2026: sha384withRSA TrustAsia C2PA TSA ECC CA 2026: sha384withECDSA
Issuer			Byte-for-byte match with issuing CA's Subject
Validity: notBefore			No more than 24 hours before time of issuance
Validity: notAfter			15 years
Subject	Common Name (CN)		TrustAsia C2PA TSA RSA CA 2026 or TrustAsia C2PA TSA ECC CA 2026
	Organization (O)		TrustAsia Technologies, Inc.
	Country (C)		CN
Subject Public Key Info			RSA 4096 or ECDSA P-384
Signature Algorithm			Matches TBSCertificate
Extension: subjectKeyIdentifier		Non-critical	160-bit SHA-1 hash of subjectPublicKey, per RFC 5280
Extension: authorityKeyIdentifier		Non-critical	Matches issuing certificate's subjectKeyIdentifier
Extension: certificatePolicies		Non-critical	Policy Identifier=1.3.6.1.4.1.62558.1.1
Extension: basicConstraints		Critical	Subject Type=CA Path Length Constraint=0
Extension: keyUsage		Critical	keyCertSign, cRLSign
Extension: extKeyUsage		Non-critical	id-kp-timeStamping(1.3.6.1.5.5.7.3.8)

Certificate Field	Critical	Content
Extension: authorityInfoAccess	Non-critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.c2pa.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.c2pa.trustasia.com/<Issuername>
Extension: cRLDistributionPoints	Non-critical	CRL HTTP URL= http://crl.c2pa.trustasia.com/<Issuername>.crl

11.3 Subscriber (End-Entity) Certificates

11.3.1 C2PA Assurance Level 1 Certificate

Certificate Field		Critical	Content
Version			v3
Serial Number			Contains at least 64 bits from a CSPRNG
TBSCertificate Signature			sha256withRSA or sha384withRSA or sha384withECDSA or Ed25519
Issuer			Byte-for-byte match with issuing CA's Subject
Validity: notBefore			No more than 24 hours before time of issuance
Validity: notAfter			Not to exceed 366 days
Subject	Common Name (CN)		Consistent with the C2PA Compliant Product DN content; CN, O, C are required; OU is present if it exists in the CPL record
	Organization (O)		
	Organizational Unit (OU)		
	Country (C)		
Subject Public Key Info			RSA 2048, 3072, or 4096; ECC P-256, P-384, or P-521; or Ed25519
Signature Algorithm			Matches TBSCertificate
Extension: subjectKeyIdentifier		Non-critical	160-bit SHA-1 hash of subjectPublicKey, per RFC 5280
Extension: authorityKeyIdentifier		Non-critical	Matches issuing certificate's subjectKeyIdentifier

Certificate Field	Critical	Content
Extension: certificatePolicies	Non-critical	Policy Identifier=1.3.6.1.4.1.62558.1.1
Extension: basicConstraints	Critical	Subject Type=End Entity Path Length Constraint=None
Extension: keyUsage	Critical	digitalSignature, nonRepudiation
Extension: extKeyUsage	Non-critical	c2pa-kp-claimSigning(1.3.6.1.4.1.62558.2.1) id-kp-emailProtection(1.3.6.1.5.5.7.3.4) id-kp-documentSigning(1.3.6.1.5.5.7.3.36)
Extension: authorityInfoAccess	Non-critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.c2pa.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.c2pa.trustasia.com/<Issuername>
Extension: cRLDistributionPoints	Non-critical	CRL HTTP URL= http://crl.c2pa.trustasia.com/<Issuername>.crl
Extension: C2PA Assurance Level(1.3.6.1.4.1.62558.3)	Non-critical	1.3.6.1.4.1.62558.3.10
Extension: C2PA CPL Record ID(1.3.6.1.4.1.62558.4)	Non-critical	36-character UUID of the Generator Product in the CPL

11.3.2 C2PA Assurance Level 2 Certificate

Certificate Field	Critical	Content
Version		v3
Serial Number		Contains at least 64 bits from a CSPRNG
TBSCertificate Signature		sha256withRSA or sha384withRSA or sha384withECDSA or Ed25519
Issuer		Byte-for-byte match with issuing CA's Subject
Validity: notBefore		No more than 24 hours before time of issuance
Validity: notAfter		Not to exceed 90 days

Certificate Field		Critical	Content
Subject	Common Name (CN)		Consistent with the C2PA Compliant Product DN content; CN, O, C are required; OU is optional
	Organization (O)		
	Organizational Unit (OU)		
	Country (C)		
Subject Public Key Info			RSA 2048, 3072, or 4096; ECC P-256, P-384, or P-521; or Ed25519
Signature Algorithm			Matches TBSCertificate
Extension: subjectKeyIdentifier		Non-critical	160-bit SHA-1 hash of subjectPublicKey, per RFC 5280
Extension: authorityKeyIdentifier		Non-critical	Matches issuing certificate's subjectKeyIdentifier
Extension: certificatePolicies		Non-critical	Policy Identifier=1.3.6.1.4.1.62558.1.1
Extension: basicConstraints		Critical	Subject Type=End Entity Path Length Constraint=None
Extension: keyUsage		Critical	digitalSignature, nonRepudiation
Extension: extKeyUsage		Non-critical	c2pa-kp-claimSigning(1.3.6.1.4.1.62558.2.1) id-kp-emailProtection(1.3.6.1.5.5.7.3.4) id-kp-documentSigning(1.3.6.1.5.5.7.3.36)
Extension: authorityInfoAccess		Non-critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.c2pa.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.c2pa.trustasia.com/<Issuername>
Extension: cRLDistributionPoints		Non-critical	CRL HTTP URL= http://crl.c2pa.trustasia.com/<Issuername>.crl
Extension: C2PA Assurance Level(1.3.6.1.4.1.62558.3)		Non-critical	1.3.6.1.4.1.62558.3.20
Extension: C2PA CPL Record ID(1.3.6.1.4.1.62558.4)		Non-critical	36-character UUID of the Generator Product in the CPL

11.3.3 OCSP Signing Certificate

Certificate Field		Critical	Content
Version			v3
Serial Number			Contains at least 64 bits from a CSPRNG
TBSCertificate Signature			sha384withRSA or sha384withECDSA
Issuer			Byte-for-byte match with issuing CA's Subject
Validity: notBefore			No more than 24 hours before time of issuance
Validity: notAfter			Not to exceed the notAfter of the signing CA
Subject	Common Name (CN)		<CA Common Name> - OCSP Responder
	Organization (O)		TrustAsia Technologies, Inc.
	Country (C)		CN
Subject Public Key Info			RSA 2048, 3072, or 4096; or ECDSA P-256 or P-384
Signature Algorithm			Matches TBSCertificate
Extension: subjectKeyIdentifier		Non-critical	160-bit SHA-1 hash of subjectPublicKey, per RFC 5280
Extension: authorityKeyIdentifier		Non-critical	Matches issuing certificate's subjectKeyIdentifier
Extension: basicConstraints		Critical	Subject Type=End Entity Path Length Constraint=None
Extension: keyUsage		Critical	digitalSignature
Extension: extKeyUsage		Non-critical	id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9)
Extension: id-pkix-ocsp-nocheck(1.3.6.1.5.5.7.48.1.5)		Non-critical	0x0500

11.3.4 Timestamp Certificate

Certificate Field	Critical	Content
Version		v3
Serial Number		Contains at least 64 bits from a CSPRNG
TBSCertificate Signature		sha256withRSA or sha384withRSA or sha384withECDSA or Ed25519
Issuer		Byte-for-byte match with issuing CA's Subject

Certificate Field		Critical	Content
Validity: notBefore			No more than 24 hours before time of issuance
Validity: notAfter			Not to exceed 4,110 days
Subject	Common Name (CN)		TrustAsia C2PA Time-Stamp Signing RSA or ECC <Year>
	Organization (O)		TrustAsia Technologies, Inc.
	Country (C)		CN
Subject Public Key Info			RSA 2048, 3072, or 4096; ECC P-256, P-384, or P-521; or Ed25519
Signature Algorithm			Matches TBSCertificate
Extension: subjectKeyIdentifier		Non-critical	160-bit SHA-1 hash of subjectPublicKey, per RFC 5280
Extension: authorityKeyIdentifier		Non-critical	Matches issuing certificate's subjectKeyIdentifier
Extension: certificatePolicies		Non-critical	Policy Identifier=1.3.6.1.4.1.62558.1.1
Extension: basicConstraints		Critical	Subject Type=End Entity Path Length Constraint=None
Extension: keyUsage		Critical	digitalSignature, nonRepudiation
Extension: extKeyUsage		Non-critical	id-kp-timeStamping(1.3.6.1.5.5.7.3.8)
Extension: authorityInfoAccess		Non-critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.c2pa.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.c2pa.trustasia.com/<Issuername>
Extension: cRLDistributionPoints		Non-critical	CRL HTTP URL= http://crl.c2pa.trustasia.com/<Issuername>.crl