Trufo
CP + CPS

Certificate Policy
Certification Practices Statement
Version 1.0

October 2024

trufo.ai

Table of Contents

1. Introduction

Trufo is a Certification Authority (CA) that manages a public key infrastructure (PKI) according to the Trufo Certificate Policy (CP) and Certification Practice Statement (CPS). The PKI is designed to support the validation of source identities and content annotations in the context of an authenticity infrastructure for digital content. To achieve this, the Trufo Certificate Authority (TCA) performs PKI services that include the issuing, renewing, and revoking of digital certificates. The TCA further maintains and publishes a Certificate Revocation List (CRL).

1.1. Overview

This document details the Certificate Policy (CP) and Certification Practice Statement (CPS) of entities participating in Trufo's public key infrastructure (PKI). It describes the requirements set forth by Trufo Inc. for the management of Certificates trusted by the PKI. It further describes the practices employed by the TCA, wherein said practices are defined in accordance with said CP requirements.

This CP/CPS governs Certificate practices under guidelines adopted by the Certificate Authority/Browser (CAB) Forum, in particular:

- The CAB Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates (PTCs).
- The CAB Forum Guidelines for Extended Validation Certificates (EVCs).
- The CAB Forum Guidelines for the Issuance and Management of Code Signing Certificates (CSCs).
- Trufo timestamping services follow IETF RFC3161.

Furthermore, since authenticity infrastructure for digital content is a nascent domain, this CP/CPS will also comply with anticipated best practices put forth specifically for this PKI context, in particular:

- In-progress conformance standards specified by AISIC and other government-affiliated working groups.
- In-progress conformance standards specified by C2PA, IPTC, and other working groups on metadata and provenance.

This CP/CPS is one of several documents that governs Certificate practices provided by Trufo. Other documents include but are not limited to specific agreements with other parties.

1.2. Document Name and Identification

The name of this document is the Trufo Certificate Policy and Certification Practices Statement (“this” CP/CPS). This document is organized according to the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647).

The OID assigned to Trufo by IANA is:

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

A special OID arc is allocated for this CP/CPS:

1.3.6.1.4.1.62524(.1.1 – CP/CPS)(.1.0 – version)

This CP/CPS was first published on October 23, 2024. The table below specifies all revisions made:

Date	Version	Changelog
2024/10/23	1.0	Initial publication.

The provisions of this CP/CPS will be amended periodically. The most recent version is publicly available at https://trufo.ai/cpcps.

1.3. PKI Participants

There are four primary roles that entities may take on in Trufo’s PKI:

- A Certification Authority (CA) is an entity responsible for issuing Certificates.
- A Registration Authority (RA) is responsible for identifying, authenticating, and managing a Subscriber’s Certificate Request information.
- A Subscriber is any entity that has been issued a Certificate by the TCA.
- A Relying Party is any entity that performs functions that rely on a Certificate issued by a CA.

The term “entity” corresponds to a wide variety of PKI participants, including but not limited to: organizations, individuals, physical devices, application instances, and combinations thereof.

1.3.1. Certification Authorities

Trufo operates a root Certification Authority (RCA) and a number of issuing Certification Authorities (ICAs). The ICAs are broadly defined by the security requirements of the type of entity they serve. Both the RCA and the ICAs are managed by the Trufo Policy Authority (TPA), the members of which are appointed by Trufo’s executive management.

Trufo also supports external intermediate Certification Authorities (ECAs), provided that they follow this CP/CPS. Trufo further operates Timestamping Authorities (TAs).

1.3.2. Registration Authorities

Any CA utilizes at least one RA for identifying, authenticating, and managing a Subscriber’s Certificate Request information. Depending on the registration requirements of this CA, a Subscriber may need to perform specific registration operations, some of which may require in-person validation. These operations are performed by RAs operated under the supervision of Trufo.

Trufo’s RCA and ICAs may act as RAs for the Certificates they issue. Trufo may operate separate RAs, broadly defined by the access method used by the Subscriber.

Trufo may also delegate the verification of Certificate Requests to enterprise RAs (ERAs). ERAs may only verify information for entities associated with said enterprise entity. Furthermore, this association information is retained in the issued Certificate.

Trufo shall verify that any delegated RA meets the requirements set forth in this CP/CPS.

1.3.3. Subscribers

Subscribers to Trufo’s services are entities that have been issued a Certificate by the TCA. For conformance purposes, the bound entity can be either the Subscriber (in the case of a natural person or a legal entity) or the organization that is responsible for the Subscriber (in the case of a physical device or an application instance).

An Applicant is a Subscriber that is seeking the issuance or the renewal of a Certificate.

1.3.4. Relying Parties

Relying Parties are entities that perform functions that rely on a Certificate issued by a CA. Before relying on a Trufo certificate, Relying Parties should read this CP/CPS and assess the certificate to determine the extent to which the certificate should be trusted.

1.3.5. Other Participants

Subscribers may use Timestamp Authorities to provide proof that specified data existed at a specific time.

1.4. Certificate Usage

Subscribers and Relying Parties must use certificates in accordance with the relevant agreements.

1.4.1. Appropriate Certificate Uses

A Certificate issued by Trufo under the guidelines of this CP/CPS shall be used only for the following purposes:

- Code Signing and EV Code Signing, recommended.
    - Used to sign hashes and other structured and unstructured information, in particular in the context of content annotations comprising data about a Subscriber entity or an item of digital media.
- Document Signing, recommended.
    - Used to sign electronic documents, which in this context is primarily digital audiovisual media (images, videos, audio).
- DV/OV/EV TLS, if needed.
    - Used for secure online communication.
- S/MIME, if needed.
    - Used for secure email sender identification.

Depending on the security level demanded by the use case, an appropriate Certificate shall be selected.

1.4.2. Prohibited Certificate Uses

Any uses other than those described in Section 1.4.1 are prohibited. In particular, what Certificates are able to guarantee shall not be misrepresented, and any local laws and guidelines shall be followed.

1.5. Policy Administration

1.5.1. Organization Administering the Document

This CP/CPS is administered by the Trufo Policy Authority (TPA), the members of which are appointed by Trufo’s executive management.

1.5.2. Contact Person

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

1.5.3. Person Determining CPS Suitability for the Policy

The TPA determines the suitability of this CP/CPS.

1.5.4. CPS Approval Procedures

This CP/CPS is reviewed on an annual basis, and is further reviewed whenever it is recommended by the TPA.

1.6. Definitions and Acronyms

1.6.1. Definitions

Applicant: an entity applying for a Certificate.

Attestation Letter: a letter attesting Subject Information, written by a legal entity.

Certificate: an electronic document that uses a digital signature to bind a Public Key and an entity.

Hardware Cryptography Module: a processor configured for cryptography, and in particular for the secure implementation of cryptographic keys.

Key Pair: a Private Key and associated Public Key.

OCSP Responder: an online software application operated within Trufo's PKI for processing Certificate status requests.

Private Key: the key of a Key Pair that is kept secret by the holder, to create digital signatures.

Public Key: the key of a Key Pair that may be publicly disclosed by the holder, to be used by a Relying Party to verify digital signatures created with the Private Key of the Key Pair.

Relying Party: an entity that relies upon the information contained within a Trufo certificate or a Trufo timestamp token.

Subject Identity Information: information that identifies the subject of the Certificate.

Subscriber: an entity that holds a registered Certificate.

1.6.2. Acronyms

AISIC: U.S. Artificial Intelligence Safety Institute Consortium

C2PA: Coalition for Content Provenance and Authenticity

CA: Certification Authority

CAB: Certificate Authority/Browser (Forum)

CN: Common Name

CP: Certificate Policy

CPS: Certificate Practice Statement

CRL: Certificate Revocation List

CSC: Code-Signing Certificates

CSS: Certificate Status Services

DCAA: Defence Contract Audit Agency

DN: Distinguished Name

DV: Domain Validated

EE: End-Entity (Certificate)

ERA: Enterprise Registration Authority

EST: Enrollment over Secure Transport

EV: Extended Validation

ICA: Issuing Certification Authority

IETF: Internet Engineering Task Force

IPTC: International Press Telecommunications Council

NIST: National Institute of Standards and Technology
OCSP: Online Certificate Status Protocol
OV: Organization Validated
PKI: Public Key Infrastructure
PKI-PA: PKI Policy Authority (TPA)
RA: Registration Authority
RCA: Root Certification Authority
RFC: Request for Comments
RPS: Registration Practice Statement
SCVP: Server-Based Certification Validation Protocol
S/MIME: Secure/Multipurpose Internet Mail Extensions
TCA: Trufo Certification Authority
TLS: Transport Layer Security
TPA: Trufo Policy Authority
TSA: Timestamp Authority
TPKI: Trufo PKI
TS: Timestamping Authority

2. Publication and Repository Responsibilities

2.1. Repositories

Trufo maintains a central repository at https://trufo.ai to allow access to documents related to Trufo's policies and practices, including this CP/CPS and relevant CRLs. The central repository is maintained with resources sufficient to provide a commercially reasonable response time for access at all times.

2.2. Publication of Certification Information

The Trufo CP/CPS is available at https://trufo.ai/cpcps. The Trufo Terms of Service (ToS) and Privacy Policy (PP) documents can also be found on the main website.

Both Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) responses are available through online API endpoints maintained by Trufo. These endpoints provide Relying Parties with pertinent information regarding the status of a Trufo certificate.

Additional information not suitable for public dissemination, such as auditor report letters, can be requested by contacting the TPA at compliance@trufo.ai.

2.3. Time or Frequency of Publication

Certificate information is published promptly upon acceptance by the Subscriber or upon revocation of the Certificate. See Section 4.4.2 for more details.

The CRLs are updated daily. See Section 4.9.7 for more details.

The CP/CPS is updated annually, or whenever a significant change is made. See Section 1.5.4 for more details.

2.4. Access Controls on Repositories

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

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

3. Identification and Authentication

3.1. Naming

3.1.1. Types of Names

The subject of each certificate issued by Trufo is identified by a Distinguished Name (DN) in compliance with the ITU X.500 standards. The DN will consist of a single Common Name (CN) attribute with a value generated by Trufo.

3.1.2. Need for Names to Be Meaningful

Trufo uses DNs to identify an entity as introduced in Section 1.3, and therefore names submitted to Trufo during the certificate application process must be meaningful, unambiguous, and unique. The Subject name in each certificate should not be meaningful in the conventional, human-readable sense, but rather should follow commonly understood semantics that the RAs and CAs in the Trufo PKI follow.

3.1.3. Anonymity or Pseudonymity of Subscribers

Trufo supports anonymous Subject names for certain types of entities, wherein the individual entity may not be publicly identifiable but the entity type is. In particular, physical capture devices and content editing applications may be made anonymous, though the device model and application name, respectively, will be identifiable. The full list of applicable entity types follows internal and industry-specific security and conformance guidelines.

For all other types of entities, the Subscriber information will not be made anonymous.

3.1.4. Rules for Interpreting Various Name Forms

Trufo Certificates shall be issued with DNs interpreted using X.500 standards and ASN.1 syntax.

3.1.5. Uniqueness of Names

The full combination of the Subject Attributes shall be unique in Trufo’s PKI among active (non-revoked) Certificates. Depending on the type of Certificate and the entity type of the Subscriber, different

elements of the Certificate ensure uniqueness. RAs are further required to enforce name uniqueness in communities where they participate.

3.1.6. Recognition, Authentication, and Role of Trademarks

Applicants agree by submitting a Certificate Request to Trufo that their request does not contain content which in any way infringes on the intellectual property rights of another entity. Unless otherwise specifically stated in an agreement with a customer, DigiCert does not verify an Applicant’s right to use a trademark and does not resolve trademark disputes.

Trufo may reject any application or require revocation of any certificate that is part of a trademark dispute.

Applicants requesting Trufo Certificates shall be responsible for the legality of the information they present for verification and/or use in Certificates for any jurisdiction in which such content may be used or viewed.

Subscribers shall defend, indemnify, and hold Trufo harmless for any loss or damage resulting from any interference or infringement upon the rights of third parties.

3.2. Initial Identity Validation

Trufo may use any legal means of communication or investigation to ascertain the identity of an Applicant entity. Trufo may refuse to issue a Certificate in its sole discretion.

All Certificate Requests submitted by an Applicant shall establish possession of the Private Key related to the request and shall be verified at the level of assurance appropriate to the certificate requested. Trufo issues different types of Certificates (including Code Signing, EV Code Signing, and Document Signing) with different levels of security depending on the type of entity the Applicant belongs to.

Trufo shall inspect any document relied upon for verification for alteration and falsification. Any compromise in the security of the document or any misrepresentation of the Applicant identity shall constitute grounds for refusal of Certificate issuance.

3.2.1. Method to Prove Possession of Private Key

Any Applicant must submit a Certificate Signing Request that is signed by the Applicant’s Private Key per the PKCS #10 specification or an equivalent alternative.

This requirement does not apply when a Key Pair is generated by Trufo on behalf of a Subscriber.

3.2.2. Authentication of Organization Identity

Certificate Requests which include an organization identity shall be verified using the criteria described below.

Trufo may use external Reliable Data Sources (RDSs) in the process of this verification; a data source is considered a RDS based on an internal evaluation of the age, purpose, provider, accessibility, and security measures of the information in the database.

3.2.2.1. Verification of Identity

If the Subject Identity information includes the name, address, or DBA of an organization, Trufo shall verify the identity of the Applicant using documentation provided by at least one of the following:

- A government agency or Incorporating Agency or Registration Agency in the jurisdiction of the Applicant’s legal creation;
- A third-party database that is considered a Reliable Data Source;
- A site visit by Trufo or a third party who is acting as an agent for Trufo; or
- A formal Attestation Letter written by a legal representative of the Applicant.

Trufo may further verify the organizational unit of the Applicant if included in the Subject Identity via the same methods.

3.2.2.2. Verification of Country

If the Subject Identity information includes the country name, Trufo shall verify the associated country using one of the following:

- The country range of either the Applicant’s IP Address or the organization’s web site’s IP Address per DNS records.
- The ccTLD of the requested Domain Name.
- Any of the methods identified in Section 3.2.2.1.

Trufo may further verify the state and locality of the Applicant via the same methods.

3.2.3. Authentication of Individual Identity

Certificate Requests which include an individual identity shall be verified using the criteria described below.

3.2.3.1. Verification of Identity

If the Subject Identity information includes the name, address, or email of an individual, Trufo shall verify the identity of the Applicant using documentation provided by at least one of the following:

- A government-issued photo ID (passport, driver’s license, national ID, or equivalent document type).
- A secure email or video communication with the Applicant or a representative of the Applicant.
- A third-party identity service that is determined by Trufo to be secure.

When using a third-party identity service, not every Subject Identity field may be present, or if they are present, authenticated to a satisfactory degree. In these cases, Trufo shall inspect the identity service and separate the authenticated data and the non-authenticated data. This is very common when the Applicant presents a third-party digital account, such as Google ID or Apple ID. In these cases, the email address is fully authenticated, but the legal name and physical address are not.

3.2.3.2. Verification of Legal Affiliation

Trufo shall verify the identity of any affiliated legal entity via any of the methods identified in Section 3.2.2.1.

Trufo shall verify the individual affiliation using at least one of the following:

- A secure email or video communication with the Applicant or a representative of the Applicant.
- A third-party enterprise identity management service that is determined by Trufo to be secure.

3.2.4. Non-verified Subscriber Information

For most entity types, Trufo does not verify the Organization Unit, Locality, and State fields.

For most entity types, and in particular for the Code Signing and EV Code Signing certificates, domain names are not specified.
Trufo may issue Testing Certificates for which the standard identity validation procedures are waived. Trufo shall clearly indicate that these Certificates are for testing purposes.

3.2.5. Validation of Authority

Trufo shall verify the authorization of all Certificate Requests.

For Code Signing, EV Code Signing, and Document Signing Certificate Requests, the Applicant’s contact information is verified with an authoritative source within the Applicant’s organization using a Reliable Method of Communication.

3.2.6. Criteria for Interoperation

The Trufo PKI is not designed to interoperate with any other PKI operated by a third-party. However, the Trufo PKI is designed to be used by Relying Parties alongside other selected third-party PKIs that follow selected conformance guidelines for digital media signing, with C2PA and VIDA being nascent examples of such conformance guidelines.

3.2.7. Authentication of Identity for Other Entity Types

Trufo issues certificates to entities that do not fall under the typical domain name, organization, or individual classifications. For these entities, Trufo validates the entity type and, depending on the security level required, validates additional information.

Some important entity types include:

- Physical capture devices, such as cameras and phones. These require hardware-level security and authentication, and are the most demanding.
- Software applications, such as digital media editing programs. These require instance-level security and authentication, on the local device.
- Online SaaS products, which in addition to identity validation, must be audited and approved by Trufo as CAs and/or RAs to issue or participate in the issuance of Certificates.
- Individual accounts linked to third-party accounts, such as Google and Apple user accounts. These require third-party login verification.

Many of these CA services provided by Trufo fall outside the existing purview of Internet CA standards, due to the nascent nature of the digital media authenticity domain. Trufo is working with a selection of relevant governance working groups to determine suitable CP standards for such CA services.

3.3. Identification and Authentication for Re-key Requests

Subscribers may request re-keying of a Trufo Certificate prior to the Certificate's expiration. Subordinate CAs of Trufo may request re-keying of a Certificate registered by them prior to the Certificate's expiration. The re-keying process is detailed in Section 4.7.

3.3.1. Identification and Authentication for Routine Re-key

A Subscriber may request a re-key of any unexpired Trufo Certificate via the registration procedures described in Section 3.2 or by presenting proof of possession of the Private Key via a digital signature submitted over a Reliable Method of Communication. In the latter, Trufo will check for signs of any alteration or falsification of information.

Trufo operates an online API for Subscribers to request a re-key.

3.3.2. Identification and Authentication for Re-key after Revocation

A Subscriber requesting a re-key of a Trufo Certificate after said Certificate has been revoked will need to follow all authentication procedures for a new Trufo Certificate.

3.4. Identification and Authentication for Revocation Request

Trufo may revoke any Certificate issued within the Trufo PKI at its sole discretion. Trufo shall follow the procedures detailed in Section 4.9.3.

4. Certificate Life Cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

A Certificate application may be submitted by the Subscriber (individual or organization) or an authorized representative on the Subscriber’s behalf. This includes:

- The Subscriber: The individual or entity that is the subject of the certificate.
- Authorized Representatives: Individuals or agents authorized to act on behalf of the Subscriber, including agents of organizations or other entities.
- Registration Authorities (RAs): Designated RAs may submit certificate applications on behalf of the Subscriber.

The Subscriber is ultimately responsible for the accuracy of the information provided, whether submitted directly or through an authorized representative or RA.

4.1.2. Enrollment Process and Responsibilities

The enrollment process include the following steps, in no particular order:

- Certificate Application Submission: The Subscriber or an authorized representative submits a certificate application, including any required documentation from the associated program.
- Key Pair Generation: The Subscriber generates a key pair, either on their own device or through a designated service, depending on the requirements.
- Public Key Delivery: The public key from the Subscriber’s key pair is delivered to Trufo as part of the enrollment process.
- Subscriber Agreement: The Subscriber must review and agree to the applicable Subscriber Agreement before the issuance of the certificate.
- Payment of Fees: Any applicable fees associated with Certificate issuance must be paid as part of the process.

For Certificates issued as part of normal business practices, a separate application request may not be necessary. In such cases,

reference should be made to the specific documented practices governing Certificate issuance within the organization.

4.2. Certificate Application Processing

Information in certificate applications must be verified for accuracy before certificates are issued.

4.2.1. Performing Identification and Authentication Functions

Upon receiving a certificate application, the Trufo CA or an RA verifies the applicant's information to ensure its accuracy. Existing practices for identifying and authenticating organizations or individuals may be used as a basis for certificate issuance.

The RA is responsible for maintaining records of the verification process and communicating its completion to the Trufo CA. Both the Trufo CA and the RA evaluate the reliability of the sources used for verification before deciding whether to issue the certificate, in accordance with the relevant sections of this policy.

4.2.2. Approval or Rejection of Certificate Applications

The Trufo CA or an RA may approve a certificate application once the applicant's identity and authorization have been verified, in accordance with the relevant Certificate Policy (CP) and business practices. If the application meets all requirements, the certificate will be issued.

The Trufo CA reserves the right to reject any certificate application if the information cannot be validated or if issuing the certificate would negatively impact Trufo’s reputation, business, or violate legal agreements. Applications that do not meet the requirements outlined in the CP will also be rejected.

4.2.3. Time to Process Certificate Applications

The Trufo CA will typically process certificate applications and issue or reject the certificate within two working days after receiving all necessary details and documentation from the Subscriber, unless otherwise specified in the applicable customer agreement.

Unforeseen events outside of Trufo's control may cause delays in the process.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

Certificates are issued once the necessary requirements, including identity verification and validation of the Certificate request, have been fulfilled. These requirements include verifying the requester's identity, authority, and the integrity of the information in the request, as outlined in Sections 3.2 and 4.1.

Once all conditions are met, the Trufo CA generates the Certificate using the Certificate Request Data, adhering to the X.509 Certificate Profile. The Certificate attributes, such as validity periods and extension fields, are set according to the profile requirements. After issuance, the Certificate is stored in a database and sent to the Subscriber.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

The Trufo CA will notify the Subscriber when the Certificate has been issued, typically using Enrollment over Secure Transport (EST) to deliver the Certificate securely.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

Certificates are considered accepted 30 days after issuance, or earlier if evidence exists that the Subscriber has used the certificate. Subscribers are solely responsible for installing the issued certificate on their computer or hardware security module. The Trufo CA may publish the certificate and notify the Subscriber without requiring prior review and acceptance.

4.4.2. Publication of the Certificate by the CA

The Trufo CA will publish Certificates once issued. This publication will occur within typically 2 business days. The Certificates will be

delivered to the Subscriber and published through the methods described in Section 2.1.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

The Trufo CA may notify other relevant entities of the Certificate issuance as required by legal agreements or internal procedures. Any such notification will be made in a secure manner, based on the specific needs of the Subscriber and the associated business processes.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Subscribers are responsible for their Private Keys from unauthorized use or disclosure, and follow the revocation and expiration policies set forth in this CP/CPS. Subscribers are obligated to use Certificates in accordance with their intended purpose.

4.5.2. Relying Party Public Key and Certificate Usage

The primary Relying Parties in this PKI are organizations that use TPKI Certificates to verify TPKI-signed objects. Relying parties are referred to Section 4.5.2 of [RFC6484] for additional guidance with respect to acts of reliance on TPKI Certificates.

4.6. Certificate Renewal

4.6.1. Circumstance for Certificate Renewal

As per RFC 6484, a Certificate will be processed for renewal based on its expiration date or a renewal request from the Certificate Subject. The request may be implicit, a side effect of renewing a resource holding agreement, or explicit. If Trufo initiates the renewal process based on the Certificate expiration date, then Trufo will notify the subscriber 2 weeks in advance of the expiration date. The validity interval of the new (renewed) Certificate will overlap that of the previous Certificate by 1 week, to ensure uninterrupted coverage.

Certificate renewal will incorporate the same public key as the previous Certificate, unless the private key has been reported as compromised (see Section 4.9.1). If a new key pair is being used, the stipulations of Section 4.7 will apply.

4.6.2. Who May Request Renewal

Only the Certificate subject or an authorized representative of the Certificate subject may request the renewal of the Subscriber's Certificates. The Trufo CA may renew a certificate without a corresponding request if the signing Certificate is re-keyed. In the case of the Subscriber initiating the renewal process, procedures will be implemented to authenticate the identity of the Subscriber per Section 3. This will include verifying proof of possession (PoP) of the private key corresponding to the public key in the Certificate being renewed or the new public key if a key change is involved.

4.6.3. Processing Certificate Renewal Requests

The procedures for handling Certificate renewal requests will mirror those used during the original issuance of the Certificate, as specified in the applicable program CP. The Trufo CA may refuse to renew a Certificate if it cannot verify any rechecked information. If the individual renewing a client certificate provides information that has not changed, no additional identity vetting will be required. If both the private key and domain information remain unchanged, the Subscriber may renew a Certificate using the previously issued Certificate or a provided Certificate Signing Request (CSR). RAs must confirm the identity of the Subscriber according to the relevant CP requirements, which will be documented in the RA’s RPS.

4.6.4. Notification of New Certificate Issuance to Subscriber

The Trufo CA will notify the Subscriber when the renewed certificate has been issued, typically using Enrollment over Secure Transport (EST) to deliver the certificate securely.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1.

4.6.6. Publication of the Renewal Certificate by the CA

See Section 4.4.2.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.7. Certificate Re-key

4.7.1. Circumstance for Certificate Re-key

As per RFC 6484, re-key of a Certificate will be performed only when required, based on:

1. knowledge or suspicion of compromise or loss of the associated private key, or
2. the expiration of the cryptographic lifetime of the associated key pair.

If a Certificate is revoked to replace the RFC 3779 extensions, the replacement certificate will incorporate the same public key, not a new key.

If the re-key is based on a suspected compromise, then the previous Certificate will be revoked.

4.7.2. Who May Request Certification of a New Public Key

Only the holder of a certificate may request a re-key. The Trufo CA may also initiate a re-key based on a verified compromise report. If the Subscriber requests the re-key, authentication will be conducted using the appropriate methods. In cases where a compromise report is received from a source other than the Subscriber, the Trufo CA will verify the report through established procedures to ensure its validity.

4.7.3. Processing Certificate Re-keying Requests

The Trufo CA will handle re-keying requests in accordance with the process described in Section 4.3. Existing verification information

may be reused unless re-verification and authentication are mandated by contract or if the Trufo CA believes the information has become inaccurate. The Trufo CA or the RA will confirm the identity of the Subscriber based on the requirements specified in the relevant CP and contractual agreements for the authentication of the original certificate application. The RAs will document these practices in their respective RPS.

CA certificate re-key requests will be approved according to the guidelines and requirements specified in the associated contract and CP.

4.7.4. Notification of New Certificate Issuance to Subscriber

The Trufo CA will notify the Subscriber when the re-keyed certificate has been issued, typically using Enrollment over Secure Transport (EST) to deliver the certificate securely.

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

When a re-keyed certificate is issued, the CA will publish it in the repository and notify the subscriber. See Section 4.4.1.

4.7.6. Publication of the Re-keyed Certificate by the CA

The Trufo CA will publish the re-keyed certificates once issued. This publication will occur within typically 2 business days. The certificates will be delivered to the Subscriber and published through the methods described in Section 2.1. Simultaneously, the old certificates will be marked as revoked.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8. Certificate Modification

4.8.1. Circumstance for Certificate Modification

As per RFC 6484, modification of a certificate occurs to implement changes to the RFC 3779 extension values or the SIA extension in a

certificate. A subscriber can request a certificate modification when this information in a currently valid certificate has changed or as a result of change of the repository publication point data.

4.8.2. Who May Request Certificate Modification

The Subscriber or the Trufo CA may initiate the certificate modification process. To verify the identity and authorization of the entity requesting the modification, the Trufo CA will follow established procedures that include validating the requester's identity, ensuring that the request complies with the relevant CP, and confirming that the requester has the authority to make such modifications.

4.8.3. Processing Certificate Modification Requests

Upon receiving a request for modification, the Trufo CA or an RA will verify any changed information in accordance with Section 3.2 of this CP/CPS and the applicable CP or guidelines. The procedures for the issuance of a new certificate will be consistent with the processes described in Sections 4.2 and 4.3.1. RAs that handle Certificate modifications will detail their compliant practices in their respective RPS according to this CP/CPS and the specific CP for the certificate type and subject.

4.8.4. Notification of Modified Certificate Issuance to Subscriber

The Trufo CA will notify the Subscriber when the modified certificate has been issued, typically using Enrollment over Secure Transport (EST) to deliver the certificate securely.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

When a modified Certificate is issued, the Trufo CA will publish it to the repository and notify the subscriber. See Section 4.4.1.

4.8.6. Publication of the Modified Certificate by the CA

The Trufo CA will publish the modified Certificates once issued. This publication will occur within typically 2 business days. The

Certificates will be delivered to the Subscriber and published through the methods described in Section 2.1.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

A Certificate is revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. Circumstances that may lead to revocation include:

- Identifying information or affiliation components of any names in the certificate becoming invalid.
- Privilege attributes asserted in the Subscriber's certificate being reduced.
- The Subscriber violating the stipulations of its Subscriber agreement.
- Reason to believe that the private key has been compromised.
- The media or its location being intentionally falsified.
- The media being illegal within the jurisdiction of the Trufo CA.
- The media being affected by a copyright claim within the jurisdiction of the Trufo CA.
- The Subscriber or another authorized party requests the revocation of the certificate.

Whenever any of the above circumstances occur, the associated certificate will be revoked, and this information will be made available for Certificate Status Services (CSS). Revoked Certificates will be included in all new publications of the Certificate status information until they expire.

4.9.2. Who Can Request Revocation

The Subscriber or the Trufo CA may request revocation of a Certificate. The Trufo CA will verify the identity and authority of the entity requesting the revocation, ensuring that the request is legitimate and authorized.

4.9.3. Procedure for Revocation Request

The process for handling a certificate revocation request generally follows these steps:

1. The requesting entity must submit a revocation request identifying the certificate to be revoked and explaining the reason for the request.

2. The Trufo CA logs the identity of the entity making the request and the reason for the revocation.

3. If applicable, the Trufo CA may request confirmation of the revocation from the Subscriber or a known administrator via out-of-band communication (e.g., telephone, fax, etc.).

4. Upon authentication of the request, the Trufo CA will proceed to revoke the certificate.

5. If the request originates from a third party, the Trufo CA personnel will investigate the request, considering factors such as the nature of the alleged problem, the number of reports received, and the identity of the complainants.

6. If deemed appropriate, the Trufo CA will revoke the Certificate and update the Certificate Revocation List (CRL).

The Trufo CA maintains a continuous ability to respond to high-priority revocation requests.

4.9.4. Revocation Request Grace Period

A Subscriber is required to request revocation as soon as possible after the need for revocation has been identified.

4.9.5. Time within Which CA Must Process the Revocation Request

The Trufo CA will process a revocation request as quickly as practical, generally within 48 hours of receiving a validated request.

4.9.6. Revocation Checking Requirement for Relying Parties

As per RFC 6484, a relying party is responsible for acquiring and checking the most recent, scheduled CRL from the issuer of the certificate, whenever the relying party validates a certificate.

4.9.7. CRL Issuance Frequency

CRLs for end-entity certificates will be published at least every 24 hours. The Trufo CA may issue CRLs more frequently to ensure the timeliness of information.

4.9.8. Maximum Latency for CRLs

CRLs will be published to the repository system within a maximum latency of 30 minutes after generation.

4.10. Certificate Status Services

The Trufo CA does not support the Online Certificate Status Protocol (OCSP) or the Server-Based Certificate Validation Protocol (SCVP). The Trufo CA issues CRLs for certificate status verification.

5. Facility, Management, and Operational Controls

5.1. Physical Controls

5.1.1. Site Location and Construction

Trufo performs its CA and TSA operations from two types of secure data centers: servers operated by Trufo and servers operated by trusted third parties. Depending on the type of Certificate, the corresponding data will be stored in one or both types of servers as is appropriate for the level of security required.

The physical security practices of servers operated by trusted third parties shall be examined and approved by the TPA periodically.

5.1.2. Physical Access

All Trufo-operated data centers (TDCs) are located in physical areas that are protected against unauthorized access. Authorized individuals shall present identification before entering the premises. There is a 24-hour security presence as well as both physical security systems (e.g. door locks) and software security systems (e.g. password).

5.1.3. Power and Air Conditioning

TDCs shall have access to continuous power and air conditioning.

5.1.4. Water Exposures

No stipulation.

5.1.5. Fire Prevention and Protection

TDCs are equipped with fire sprinklers and fire extinguishers.

5.1.6. Media Storage

No stipulation.

5.1.7. Waste Disposal

No stipulation.

5.1.8. Off-Site Backup

Backup files are maintained across multiple physical servers.

5.2. Procedural Controls

5.2.1. Trusted Roles

Personnel acting in trusted roles include:

- CA and RA administrator personnel, who install and configure the CA and RA software.
- System engineers, who install and configure system hardware, including servers, routers, firewalls, and network settings.
- Internal auditors.

5.2.2. Number of Persons Required per Task

Trufo follows the two-person rule for most sensitive tasks.

5.2.3. Identification and Authentication for Each Role

All personnel are required to present identification and complete an authentication process before they are allowed to access TDC systems.

5.2.4. Roles Requiring Separation of Duties

No stipulation.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

The TPA is responsible for Trufo’s PKI operations and ensures compliance with this CP/CPS. Trufo shall verify the identity and other qualifications of any trusted personnel.

5.3.2. Background Check Procedures

For any trusted personnel, the TPA shall verify a government-issued photo identification document. The TPA shall further screen the individual’s qualifications, via a combination of:

- Employment history.
- Education history.
- Criminal history.
- Personal references.

5.3.3. Training Requirements

The TPA shall provide all trusted personnel with relevant training, on topics including:

- Basic PKI knowledge.
- Relevant CA or RA software.
- Relevant system software.
- Relevant security policies, in accordance with this CP/CPS and with CAB forum guidelines.
- Common security threats, such as phishing.

5.3.4. Retraining Frequency and Requirements

No stipulation.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

Trusted personnel who fail to comply with this CP/CPS will be subject to internal processes specifying guidance on administrative or disciplinary actions.

5.3.7. Independent Contractor Requirements

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this section 5.3.

5.3.8. Documentation Supplied to Personnel

No stipulation.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

Electronic records of the following events are kept:

- PKI key generation and registration.
- Certificate requests and the response result.
- Certificate issuance, renewal, and re-keying.
- Certificate revocation.
- System access attempts.

The date and time of these events are recorded. The responsible user or process is also recorded.

5.4.2. Frequency of Processing Log

The TPA will review the logs periodically, at least once per quarter. In these checks, the TPA will check for evidence of tampering with the log. and if necessary, will prepare a written summary of the review.

5.4.3. Retention Period for Audit Log

No stipulation.

5.4.4. Protection of Audit Log

No stipulation.

5.4.5. Audit Log Backup Procedures

No stipulation.

5.4.6. Audit Collection System (Internal vs. External)

No stipulation.

5.4.7. Notification to Event-Causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

To meet requirements of the CAB Forum baseline requirements, the TPA performs an annual risk assessment to assess foreseeable internal and external threats that could result in unauthorized access or misuse of any CA data.

5.5. Records Archival

No stipulation.

5.6. Key Changeover

Each Trufo CA Certificate will contain a validity period that is at least as long as that of any certificate being issued under that certificate.

As a Trufo CA Certificate is retired, a new CA signing key pair is commissioned and all newly signed Certificates will be signed with the new Trufo CA Certificate. The retirement date is well before the end of the validity period. More than one Trufo CA Certificate can be active at any given time, but only one will be used to sign issued Certificates.

5.7. Compromise and Disaster Recovery

Trufo makes regular system backups and maintains backup copies of its CA Private Keys. If Trufo suspects that one if its CA Private Keys has been compromised or lost, then an emergency response team will convene and assess the situation to determine the degree and scope of the incident and take the appropriate action. The appropriate entities, such as affected PKI participants and if needed, government agencies and law enforcement, will be notified. Trufo will then generate a new Key Pair and sign a new Certificate.

5.8. CA or RA Termination

No stipulation.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

All key pairs shall be generated using a FIPS-approved method or equivalent international standard.

All Trufo CA key pairs are generated following the two-person rule using a hardware cryptographic module that is evaluated to FIPS 140-2 level 2 or higher.

All Subscribers must generate their key pairs in a manner that is appropriate for the certificate type and for their entity types. In particular, any Certificates issued at a high hardware or biometric security level must be generated using a hardware cryptographic module via a FIPS-approved method.

6.1.2. Private Key Delivery to Subscriber

If Trufo or a participating RA generates a key pair for a Subscriber, then it must deliver the Private Key securely to the Subscriber. Keys may be delivered electronically (such as through secure email or a secure cloud-based storage system) or on a hardware cryptographic module. The Subscriber must acknowledge receipt of the Private Key.

If Trufo or a participating RA becomes aware that a Subscriber’s Private Key has been communicated to an unauthorized entity, then all certificates associated with said Private Key will be revoked.

6.1.3. Public Key Delivery to Certificate Issuer

If the Subscriber generates a key pair for use in the Trufo PKI, the Subscriber shall deliver the Public Key along with a digital signature signed with the Private Key to the issuing CA. The payload may be delivered electronically (such as through secure email or a secure cloud-based storage system) or on a hardware cryptographic module. The issuing CA must validate the digital signature.

6.1.4. CA Public Key Delivery to Relying Parties

Trufo’s CA Public Keys are provided in root stores and trust lists.

6.1.5. Key Sizes

All generated key pairs shall be generated to at least 128-bits of security. The generation method shall be one of:

- 256-bit Ed25519 key (128 bits of security) + SHA-512.
- 448-bit Ed448-Goldilocks key (224 bits of security) + SHAKE256.

RSA key pairs are not permitted. For symmetric encryption, AES-256 or higher is used.

6.1.6. Public Key Parameter Generation and Quality Checking

Trufo uses the widely-recommended Ed25519 and Ed448-Goldilocks ECC curves for key pair generation, and conforms to FIPS 186 requirements.

6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field)

Private Keys corresponding to Root CA Certificates are used for:

- Self-signed Certificates to represent the Root CA.
- Certificates for Subordinate CAs.
- Certificates for OCSP Response verification.
- Signatures in published CRLs.

Subscriber Certificates do not include any extended key usage.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

Hardware cryptographic modules used in EV and OV Code Singing are held to FIPS 140-2 Level 2 or higher.

For certain entity types, lower-security Certificates may be issued. Subscribers are held to:

- Free: None (FIPS 140-2 Level 1 for RA).
- Basic: FIPS 140-1 Level 1 (FIPS 140-2 Level 1 for RA).
- Trusted: FIPS 140-2 Level 2 for hardware; FIPS 140-1 Level 1 for software (FIPS 140-2 Level 2 for RA).

6.2.2. Private Key (n out of m) Multi-Person Control

Access to Trufo’s CA Private Keys follow the two-person rule, and are stored in a physically secure location.

6.2.3. Private Key Escrow

No stipulation.

6.2.4. Private Key Backup

Trufo’s CA Private Keys are held on multiple hardware cryptographic modules held to FIPS 140-2 Level 2 or higher. The backup process is subject to the two-person rule.

6.2.5. Private Key Archival

No stipulation.

6.2.6. Private Key Transfer into or from a Cryptographic Module

Any Private Keys that are transferred are first encrypted before leaving the hardware cryptographic module.

6.2.7. Private Key Storage on Cryptographic Module

Trufo’s CA Private Keys are stored in a hardware cryptographic module held to FIPS 140-2 Level 2 or higher.

6.2.8. Method of Activating Private Key

The Subscriber shall indicate the successful generation or receipt of a Private Key by sending a signed digital signature to a participating CA or RA. Subscribers are solely responsible for protecting their Private Keys in a manner commensurate with the certificate type.

6.2.9. Method of Deactivating Private Key

No stipulation.

6.2.10. Method of Destroying Private Key

Trufo personnel shall destroy CA and RA Private Keys when no longer needed, following the two-person rule. Subscribers shall destroy their Private Keys when the corresponding Certificate is revoked or expired or if the Private Key is no longer needed.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

No stipulation.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Trufo’s Certificates have a maximum validity period of 25 years, with a Private Key use period of 10 years, to minimize the disruption caused by key changeover.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

No stipulation.

6.4.2. Activation Data Protection

No stipulation.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. Computer Security Controls

Trufo’s CA servers and access points run on trustworthy systems that are configured to follow industry security practices.
RAs must ensure that systems maintaining RA software and data files are trustworthy and with adequate protection from unauthorized access. This can be demonstrated through compliance with audit criteria as specified in Section 5.4.1.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

Trufo has mechanisms in place to control and monitor the acquisition and development of its CA systems. Vendors for software and hardware are selected after market assessment is conducted. Some PKI software components are developed in-house, and the TPA will audit the software to ensure that the system design and development process follows security policies.

6.6.2. Security Management Controls

No stipulation.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. Network Security Controls

Trufo and related CA and RA functions are performed over trusted networks. All communications are encrypted and unauthorized access to the network is protected by authentication requirements and firewalls.

6.8. Time-Stamping

Trufo’s computers use NTP time synchronization to synchronize system clocks at least once per day.

7. Certificate and CRL Profiles

7.1. Certificate Profile

All Certificates are X.509 version 3 Certificates, and the algorithm used is the ECDSA algorithm using the Ed25519 curve and SHA-512 hash. In certain cases, the Ed448 curve and SHAKE256 hash may be used to obtain increased bits of security.

The Distinguished Name, Common Name, and other Subject Identity fields are validated following the requirements of Section 3.

7.2. CRL Profile

Trufo specifies the following reason codes from RFC5280 to indicate the reason for revocation of Certificates:

- (0) unspecified.
- (1) keyCompromise.
- (2) cACompromise.
- (3) affiliationChanged.
- (4) superseded.
- (5) cessationOfOperation.
- (7) privilegeWithdrawn.

Trufo will determine the most appropriate reason; this reason will be included in the CRL under the CRLReason field.

The CRL consists of:

- CRL Reason.
- Issuer Distinguished Name.
- Issuer Signature Algorithm.
- CRL Issue Timestamp.
- Revoked Certificates.
    - Distinguished Name.
    - CRL Reason.
    - Revocation Timestamp.
    - Subject Identity information.
- Issuer’s Digital Signature.

7.3. OCSP Profile

No Stipulation.

8. Compliance Audit and Other Assessments

The practices in this CP/CPS are designed to meet or exceed the requirements of generally accepted industry standards. In this first published version, the core practices are laid out. Since the content authentication space is nascent, with many conformance guidelines still being drafted, many details are yet to be fully fleshed out and standardized. Any missing or incomplete stipulations will be completed as practices and requirements are established.

8.1. Frequency and Circumstances of Assessment

Trufo receives an annual audit by an independent external auditor to assess Trufo’s compliance with this CP/CPS.

8.2. Self-Audits

On at least a quarterly basis, Trufo performs an internal audit on its CA practices.

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

Subscribers may be charged a fee for the issuance, management, and renewal of Certificates.

9.1.2. Certificate Access Fees

CAs must not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3. Revocation or Status Information Access Fees

CAs must not charge a fee as a condition of making CRLs available in a repository or otherwise available to Relying Parties.

9.1.4. Fees for Other Services (if Applicable)

No stipulation.

9.1.5. Refund Policy

Refund policies should be stipulated in the appropriate agreement (i.e., Digital Certificate Authorization Agreement (DCAA)).

9.2. Financial Responsibility

9.2.1. Insurance Coverage

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

9.2.2. Other Assets

CAs must have enough financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to Subscribers and Relying Parties.

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

The following Subscriber information must be kept confidential and private:

- CA application records Certificate Application records.
- Personal or non-public information about Subscribers.
- Transactional records (both full records and the Audit trail of transactions).
- Security measures controlling the operations of CA hardware and software.

9.3.2. Information Not within the Scope of Confidential Information

Certificates, Certificate revocation, and other status information, Trufo repositories, and information contained within them, must not be considered Confidential or Private Information.

9.3.3. Responsibility to Protect Confidential Information

Trufo PKI Participants receiving private information must secure it from Compromise and disclosure to third parties.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

No stipulation.

9.4.2. Information Treated as Private

CAs must protect all Subscribers' personally identifying information from unauthorized disclosure. Records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognized agents. The contents of the archives maintained by CAs operating under this CP must not be released except as required by law.

9.4.3. Information Not Deemed Private

Information included in the Certificates is deemed public information and is not afforded protections.

9.4.4. Responsibility to Protect Private Information

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

9.4.5. Notice and Consent to Use Private Information

The PKI-PA or Trufo CAs are not required to provide any notice or obtain the consent of the Subscriber to release private information.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

The PKI-PA or Trufo CAs must not disclose private information to any third party unless authorized by this CP, required by law, government rule or regulation, or order of a court of competent jurisdiction.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. Intellectual Property Rights (if Applicable)

CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue.

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate

Application and DN within any Certificate issued to such Certificate Applicant.

Private keys corresponding to Certificates of CAs and Subscribers are the property of the CAs and Subscribers that are the respective Subjects of these Certificates. Secret Shares of a CA's private key is the property of the CA, and the CA retains all Intellectual Property Rights in and to such Secret Shares.

Without limiting the generality of the foregoing, Trufo' Root public keys and Certificates containing them, including all CA and Subscriber public keys and Certificates containing them, are the property of Trufo. Trufo licenses software and hardware MFRs to reproduce such public key Certificates to place copies in Trufo compliant hardware devices or software.

9.6. Representations and Warranties

The PKI-PA must:

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

9.6.1. CA Representations and Warranties

CAs operating under this CP must warrant that:

- The CA procedures are implemented in accordance with this CP
- The CA will provide its CPS to the PKI-PA, as well as any subsequent changes, for conformance assessment.
- The CA operations are maintained in conformance to the stipulations of the approved CPS Any Certificate issued is in accordance with the stipulations of this CP.

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate.
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application because of a failure to exercise reasonable care in managing the Certificate Application.
- Its Certificates meet all material requirements of this CP and the applicable CPS The revocation of Certificates is in accordance with the stipulations in this CP.
- Revocation services (when applicable) and use of a repository conform to all material requirements of this CP and the applicable CPS in all material aspects.

9.6.2. RA Representations and Warranties

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

9.6.3. Subscriber Representations and Warranties

Subscribers must sign an agreement containing the requirements the Subscriber must meet, including protection of their private keys and use of the Certificates before being issued the Certificates. In addition, Subscribers must warrant that:

- The Subscriber must abide by all the terms, conditions, and restrictions levied on the use of their private keys and Certificates.
- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created.
- Subscriber’s private keys are protected from unauthorized use or disclosure.
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true.
- All information supplied by the Subscriber and contained in the Certificate is true.

- The Certificate is being used exclusively for authorized and legal purposes, consistent with all material requirements of this CP.
- The Subscriber will promptly notify the appropriate CA upon suspicion of loss or Compromise of their private key(s).
- The Subscriber is an end-user Subscriber and not a CA and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

DCAAs may include additional representations and warranties.

9.6.4. Relying Party Representations and Warranties

This CP does not specify the steps a Relying Party should take to determine whether to rely upon a Certificate. The Relying Party decides, pursuant to its own policies, what steps to take. The CA merely provides the tools (i.e., Certificates and CRLs) needed to perform the trust path creation, validation, and CP mappings that the Relying Party may wish to employ in its determination. Relying Parties acknowledge that they have enough information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they must bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CP.

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. Disclaimers of Warranties

To the extent permitted by applicable law, DCAAs must disclaim Trufo’ and the applicable Subscriber’s possible warranties, including any warranty of merchantability or fitness for a particular purpose.

9.8. Limitations of Liability

The liability (and/or limitation thereof) of Subscribers must be as set forth in the applicable DCAAs.

9.9. Indemnities

To the extent permitted by applicable law, Subscribers are required to indemnify CAs for:

- Falsehood or misrepresentation of fact by the Subscriber on the Certificate Application.
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party The Subscriber’s failure to take the precautions necessary to prevent the Compromise, loss, disclosure, modification, or unauthorized use of the Subscriber’s private key(s) or a digital certificate. In the event of the imbedding of a digital certificate in a device not manufactured to the appropriate Trufo specification Subscriber is to pay to Trufo the gross revenue from the sale/use of such unauthorized devices.
- The Subscriber’s use of a name, including that which infringes upon the Intellectual Property Rights of a third party.

9.10. Term and Termination

9.10.1. Term

This CP becomes effective when approved by the PKI-PA. Amendments to this CP become effective upon publication. This CP has no specified term.

9.10.2. Termination

This CP, as amended from time to time, must remain in force until it is replaced by a new version. Termination of this CP is at the discretion of the PKI-PA.

9.10.3. Effect of Termination and Survival

Upon termination of this CP, Trufo PKI Participants are nevertheless bound by its terms for all Certificates issued for the remainder of the Validity Periods of such Certificates.

9.11. Individual Notices and Communications with Participants

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

9.12. Amendments

9.12.1. Procedure for Amendment

The PKI-PA must review this CP at least once every year. Corrections, updates, or changes to this CP must be made publicly available. Suggested changes to this CP must be communicated to the PKI-PA; such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.2. Notification Mechanism and Period

The PKI-PA reserves the right to amend this CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to web links, and changes to contact information. The PKI-PA’s decision to designate amendments as material or non-material must be within the PKI-PA’s sole discretion.

Change notices to this CP must be distributed electronically to Trufo PKI Participants and observers in accordance with the PKI-PA document change procedures.

9.12.3. Circumstances Under Which OID Must be Changed

If the PKI-PA determines that a change is necessary in the OID corresponding to a certificate policy, the amendment must contain new object identifiers for the certificate policies corresponding to each class of Certificate. Otherwise, amendments must not require a change in certificate policy object identifier.

9.13. Dispute Resolution Provisions

The PKI-PA must facilitate the resolution between entities when conflicts arise because of the use of Certificates issued under this CP.

9.14. Governing Law

Subject to any limitation appearing in applicable law, the laws of the State of New York, should govern the enforceability, construction, interpretation, and validity of this CP. This choice of law is made to ensure uniform procedures and interpretation for all Trufo PKI Participants, no matter where they are located.

9.15. Compliance with Applicable Law

This CP is subject to applicable national, state, local, and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. All CAs operating under this CP must comply with applicable law.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

No stipulation.

9.16.2. Assignment

No stipulation.

9.16.3. Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP must remain in effect until this CP is updated.

If a clause or provision of this CP is held to be unenforceable by a court of law or other tribunal having authority, the remainder of this CP must remain valid.

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5. Force Majeure

To the extent permitted by applicable law, Trufo PKI agreements (e.g., DCAAs) must include a force majeure clause protecting Trufo and the applicable Subscriber.

9.17. Other Provisions

No stipulation.