TrustCor CA Certification Practice Statement

Version 1.10.0

TrustCor Policy Authority

2022-11-07

Contents

1 Introduction

The Certification Authority ("CA") component of TrustCor Systems S. de R.L. ("TrustCor CA") is that section of the company which deals with the requesting, validation, issuance and revocation of digital certificates following the X.509 standard for specified business purposes to the general public.

This document is the TrustCor Systems S. de R.L. ("TrustCor CA") Certification Practice Statement ("CPS") which details the policies, principles and practices adhered by the Certification Authority ("CA") for its business operations involving the issuance and management of TrustCor CA's certificate services.

1.1 Overview

This CPS describes the practices which TrustCor CA must follow to comply with the current versions of the following policies, guidelines, and requirements:

- the Certificate Authority/Browser Forum ("CA/B Forum") Baseline Requirements for the Issuance and Management of Publicly–Trusted Certificates ("Baseline Requirements") - This version of the CPS, conforms to the current Version 1.8.4 of the Baseline Requirements published April 23, 2022
- the CA/B Forum Network and Certificate Systems Security Requirements, Version 1.7
- the CA/B Forum Baseline Requirements for Code-Signing Certificates, Version 2.8
- the WebTrust Principles and Criteria for Certification Authorities, Version 2.2.2, issued by Chartered Professional Accountants of Canada ("CPA Canada") on 1 June 2021
- the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, Version 2.6, issued by Chartered Professional Accountants of Canada ("CPA Canada") on 31 January 2022
- the WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements – Version 2.7, issued by the Chartered Professional Accountants of Canada ("CPA Canada") on 31 January 2022

This CPS is one of a set of documents which establish the governance and practices of the TrustCor CA business offerings. Other documents include, but are not limited to:

- The TrustCor CA Certificate Policy (CP)
- The TrustCor CA Privacy Policy
- The TrustCor CA Information Security Policy (+)
- The TrustCor Master Subscriber Agreement
- The TrustCor Terms of Use

- The TrustCor Relying Party Agreement
- Enterprise Subordinate CA Business Agreement(s) (+)

Note that not all documents are in the public domain - those marked with (+) are held to be company confidential, and are not disclosed generally.

Those documents which are publicly available can be reached online at

`https://www.trustcor.ca/resources`

If any inconsistency exists between this CPS and the policies, guidelines, and requirements given above, then those publications take precedence over this document.

1.2 Document Name and Identification

This document is version 1.10.0 of the TrustCor CA Certification Practice Statement, created and published on 2022-11-07. It carries the OID of `1.3.6.1.4.1.44031.1.1.17`.

1.3.6.1.4.1.44031 is the root branch of the enterprise OID space allocated to TrustCor Systems S. de R.L. via

`https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers`

1.2.1 Revisions

Date	Changes	Version
2022-11-07	Updates to sections 1.5.4, 1.6.1, 2.3, 3.2.2.4, 4.9.7 and 4.9.8	1.10.0
2022-06-29	Updates to sections 4.9.1.1.1, 5.4.1, 5.4.3, 5.5.2 as per SC 51 and root store updates	1.9.0
2022-02-08	Updates to sections 4.9.7, 5, 7.2, 7.3 and 8.7	1.8.1
2021-09-22	Updated sections 1.1, 1.5.2, 4.9.3, 6.3.2 and 8.4. Updated sections 1.6.1 and 7.1.4.2.1 as per SC 48. Reorganized section 7.1.	1.8.0
2021-07-07	Fixes for typos, statement on TLS over ALPN, license	1.7.2
2021-05-28	Updates to public suffix checking statements,OID fix, revoke	1.7.1

Date	Changes	Version
2020-10-20	Updates to domain control validation methods and wildcards	1.7.0
2020-03-27	Update with TSA/Code Signing and 2020 CAs	1.6.0
2019-10-21	Clarification of text and rearrangement of information	1.5.1
2019-04-19	Major review of all sections	1.5.0
2018-10-23	Update to revocation practices	1.4.2
2018-08-16	OCSP response lifetime changes	1.4.1
2018-02-16	Update to 3.2.2.4, CT publication policy and SHA-256 signatures	1.4.0
2017-08-15	Update to OCSP Response Policy	1.3.3
2017-08-14	Clarifications added in response to Mozilla Public Discussion	1.3.2
2017-04-19	Changes to policies to meet with BR 1.4.4	1.3.1
2016-09-15	Changes to policies to meet with BRs 1.4.0	1.3.0
2016-07-04	Review of document - no changes made	1.2.2
2016-01-23	Change to typo in policyId root (1.3.6.1.4.4 -> 1.3.6.1.4.1)	1.2.2
2015-12-10	Change to Subordinate CA names, replacing obsolete ones	1.2.1
2015-11-16	This version replaces 1.1.0 and converts into RFC 3647 format	1.2.0

1.3 PKI Participants

1.3.1 Certification Authorities

TrustCor CA operates three root certificates in its CA infrastructure:

- The Basic Root Certificate (CA-1) - used to ultimately be the root of trust for all certificates issued under the Basic Assurance program.
- The Enhanced Root Certificate (CA-2) - used as the root of trust for certificates issued under the Enhanced Assurance program.
- The Enterprise Root Certificate (ECA-1) - used as the ultimate root for enterprise PKIs issuing credentials to their principals in restricted namespaces.

TrustCor CA undertakes to ensure that all operations conducted using these certificates, including registration of entities, validation of same, issuance and revocation of certificates are

performed in accordance with the strictures of this document, the governing CP. Note that any Enterprise Subordinate CA certificates are still TrustCor CA certificates, and TrustCor CA is responsible for their issuance, insofar as the enterprise Subscriber Agreements is obeyed. TrustCor CA is responsible for revoking an enterprise subordinate CA should it discover substantive violations of its enterprise agreements.

TrustCor CA declares that it has not entered into any trust relationship with any other party which results in the establishment of a Cross Certificate identifying TrustCor CA as its Subject.

1.3.2 Registration Authorities

Registration authorities (RAs) are those parts of the PKI which deal with the collection of Subscriber information, validation of same and approve or reject the issuance process of certificates.

TrustCor CA has an internal RA which is used to collect Subscriber information, and react to requests for revocation and/or certificate pickup. It is managed in the same infrastructure as its CA offerings, detailed herein.

External RAs are present where external Enterprise CAs have been licensed to issue name restricted TrustCor CA certificates; such RAs must adhere to the terms of registration, validation and publication as noted in this document as well as the Enterprise Subscriber Agreement between TrustCor CA and the subscribing organization.

External RAs are not entitled to perform general domain or organizational validation; they are strictly limited to registration for credentials to domains and principals assigned to their specific organization.

1.3.3 Subscribers

Subscribers are those parties who apply for certificates or certification services from TrustCor CA and agree to be bound by the relevant Subscriber Agreement for the business offering selected. In this document, a Subscriber who has registered, but not yet received, a certificate is referred to as an Applicant.

1.3.4 Relying Parties

Relying Parties (RPs) are those who elect to use the information contained within a TrustCor CA certificate to identify an entity using SSL/TLS or S/MIME cryptographic protocols, and to cryptographically protect information using the public keys inside those certificates.

In order to have any confidence that the identification is a valid one, RPs must use either the CRLs or OCSP responses issued by TrustCor CA to have confidence that the certificates issued are still valid.

RPs should also refer to the subsections in Section 1.4 of this document to see whether TrustCor CA permits or prohibits the identification within a particular context (for example, whether certificates can be for identification/protection in high hazard environments).

1.3.5 Other Participants

The browser Root Program maintainers, while not playing a part in the issuance processes of TrustCor CA, may be party to an expedited revocation process, described in Section 4.9.

For the TSA facility, Time Stamp Token (TST) Requesters and Time Stamp Verifiers are participants.

1.4 Certificate Usage

All certificates issued by TrustCor CA have a set of identifiers embedded into them which limit the permissible types of use for the certificate (and its corresponding private key).

All certificates are issued under the aegis of a Subscriber Agreement which stipulates the permitted uses for the certificate. They are as follows:

- Basic and Enhanced Secure Email - to be used for protection of email contents and signing of emails.
- Basic and Enhanced Secure Site - to be used for termination of SSL/TLS connections to a particular IP service (for example, HTTPS, IMAP, LDAP, etc.)
- External PKI Subordinate CA - to be used to sign technically constrained S/MIME and SSL certificates (an agreement and certificate constraint may exist which limits publication to only one of those options). In all cases, the names expressible via the signed certificate will be embedded into the subordinate CA certificate.

Subscribers are constrained by their agreements not to use certificates outside of those specified purposes.

1.4.1 Appropriate Certificate Uses

The uses permitted for each certificate vary by the business offering. Because TrustCor CA has different pricing for its offerings dependent on certificate type, prospective Subscribers must

evaluate which type of certificate is most likely to fit their needs dependent on the type of information they wish certified and the evidence of identity which they are willing to submit to TrustCor CA.

TrustCor CA will embed OIDs in its end-entity certificates which denote the type of validation which was used in the issuance process.

Domain Validated (DV) Certificates are those used to terminate SSL connections either as clients or servers using the TLS protocols. The validation establishes that the private key holder has the ability to control the domain or end points which the certificate will hold. DV certificates can only certify a single end point. They are intended to be used where the risk of damage to the private key holder, in the event of compromise, is relatively low.

Organization Validated (OV) Certificates can be used for either S/MIME or SSL certificates. They are issued after a greater degree of investigation into the rights of the private key holder to claim both the organizational identity in the certificate, as well as the individual identities claimed within. They should be used where asserting an organizational identity is needed, and where the data protected using the private key/certificate pair contains moderate risk in the event of compromise. OV Certificates for SSL use may have multiple host names contained within their certificates; OV S/MIME certificates may not.

Time Stamp Tokens (TSTs) are used to establish that a given block of data existed at a set point in time.

1.4.2 Prohibited Certificate Uses

As per the CP, no TrustCor CA certificate may be used:

- in violation of local law where it is deployed
- for any purpose other than the permitted usages embedded in the certificate
- to act as testimony for an end-entity's identity which has not been established via the certificate issuance process.
- in violation of the Subscriber Agreement under which it was issued
- in any environment where fail-safe operation is required, or where it forms part of the control equipment involving hazardous materials. Such environments include, but are not limited to:
  - air traffic control systems
  - nuclear reactor facilities
  - weapons control systems

- aircraft navigation systems
- any system whose failure places human life in danger of injury or death

1.5 Policy Administration

1.5.1 Organization Administering the Document

This document is maintained via the TrustCor Policy Authority (TCPA), which also administers the CP, and the other TrustCor CA governing documents. The TCPA can be contacted at this address:

```
TrustCor Policy Authority,
371 Front Street West #227,
Toronto ON M5V3S8
Canada
```

The TCPA can be emailed at: legal@trustcor.ca

1.5.2 Contact Person

The following person can be used as a contact point for policy related enquiries:

```
Name: Rachel McPherson
Email: rachel@trustcor.ca
Tel: +1 (289) 408-9998
```

TrustCor CA provides an online form for reporting certificates that are believed to be used for malicious or harmful purposes. This includes reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other problematic matter related to Certificates. This form can be found at `https://trustcor.com/report-abuse`.

1.5.3 Person Determining CPS Suitability for the Policy

The TCPA determines whether this CPS adheres to the policy requirements set down in the CP.

1.5.4 CPS Approval Procedures

The TCPA may enact amendments to the CP and/or CPS as required, and update both the CP and CPS versioning accordingly. All changes made to the CP or CPS shall be noted in the Revisions section of the associated document.

The TCPA determines whether an amendment to the CP or CPS requires an OID change. On an annual basis, if no other changes are made to this document, its version number shall be incremented along with a dated entry in the Revisions section to denote that.

1.6 Definitions and Acronyms

1.6.1 Definitions

Affiliate A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate is issued, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

Applicant Representative A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA.

Application Software Supplier A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates; or A supplier of software or other relying-party application software that displays or uses Code Signing Certificates, incorporates Root Certificates, and adopts these Requirements as all or part of its requirements for participation in a root store program.

Attestation Letter A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

Audit Report A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.

Authorization Domain Name The FQDN used to obtain authorization for a given FQDN to be included in a Certificate. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If a Wildcard Domain Name is to be included in a Certificate, then the CA MUST remove "`*.`" from the left-most portion of the Wildcard Domain Name to yield the corresponding FQDN. The CA may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and may use any one of the values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.

Base Domain Name The portion of an applied-for FQDN that is the first Domain Name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

CAA From RFC 6844 (http://tools.ietf.org/html/rfc6844)

> "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue."

CA Key Pair A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

Certificate An electronic document that uses a digital signature to bind a public key and an identity.

Certificate Data Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Problem Report Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Profile A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7, e.g. a Section in a CA's CPS or a certificate template file used by CA software.

Certificate Requester A natural person who is the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or the employee or agent of a third party (such as software publisher) who completes and submits a Certificate Request on behalf of the Applicant.

Certificate Revocation List A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs.

Certification Practice Statement One of several documents forming the governance framework in which Certificates are created, issued, managed, and used. This document.

Code Signature A Signature logically associated with a signed Object.

Code Signing Certificate A digital certificate issued by a CA that contains a code Signing EKU, contains the anyExtendedKeyUsage EKU, or omits the EKU extension and is trusted in an Application Software Provider's root store to sign software objects. [NOTE: Appendix B, subsection (3) of Appendix B requires the presence of the codeSigning EKU and prohibits use of the anyExtendedKeyUsage EKU.]

Control "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: 1) direct the management, personnel, finances, or plans of such entity; 2) control the election of a majority of the directors; or 3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country Either a member of the United Nations OR a geographic region recognized as a sovereign nation by at least two UN member nations.

Cross Certificate A certificate that is used to establish a trust relationship between two Root CAs.

CSPRNG A random number generator intended for use in a cryptographic system.

Delegated Third Party A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Domain Authorization Document Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

Domain Name An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.

Domain Namespace The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar A person or entity that registers Domain Names under the auspices of or by agreement with: i. the Internet Corporation for Assigned Names and Numbers (ICANN), ii. a national Domain Name authority/registry, or iii. a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Domain Label From RFC 8499 (http://tools.ietf.org/html/rfc8499)

> "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names."

Effective Date These Requirements come into force on the date of approval of this document.

Enterprise RA An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

Expiry Date The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

Fully-Qualified Domain Name A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.

Government Entity A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

High Risk Certificate Request A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

High Risk Region of Concern (HRRC) As set forth in Appendix D of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, a geographic location where the detected number of Code Signing Certificates associated with signed Suspect Code exceeds 5% of the total number of detected Code Signing Certificates originating or associated with the same geographic area.

Internal Name A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

IP Address A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.

Issuing CA In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Key Compromise A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see `http://wiki.debian.org/SSLkeys`) or if there is clear evidence that the specific method used to generate the Private Key was flawed.

Key Generation Script A documented plan of procedures for the generation of a CA Key Pair.

Key Pair The Private Key and its associated Public Key.

LDH Label From RFC 5890 (http://tools.ietf.org/html/rfc5890)

> "A string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string. Like all DNS labels, its total length must not exceed 63 octets."

Legal Entity An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Non-Reserved LDH Label From RFC 5890 (http://tools.ietf.org/html/rfc5890)

> "The set of valid LDH labels that do not have '--' in the third and fourth positions."

Object Identifier A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Parent Company A company that Controls a Subsidiary Company.

P-Label A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3492, Section 6.3) from the fifth and subsequent positions.

Platform The computing environment in which an Application Software Supplier uses Code Signing Certificates, incorporates Root Certificates, and adopts these Requirements.

Private Key The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created

with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly-Trusted Certificate A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor A natural person or Legal Entity that meets the requirements of Section 8.2 (Identity/Qualifications of Assessor).

Registered Domain Name A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA) Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Reliable Data Source An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Repository An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Requirements The CA/B Forum's Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

Reserved IP Address An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries: https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml , https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

Root CA The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate The self-signed Certificate issued by the Root CA to identify itself and to facilitate

verification of Certificates issued to its Subordinate CAs.

Signing Service An organization that signs an Object on behalf of a Subscriber using a Private Key associated with a Code Signing Certificate.

Sovereign State A state or country that administers its own government, and is not dependent upon, or subject to, another power.

Subject The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber or Terms of Use Agreement.

Subscriber Agreement An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Subsidiary Company A company that is controlled by a Parent Company.

Technically Constrained Subordinate CA Certificate A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Terms of Use Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA.

Timestamp Authority A service operated by the CA or a delegated third party for its own code signing certificate users that timestamps data using a certificate chained to a public root, thereby asserting that the data (or the data from which the data were derived via a secure hashing algorithm) existed at the specified time. If the Timestamp Authority is delegated to a third party, the CA is responsible that the delegated third party complies with these guidelines.

Timestamp Certificate A certificate issued to a Timestamp Authority to use to timestamp data.

Trustworthy System Computer hardware, software, and procedures that are: * reasonably secure from intrusion and misuse; * provide a reasonable level of availability, reliability, and correct operation; * are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Unregistered Domain Name A Domain Name that is not a Registered Domain Name.

Valid Certificate A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialist Someone who performs the information verification duties specified by these Requirements.

Validity Period From RFC 5280 (http://tools.ietf.org/html/rfc5280)

> "The period of time from notBefore through notAfter, inclusive."

Wildcard Certificate A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.

Wildcard Domain Name A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.

XN-Label From RFC 5890 (http://tools.ietf.org/html/rfc5890)

> "The class of labels that begin with the prefix"xn–" (case independent), but otherwise conform to the rules for LDH labels."

1.6.2 Acronyms

AICPA American Institute of Certified Public Accountants
CA Certification Authority
CAA Certification Authority Authorization
ccTLD Country Code Top-Level Domain
CICA Canadian Institute of Chartered Accountants
CP Certificate Policy
CPA Chartered Professional Accountants (Canada)
CPS Certification Practice Statement
CRL Certificate Revocation List
DBA Doing Business As
DN Distinguished Name
DNS Domain Name System
EU The European Union
FIPS (US Government) Federal Information Processing Standard
FQDN Fully-Qualified Domain Name
IM Instant Messaging
IANA Internet Assigned Numbers Authority
ICANN Internet Corporation for Assigned Names and Numbers
ISO International Organization for Standardization
NIST (US Government) National Institute of Standards and Technology
OCSP Online Certificate Status Protocol
OID Object Identifier

PII Personal Identifying Information
PKI Public Key Infrastructure
RA Registration Authority
RP Relying Party
S/MIME Secure MIME (Multipurpose Internet Mail Extensions)
SSL Secure Sockets Layer
TC-OID TrustCor CA OID branch: 1.3.6.1.4.1.44031
TCPA TrustCor Policy Authority
TLD Top-Level Domain
TLS Transport Layer Security
VOIP Voice Over Internet Protocol
WebTrust for CAs Trust Service Principles and Criteria for Certification Authorities, Version 2.0

2 Publication and Repository Responsibilities

2.1 Repositories

The public documents establishing the practices for TrustCor CA's services can be found online at `https://www.trustcor.ca/resources`

All certificates which are used to sign TrustCor CA's end-entity certificates can be located at specific paths under `http://certs.trustcor.ca/`

Note that end-entity certificates are **not** published into a publicly facing repository, with the exception of site certificates which are published into CT logs as mentioned elsewhere in this document.

Any CRLs issued are found under `http://crl.trustcor.ca/`

OCSP responders are located under `http://ocsp.trustcor.ca/`

These repositories are replicated across multiple geographical sites in order to preserve a 24x7 service availability, with no more than 1% downtime caused by failures, and no more than 0.5% of downtime caused by planned maintenance.

2.2 Publication of Information

In addition to the above web locations into which TrustCor CA publishes its certification information, email to `legal@trustcor.ca` requests for information will yield the same documentation.

TrustCor CA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at `https://www.cabforum.org`. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

TrustCor CA conforms to the current version of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at `https://aka.ms/csbr`. If there is any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

Test web pages for valid, revoked and expired certificates for each root:

Root CA	State	URI
RootCert CA-1	valid	https://catest1.trustcor.ca/
RootCert CA-1	revoked	https://catest1-revoke.trustcor.ca/
RootCert CA-1	expired	https://catest1-expire.trustcor.ca/
RootCert CA-2	valid	https://catest2.trustcor.ca/
RootCert CA-2	revoked	https://catest2-revoke.trustcor.ca/
RootCert CA-2	expired	https://catest2-expire.trustcor.ca/
ECA1-External	valid	https://valid.epki.external.trustcor.ca/
ECA1-External	revoked	https://revoked.epki.external.trustcor.ca/
ECA1-External	expired	https://expired.epki.external.trustcor.ca/

2.2.1 Notification of Incorrect Issuance

If and when TrustCor CA becomes aware of the issuance of any certificate which has breached the stipulations of the Baseline Requirements, or which has been issued contrary to the stipulations of this document, the following steps will be taken in regards to making the incorrect issuance known, with seven (7) days of the problem issuance being known to TrustCor CA:

- a description of the incident, listing the certificate identifiers involved, a root cause analysis of the incorrect issuance, and the remediation steps taken to address the requirements breach, shall be published under the URI

  `https://www.trustcor.ca/resources/issuance-incidents/`

with a name which is the ISO-8601-Z (with colons replaced by hyphens) timestamp with a `.txt` suffix (e.g. `2016-05-01T18-12-07Z.txt`). To the end of this report, the PEM formatted X.509 certificates shall be appended by way of an appendix.

A browser based directory listing of this `issuance-incidents` directory shall show all reports generated by TrustCor CA over a seven year period.

TrustCor CA's auditor shall have this information brought to his/her attention at the earliest possible date post-incident.

2.3 Time or Frequency of Publication

Any published certificates (ie, CA certificates) are published to the above listed repositories, as soon as possible.

CPS and CP documents are published no more than seven days after the TCPA approves their contents. New CPS and CP documents are produced as and when the Baseline Requirements (BR) change such that new text is required, or when changes in TrustCor CA's business practices require such modification. The CP and CPS documents are reviewed at least once per year.

The frequency of CRL and OCSP issuance is covered in section 4.9.7 of this document.

2.4 Access Controls on Repositories

All repositories have public read accessibility. File permissions and system security policies are in place to ensure that any alteration to the repository contents comes from authorized principals and trusted sources within TrustCor CA.

Updates to the documents are stored in a version control system to which TrustCor CA personnel alone have access; all changes are recorded with both the nature of the alteration as well as the author of the change. Document change logs are reviewed periodically as per the section on log review.

3 Identification and Authentication

3.1 Naming

TrustCor CA end-user certificates in the Basic Email or Basic Site categories may not have a subject DN in them, preferring a critical subjectAltName extension (RFC822Name in the case of Basic Email certificates; dNSName in the case of Basic Site certificates). If the certificate does

have a subject DN, it is constrained to be identical in content to the subjectAltName extension (which will not be marked critical) described before.

Enhanced grade certificates, as well as External PKI issued certificates will always have an identifying Subject DN, as well as any relevant subjectAltNames.

3.1.1 Types of Names

All subject (and issuer) DNs inside TrustCor CA certificates have ITU X.501 format names, with the components having the standard semantics.

Name components (whether DNs or subjectAltNames) may not be IPv4 or IPv6 addresses.

Names are canonicalized with respect to whitespace upon registration. For example "Example Org" will become "Example Org". Thus names which differ only in terms of whitespace are not treated as being distinct.

TrustCor CA does not currently issue EU Qualified Certificates.

3.1.2 Need for Names to be Meaningful

Any Fully-Qualified Domain Name (FQDN) which is embedded into a certificate either as a DN component, or as a dNSName subjectAltName must conform to the standard semantics for DNS names described in RFC 1034. All DNS names must be validly formed and have a recognized public ICANN recognized suffix as found via

`https://publicsuffix.org`

Special mention is made to note that the underscore (_) character may not form any part of a dNSName.

Organizational names must be validated to be syntactically identical to an entry in such public registries of organizations as was used to validate the certificate request. The only alteration permissible is where a commonly used contraction for the status of the company is substituted. For example, a British company with a "Limited" status in the Companies House registry may have the text "Ltd." instead of the word "Limited" in the certificate name. The actual text of the organization may not deviate from that recorded in the public registry.

TrustCor CA does not populate organizational unit components in either DNs or subjectAltNames (for end-entity certificates), since no agreed semantic exists for their interpretation. Subordinate CAs issued to name restricted enterprises may populate OUs to represent their internal business functions, but no Secure Email or Secure Site certificates may do so.

Country DN components must be represented as ISO-3166-1 2 letter codes, in upper case.

3.1.3 Anonymity or Pseudonymity of Subscribers

Basic S/MIME certificates may possess pseudonymous email addresses, since other personal identity information is not sought in their issuance.

Basic SSL certificates do not identify a person, thus pseudonymity is not applicable. TrustCor CA will certify a domain name where the WHOIS report does not identify an actual person as a point of contact, so long as effective control over the domain can be demonstrated to the satisfaction of TrustCor CA.

Enhanced S/MIME certificates may not have pseudonymous organizational details, but the email addresses and common names present therein may be pseudonymous if an authorized contact for the organization represents the email and name as being associated with the organization. The authorized contact must be verifiable via the organizational validation process (eg, listed as a director of the company, etc.)

Enhanced SSL certificates may not have pseudonymous organizational details, and the FQDNs represented in the certificate do not identify real-world persons.

TrustCor CA does not currently issue certificates for .onion domains, until its EV product offering becomes operational.

Enterprise subordinate CAs may offer pseudonymous S/MIME certificates or client certificates within their organization, as long as the names on such certificates satisfy the name restrictions present in their Subscriber agreement and particular CA certificate.

3.1.4 Rules for Interpreting Various Name Forms

The rules for DN name interpretation are defined in the X.520 standards, and also in RFC 4514. Where conflict between the two exists, the LDAP naming interpretation shall take precedence.

TrustCor CA does not permit multiple-AVA components in its DN components.

3.1.5 Uniqueness of Names

Issuer DNs are unique to particular business categories. No two intermediate CAs can have the same Subject DN. End entity certificates may have duplicate Subject DNs under the same Issuer DN, and the serial number is then used to distinguish between certificates bearing such duplicate names.

Domain uniqueness is enforced by ICANN and fqdn uniqueness is enforced by the DNS records of the domain owner.

Time Stamps require a unique hash and time or a unique serial number assigned to the timestamp.

3.1.6 Recognition, Authentication, and Role of Trademarks

Each Subscriber Agreement contains text to state that no Subscriber may knowingly assert identity information to which he or she has no title. This includes trademark information.

If TrustCor CA becomes aware of a dispute involving a trademark which is contained in a certificate it has issued, the company may, at its discretion, revoke any certificate bearing that trademark.

TrustCor CA checks against a list of known high value trademarks which flag any request as being potentially risky. This does not necessarily prevent issuance, but may slow it down as it escalates the level of supervision required to process the request. This list includes (but is not limited to) the trademarks and names of the Fortune 500 companies.

3.2 Initial Identity Validation

TrustCor CA may use any legal and well known paths to contact applicants, for the purposes of validation, including:

- Telephone calls to the applicant directly (for OV certs)
- Telephone calls to the published telephone number for an organization with a request to contact a named applicant (for OV certs)
- SMS messages (DV and OV certs)
- Email (DV and OV certs)
- Postal Services (OV certs, enterprise Subordinate CAs)
- Courier Services (OV certs, enterprise Subordinate CAs)

Submission of a certificate request implies acceptance of TrustCor CA's right to contact the applicant for the purposes of identity validation.

The following information is collected at registration time:

- For all Secure Mail certificates, the email address of the operator of the private/key certificate pair.
- For all Secure Site certificates, the fqdn of the endpoint which will appear as the primary identity in the subject DN.

- For all Basic certificates, whether the requester wishes for all of the certificates in the chain to the root CA to be limited to 2048 bit moduli only (sometimes needed for devices with limited processing power). This choice is not available for Enhanced grade certificates.

All Applicants generate a password/passphrase which can be used to authenticate future communications with TrustCor CA. Passwords can be changed at user request, and must pass quality checks; older passwords may not be reused once changed. Additionally, applicants may set an OTP seed, or register a U2F device, which is used to add an additional authentication factor to login attempts.

3.2.1 Method to Prove Possession of Private Key

All certificate requests must include a PKCS#10 submission, which must pass signature validation in order to prove possession of a private key.

Every PKCS#10 request must not contain a public key which is known by TrustCor CA to belong to a TrustCor CA issued certificate which has been revoked.

3.2.2 Authentication of Organization and Domain Identity

For any OV certificate, the following information is collected upon registration (nb: other information may be collected which does not form part of the validation process):

- Legal name of the organization (publicly exposed)
- Status of the organization (company, charity, NGO, etc.)
- Country of place of registration (publicly exposed)
- Organization registry numbers (e.g. company number, charity registry, tax registry numbers, DUNS number - all which apply)
- State/Province of place of registration (publicly exposed)
- City/Town of place of registration (publicly exposed)
- Technical Contact Name (name, email, telephone)
- Business Contact Name (name, email, telephone)
- Payment Information (credit card, purchase order, etc.)
- Record of acceptance of the Subscriber Agreement

In addition to the information collected in Section 3.2, TrustCor CA will also collect the following identity data:

For Enhanced Secure Site certificates:

- any other FQDNs which will form subjectAltNames in the certificate

This information is validated as per the sections 3.2.2.[1-7]. Evidence or suspicion of alteration or fraudulent representations will be used to deny the certificate issuance, and may trigger reporting of the suspicion to relevant legal authorities.

TrustCor CA does not issue certificates whose Subject Identity Information consists solely of the countryName field.

3.2.2.1 Identity Organization identities are validated using one of the three methods below:

1. Within the jurisdiction of the applicant's organization, a check on a recognized government agency must yield that the organization is registered and currently active. Such agencies can be charity registries, company registries or lists of academic institutions. In all cases the identity of the organization must match the claimed name exactly.
2. A third party database sourced from agencies in part (1) and regularly updated such that TrustCor CA considers it a reliable data source.
3. An attestation letter from a source which TrustCor CA considers reliable and able to speak with authority on the right of the applicant to assert the trade name. This would typically come from a notary public, or other accredited source requiring publicly discoverable membership of a body having the power to enforce high standards of trust amongst its members.

For all OV Code Signing certificates, if the Subject, Subject's Affiliate, Parent Company or Subsidiary Company has been formed within the last three years from time of request, the Certificate Requester's individual identity shall be additionally validated per the steps in Section 3.2.3.

3.2.2.2 DBA/Tradename DBA/Tradenames can be used within the Organization field of the Subject DN of certificates (Enhanced grade).

TrustCor CA will validate the organizational name details with one or more of the following:

1. A government agency in the jurisdiction of the applicant's incorporation capable of pronouncing authoritatively on the status of such trading names (e.g. tax agencies, local authorities, etc).
2. A third party database sourced from agencies in part (1) and regularly updated such that TrustCor CA considers it a reliable data source.
3. An attestation letter from a source which TrustCor CA considers reliable and able to speak with authority on the right of the applicant to assert the trade name.

In all cases, the validation must include reasonable evidence that the organization is currently

operational, or has updated its registration with a relevant registry within the last 398 days at time of request. Dormant or dissolved organizations may not be issued certificates.

3.2.2.3 Verification of Country For Basic grade certificates, country is not verified (and does not appear in the names contained within the certificate). Note that a country code, if present as part of an email address or FQDN does **NOT** count as an assertion by TrustCor CA that the applicant is present or has any relationship with the country identified. (e.g. applicant@this-company.co.uk does not entail validation that the applicant has any connection with the United Kingdom)

For Enhanced grade certificates, the country which appears in the certificate will be that which is derived from the validation process in Section 3.2.2.2; namely the country of incorporation of the organization.

TrustCor CA does not issue IP addressed certificates, so IP-Geo constraints are not required.

3.2.2.4 Validation of Domain Authorization or Control For Secure Email certificates, a challenge email is sent to the mailbox requested in registration. If the mailbox owner is capable of viewing the email, and clicking on a link embedded within it AND entering a verification code provided in the email, then control over the email address is deemed validated. Alternatively, if the user can reply to the email and place the verification code in the subject of the email, then the control is deemed validated.

Verification codes generated uniquely per validation request and time out after a period not exceeding 7 days (although TrustCor CA may shorten that period at its discretion). The codes contain at least 128 bits of entropy and are generated using random number generators designed for cryptographic use.

Alternatively, if an applying user can demonstrate complete control over an email domain (i.e. by control over the MX records which answer for that domain), then any email address within that mail domain may be certified. The methods for domain validation are described below.

If the request was for a Basic Secure Mail certificate, the validation process is complete, and the certificate can be issued, assuming that it would pass the normal checks for uniqueness, key strength and so on.

For Basic Secure Site certificates (and Basic Secure Email certificates where control over a mail domain is being demonstrated), any of the following methods in the following subsections may be used.

For all domain validations, the domain must end in a domain published via

`https://www.publicsuffix.org/list/public_suffix_list.dat`

Specifically, `.int` is recognized as meaning an international organization and **NOT** designating some internal domain.

Note that, unless a validation method is explicitly listed as being permitted for use, any validation method may not be used to obtain a TrustCor CA issued certificate.

3.2.2.4.1 Validating the Applicant as a Domain Contact TrustCor CA does not use Validating the Applicant as a Domain Contact as a validation method.

3.2.2.4.2 Email, Fax, SMS or Postal Mail to Domain Contact TrustCor CA may initiate contact with the applicant the registrar supplied details, communicate with the registrant using email or postal mail to ensure that the request was genuine. If the contact can respond with the correct details regarding the registration request, the domain requested is deemed validated.

In all communications, a request token as formed per section 3.2.2.4.7 is sent to the purported applicant; that same value must be echoed back in all communications. Each application will have a different token. An application which goes for 7 days without response from the applicant will be cancelled, and a fresh application will be required. Details collected in the previous application will be discarded.

Note that the request token appears only in the body of the email, and not in a URL which could be triggered by an automated system. A confirmation URL is present, but the request token must be entered by the user.

TrustCor CA does not use Fax or SMS to validate Domain Contact identity.

3.2.2.4.3 Phone Contact with Domain Contact TrustCor CA does not use the phone contact validation method.

3.2.2.4.4 Constructed Email to Domain Contact TrustCor CA may send a verification email to the well known administrative email addresses for the domains, pruning such components from the FQDN until a registered domain is reached. The administrative mailboxes will be `admin`, `administrator`, `hostmaster`, `postmaster` and `webmaster`. If the holder of any of those address can respond to an email challenge (as per section 3.2.2.4.2), then authority to use the fqdn is established.

The random value challenge sent in such emails will be unique for each email sent, and a response must be received within the 7 days normally assigned to random value challenge windows.

3.2.2.4.5 Domain Authorization Document TrustCor CA does not use Domain Authorization Documents as a validation method.

3.2.2.4.6 Agreed-Upon Change to Website TrustCor CA does not use Agreed-Upon Change to Website as a validation method.

3.2.2.4.7 DNS Change TrustCor CA may request of the applicant that a change to the DNS zone be used to demonstrate domain control.

The applicant must create a TXT record (or augment an existing record) with a token of the following format:

```
trustcor-ca-{base64 representation of a challenge value}
```

This record must be placed at the root TXT location of the domain(s) encompassing the FQDNs requested in the application. Again, it is permissible for there to be multiple such TXT records belonging to separate applications. The validation server will only pay attention to ones matching the application random value.

Alternatively, TrustCor may challenge the applicant to publish a CNAME where the DNS name lives within the authorization domain, and the value of the alias is a random value as described above.

A further option is that the random value may be published within a CAA record for the authorization domain name, where the tag is chosen not to conflict with any well known CAA tags, and the value is the random value described above.

As above, request tokens have a lifetime of 7 days from generation. If the value is not observed within that time, the application verification fails and must be restarted.

A challenge value is the ciphertext of a plaintext constructed as follows:

```
128 random bits || ISO-8601 timestamp (Zulu) || account name
```

(thus including a Random Value as defined within the Baseline Requirements)

The cipher used is AES-128-GCM where the key is randomly generated by systems operated by TrustCor CA, and where encryption and decryption are audited events.

TrustCor CA will query the authoritative DNS servers for the domains, to minimize zone transfer latency to non-authoritative ones. Note that this method can be used to demonstrate full domain control.

3.2.2.4.8 IP Address TrustCor CA does not use the IP Address as a validation method.

3.2.2.4.9 Test Certificate TrustCor CA does not use Test Certificate as a validation method.

3.2.2.4.10 TLS Using a Random Number TrustCor CA does not use TLS Using a Random Number as a validation method.

3.2.2.4.11 Any Other Method TrustCor CA does not allow for any additional validation methods described under this section.

3.2.2.4.12 Validating Applicant as a Domain Contact TrustCor CA does not use Applicant as a Domain Contact as a validation method.

3.2.2.4.13 Email to DNS CAA Contact TrustCor CA will send a challenge value (described in 3.2.2.4.7) to all email addresses present within a CAA record for the domain name being validated, having a tag `contactemail` whose value is an email address valid per the syntax of RFC 6532. The critical flag for this tag is not significant.

The email value must not contain any additional padding or structure.

The relevant resource record set for a particular domain name is described in RFC 8659 Section 3.

The challenge value must then be presented to TrustCor CA's API to verify the correct response of challenge generation. The time limit for this presentation is configured by TrustCor CA, but will never be longer that 7 days. If this time is exceeded, the domain validation is rejected and must be started again.

3.2.2.4.14 Email to DNS TXT Contact TrustCor CA will send a challenge value (described in 3.2.2.4.7) to all email addresses present within a TXT record which has the name

`` `_validate-contactemail.<DN>` ``

where `<DN>` is the domain name being validated. Each value contained within the TXT record must be a validly formed email address per RFC 6532 specifications.

The email value must not contain any additional padding or structure.

The challenge value must then be presented to TrustCor CA's API to verify the correct response. The time limit for such presentation is set by TrustCor CA, but will never be longer than 7 days. If this time is exceeded, the domain validation is rejected and must be started again.

3.2.2.4.15 Phone Contact with Domain Contact TrustCor CA does not use phone contact information as a validation method.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact TrustCor CA does not use phone contact information as a validation method.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact TrustCor CA does not use phone contact information as a validation method.

3.2.2.4.18 Agreed-upon Change to Website v2 For each FQDN requested, TrustCor CA may require of the applicant to place a resource reachable via

```
http://{fqdn}/.well-known/pki-validation
/trustcor-ca-{hash of domain name}.txt
```

(*line breaks are added for clarity*)

This document must contain a base64 representation of a challenge value generated by the TrustCor CA API (see Section 3.2.2.4.7 for token format) prefixed by the string `trustcor-ca-`.

The document may also be presented via the TLS URI

```
https://{fqdn}/.well-known/pki-validation
/trustcor-ca-{hash of domain name}.txt
```

(*line breaks are added for clarity*)

In this case, no validation of the site certificate is done.

The challenge value read will only be validated if the HTTP status code of the request is from 200 through 299 inclusive.

Challenge values have a maximum lifetime provided by the TrustCor CA API. This lifetime will never be longer than 7 days. If TrustCor CA's automated detection software does not pick up the response within that time, the domain validation is rejected, and must be started again.

TrustCor CA's detection software will follow HTTP redirects and still validate the challenge value if and only if the following conditions of the redirection are followed:

- The HTTP redirection code is one of 301, 302, 307 or 308;
- The scheme on the redirected URI is either `http` or `https`
- The URI port on the redirection must be either 80 or 443

TrustCor CA will not issue a certificate embedding a wildcard domain where the domain validation has been demonstrated using this method.

3.2.2.4.19 Agreed-upon Change to Website - ACME TrustCor CA does not use Agreed-Upon Change to Website - ACME as a validation method.

3.2.2.4.20 TLS using ALPN TrustCor CA does not use TLS using ALPN as a validation method.

3.2.2.5 Authentication for an IP Address TrustCor CA does not issue certificates containing IP address identities. Section not applicable.

3.2.2.6 Wildcard Domain Validation TrustCor CA shall issue wildcard domains IF:

- The domain part of the wildcard (ie, text to the right of the '*' character) is not a registry controlled domain. This is established by consulting the public suffix list described above, which is refreshed AT LEAST once every 30 days. Any request to obtain a certificate which is a wildcard on a registry controlled domain must be rejected.
- The validation of the domain has been demonstrated via a method listed above which is both in use and marked as acceptable for issuance of wildcard domains
- Issuance of the wildcard domain is allowed after consultation of the relevant CAA records using the `issuewild` tag. If a method is not marked as forbidden, then it is assumed to be acceptable for wildcard issuance.

3.2.2.7 Data Source Accuracy TrustCor CA reviews its set of reliable data sources regularly and may add or remove entities to that list upon the results of such reviews. The criteria for inclusion is based upon:

- the update and filing process for registry inclusion
- the reliability of the regulatory process governing such institutions
- the timeliness of update to that registry
- the publication of the liveness status of organizations within the registry.

Typically, government information services can be used to fulfill this purpose. The Dun and Bradstreet DUNS number registry may also be used for commercial organizations.

3.2.2.8 CAA Records As mentioned above, any certificate application which contains subject names which are FQDNs, will have the relevant DNS hierarchy searched for relevant CAA records, as per RFC 6844, as amended by Errata 5065.

The relevant tags and values, along with the logging policy, which TrustCor CA uses to process CAA records can be found within Section 4.2.1.

If an application is found, where TrustCor CA is explicitly not entitled to issue, and an controlling `iodef` tagged record is present, which stipulates a `mailto:` or `https:` schemed URI, then TrustCor CA shall endeavor to use that URI to report the apparent attempt to mis-issue the certificate in violation of stated CAA policy.

Both `mailto:` and `https:` reports will contain an RFC 5070 IODEF formatted message. If the protocol is `https:` then the protocols of RFC 6546 will be observed. TrustCor CA will record in its audit logs the success or failure of any reporting attempts. TrustCor CA does not guarantee to retry any failed report.

If the collection of CAA records governing the relevant FQDN does not contain any issue tags, TrustCor CA will interpret this as permission to issue. If any unrecognised tags in the set of CAA records are marked as critical, TrustCor CA will interpret this as **not** having permission to issue (ie, it will be reported as a technical failure).

CAA records are checked up to three times during the validation phase. If three subsequent DNS errors are detected, then the certificate shall not be issued.

Note that permission to issue is granted only if done within the TTL of the CAA record. If that TTL notes a duration shorter than 8 hours, then the 8 hour window applies instead.

3.2.3 Authentication of Individual Identity

For Basic Secure Mail certificates, individual identity is established as per Section 3.2.2.1. For the purposes of this document, 'the requester' means either the person requesting a certificate or a suitable representative capable of communicating on the requesters behalf (in the case where the requester is not legally competent to execute a transaction because of age, incapacity, etc.).

For Enhanced Secure Mail certificates, the requester must provide, in addition to the information above, the following documentation:

- a copy of a current government issued photo-ID, such as a passport, driving license or national identity card. The copy must establish date of birth.
- a copy of a document which establishes association with the organization claimed (letter of employment, assertion from an officer of the company). The document must be no older than 398 days from time of request.

If check codes are to be used to validate a given ID via automated services, a currently valid check code must also form part of the identity documentation submission (For example, the DVLA of the UK government allows a license holder to generate check codes such that an external validator can validate that a license is properly issued for a given purpose)

The above information is validated by contact with the appropriate government agency for identity issuance, and further contact with the organization using its published contact addresses/telephone numbers to establish the individual association.

Secure Site certificates do not establish individual identity, so this section does not apply.

For Code Signing certificates, the requester must submit, as part of its request, a copy of a valid government issued ID (passport, driver's license, national ID). The request must be digitally signed by a valid personal certificate which chains up to a trusted root in the AATL. TrustCor CA will conduct a web camera based verification of the identity of the requester where both the original of the ID used must be held by the requester at the same time as the requester appears on camera. TrustCor CA will then record that the identity of the requester matches the ID, or not. If not, the Certificate Request will be denied.

3.2.4 Non-verified Subscriber Information

No information which cannot be verified can form any part of a TrustCor CA certificate's identity information. If a field has no validation, it is omitted from the certificate.

DNS names need not be resolvable, but the domain in which they reside must be able to be validated. For example, an applicant which had established control over the entire `example.org` domain could request certificates for `test.example.org`, even if its DNS configuration did not allow `test.example.org` to be resolved from outside of its network.

3.2.5 Validation of Authority

Any applicant may, as part of the registration process, designate a set of technical contacts allowed to request (or revoke) certificates within domains over which it has demonstrated effective control. If the applicant applies as an organization for certificates designating that organization, then TrustCor CA will use the methods described above to validate the organization, using contact details derived from the validation process to establish authoritative email addresses, phone numbers or physical addresses to use to contact the applicant.

Those contacts must be verifiable via email, physical address or telephone communications with the applicant. At any time, the applicant can request the current contacts from TrustCor CA, which must reply within 2 business days.

3.2.6 Criteria for Interoperation or Certification

TrustCor CA may cross-certify other CA certificates, subject to a specific agreement between TrustCor CA and another the other party. Equally, parts of TrustCor CA's CA hierarchy may be cross-certified by another CA, subject to business agreement.

In either case of certification, the cross-signed certificates will be made available under the same terms as TrustCor CA's own CA certificates on the repository specified in Section 2.1.

3.3 Identification and Authentication for Re-key Requests

Re-keying, in this section, is defined as being the reissue of a certificate with a different public key, but containing the same identity information as was present in the original certificate.

In all re-key requests, a new public key must be submitted as a PKCS#10 document within the request.

3.3.1 Identification and Authentication for Routine Re-key

Routine re-key is authenticated by the certificate owner presenting knowledge of a shared secret to TrustCor CA's rekeying service via:

- use of a TrustCor CA website which requests a user and password combination, the password being the shared secret

This user/password combination is sufficient for all Basic grade certificates.

For Enhanced Secure Email certificates, a signed email request signed by the certificate needing re-key will suffice (assuming that the certificate has not been revoked hitherto).

Enterprise Subordinate CAs may only be re-keyed via a manual process involving reassessment of the original documents and policies that the Subscriber has submitted to TrustCor CA.

For Subscriber code signing, a username and password is sufficient to authenticate for routine re-key.

Under all circumstances, if identity validation was substantiated by documentation, that documentation must not be older than 398 days from time of re-keying. If the documentation is older, then a new certificate request must be made, after revoking the old certificate.

3.3.2 Identification and Authentication for Re-key After Revocation

For all Basic Grade Certificates and Enhanced Secure Mail Certificates, re-keying is not allowed post revocation. The certificate may be applied for again; TrustCor CA reserves the right to credit some portion of registration and issuance fees to the Subscriber in this instance.

For all Site Certificates, re-keying is not permitted post revocation.

For Enterprise Subordinate CAs, re-keying is not permitted post revocation.

3.4 Identification and Authentication for Revocation Request

Revocation authentication is dependent on who makes the request:

- Subscriber revocation: simple authentication via username and password (via website authentication) is sufficient to begin revocation. If the certificate is an S/MIME one, verifying a signed email requesting revocation of the signing certificate is sufficient identification and authentication.
- TrustCor CA revocation: CA/RA administrators are required to authenticate to the CA software via client certificates issued by an internal management CA, in order to revoke a Subscriber's certificate.

TrustCor CA will react to external trusted parties requesting revocation, evaluate the evidence, and revoke if circumstances dictate such action. In this case, the identification and authentication protocols for "TrustCor CA Revocation" hold.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

Certificate application can be done via one of two means:

- Website application: the applicant fills in a web form which then creates a certificate issuance request in TrustCor CA's ticketing software.
- Email application: the applicant submits a specified format email to the certificate request email address for TrustCor CA, which then creates a certificate issuance request in TrustCor CA's ticketing software.

4.1.1 Who Can Submit a Certificate Application

Any member of the general public, who complies with the provisions specified in this CPS and relevant Subscriber Agreement, can apply for a TrustCor CA certificate, assuming that they can either view HTTPS web servers or send and receive email.

TrustCor CA maintains an internal database of all (its own) revoked certificates and rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. This internal database is used to identify subsequent suspicious certificate requests and to determine an Applicant's eligibility for a certificate.

TrustCor CA will not issue certificates to individuals or entities thought to present an unacceptable risk of fraud or damage to TrustCor CA's business.

Application for Enterprise Subordinate CA certificates may be initiated via email, but the process of registration and validation then requires postal/courier communications, as well as possible site visit scrutiny from TrustCor CA.

4.1.2 Enrollment Process and Responsibilities

Prior to the issuance of a Certificate, TrustCor CA will obtain the following documentation from the Applicant:

- An electronic certificate request; and
- An executed Subscriber Agreement or Terms of Use, which may be electronic.

The enrollment process involves:

- Generating an account for the certificate Applicant,
- Collecting the identification information the Applicant wishes to see included in the certificate,
- Collecting a validly formed PKCS#10 (CSR) request containing either an RSA public key, or an ECC public key, and
- An agreement from the Applicant that TrustCor CA may used the methods specified in this CPS to validate any information which the Applicant provides.

The responsibilities on the Subscriber include:

- Providing complete and accurate information regarding identity,
- Keeping the private key corresponding to the public key in the CSR confidential, and
- Generating a public key which satisfies the requirements of the TrustCor CA program.

The responsibilities on TrustCor CA include:

- Preserving the integrity and confidentiality of communications between the Subscriber and TrustCor CA,
- Not permitting unauthorized disclosure of any personal identifying information (PII) in compliance with the TrustCor CA Privacy Policy, and
- Validating to the best of its ability that the evidence supplied from the Subscriber is authentic, current and suitable to establish the identity guarantees which the certificate would assert.

4.2 Certificate Application Processing

For all Basic and Enhanced grade certificates, the processing of the application is done by TrustCor CA, and the issuance done under one of the CAs described in Section 1.3.1.

For Enterprise Subordinate CAs, the processing is done by the RA belonging to the Enterprise Subscriber, and issuance is done under the technically restricted CA software under the Enterprise Subscriber's control.

4.2.1 Performing Identification and Authentication Functions

After receiving an application for a certificate, TrustCor CA will perform several validation steps, dependent on the type of certificate requested.

For all certificate types, TrustCor CA establishes that the entity making the request is the one whose identity is going to appear in the certificate. TrustCor CA further ensures that the requester has provided evidence of holding a private key. In no case, can any information used to validate a certificate request be older than 825 days from the time of request. This includes information which is used to re-validate a renewed certificate request.

TrustCor CA will check its internal database of suspect Applicants (those who have failed prior applications on grounds of providing false information, as well as those who have had certificates revoked because of improper behavior) to ensure that the applicant does not represent an unacceptable risk to TrustCor CA.

TrustCor CA will also check lists of proscribed organizations and people prohibited from receiving cryptographic services, via the US Treasure Department Specially Designated Nationals lists published by the government of the United States of America, as well as lists of domains deemed to present unacceptable risks of fraud/phishing/malware propagation. The result of that check determines whether application can proceed or not.

TrustCor CA also maintains a list of high value trademarks and domains. If a request is visually similar to an entity on that list (via the confusables mapping) the request may be designated

high risk and require human intervention to progress the application. If a request is felt (by TrustCor CA personnel) to possess a high likelihood of being fraudulent then the requester's account may be recorded in an internal database, and used to reject future requests.

TrustCor CA also checks its internal database to establish whether the request constitutes a High Risk Certificate Request (e.g. if it seems that the request includes names at higher risk for phishing or fraud, or names determined to be at a high risk for other unacceptable behavior); such certificates are not automatically issued, but flagged for additional scrutiny by the TCPA to either permit or deny the request.

TrustCor CA will flag a Certificate Request as being High Risk if TrustCor CA's validation processes show evidence that the requester has been suspected of signing Suspect Code or if the request emanates from a High Risk Region of Concern (HRRC). If TrustCor obtains evidence that the requester *has* signed Suspect Code, the request will be denied, as will all subsequent requests which appear to emanate from the same requester.

For all Secure Site certificates, TrustCor CA runs a check against DNS CAA records (as per RFC 6844 amended by Errata 5065) for the domains corresponding to the FQDNs to be in the certificate. The result of that check will instruct the certificate processing system whether to proceed or halt application.

The CAA record values which will permit TrustCor CA to issue the certificate are:

- `issue` tag: must contain the text `trustcor.ca`
- `issuewild` tag: must contain the text `trustcor.ca`.

If a certificate request to TrustCor CA is denied on the basis of CAA records preventing the application from proceeding, then the issuance is stored in the audit logs such that the details of the request and refusal on the basis of CAA policy can be demonstrated to the CA/B Forum.

For Enhanced grade certificates, TrustCor CA will use all reasonable means to validate the organizational identity claimed, and that the organization is a 'live' entity (ie, not dormant, prohibited from trading, or dissolved).

TrustCor CA does not issue certificates to FQDNs under those domains reserved as IANA managed domains (available via `https://www.iana.org/assignments/special-use-domain-names/special-use-domain.csv`), nor to any of the test domains listed in `https://www.iana.org/domains/reserved`

4.2.2 Approval or Rejection of Certificate Applications

TrustCor CA may reject an application for a certificate for any reason, or for no reason at all.

While TrustCor CA's general policy is to provide an Applicant with the reasons for which an application is rejected, it is under no obligation to do so.

TrustCor CA will reject certificate application if the public key is deemed to exhibit known mathematical weakness against attack (so called `weak keys`), or if the private key corresponding to the public key is known (by TrustCor) to have been observed in public fora.

TrustCor CA will only approve certificates containing FQDNs if it is not prohibited from issuance, or is explicitly permitted to issue, certificates via the CAA records for the relevant domains containing the FQDNs.

TrustCor CA will only issue certificates if the applicant is not on any sanctions list published by the government of the United States of America, and that the applicant does not appear within TrustCor's privately maintained blacklist.

Assuming that the validation checks succeed, and that the information for certificate processing is complete, TrustCor CA will approve the issuance of the certificate.

In the event that request details are found to be fraudulent, TrustCor CA reserves the right to store such details from the application as it deems useful to prevent further fraud or potential damage to its business. TrustCor CA also reserves the right to forward such information to law enforcement bodies for further investigation.

As mentioned elsewhere, all FQDNs and email addresses to be embedded in TrustCor CA certificates must be within the ICANN section of the public suffix database.

At most every 30 days, the public suffix list is consulted - if a gTLD is no longer on the approved ICANN list, all certificates under that previous gTLD certified by TrustCor CA will be revoked. Re-application or re-keying for such certificates will not be allowed.

4.2.3 Time to Process Certificate Applications

For Basic certificates, TrustCor CA will process a certificate request within 2 days of submission. The application will close automatically, rejecting the request, if 7 days have gone from application without the relevant demonstration of domain control having been observed.

For Enhanced certificates, TrustCor CA will either approve or reject the request within 30 days of submission. If confirmation for the organizational identity cannot be gained in that time, then the application is rejected.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

TrustCor CA issues certificates immediately post approval. Each issuance is logged with the identity of the principal issuing the certificate, and the action logged in the CA audit log.

Serial numbers on issued certificates are randomly generated, and contain a minimum of 64 bits of entropy.

Root CA certificate issuance (ie, subordinate CAs) may only be performed by individuals (natural persons, not automated processes) specifically authorized to perform this task by TrustCor CA. The signing may only be performed by a direct command being issued by that individual.

4.3.2 Notification of Certificate Issuance

The Subscriber may use TrustCor CA's CA-API to determine the issuance status of a certificate and/or download the certificate to the Subscriber's custody.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

If the Subscriber deploys the certificate into use, by signing emails, or establishing a website fronted by that certificate, then the certificate is deemed to be accepted by the Subscriber.

If the Subscriber is not satisfied with the details contained within the certificate, he or she must email `support@trustcor.ca` explaining why the certificate is not being accepted. This communication must take placed within 30 days of issuance, otherwise the certificate is deemed to have been accepted.

The mechanisms for acceptance are established in the Subscriber agreement.

4.4.2 Publication of the Certificate by the CA

In the case of DV and OV certificates, upon a positive decision to issue the certificate under application, TrustCor CA shall first produce a pre-certificate (defined per RFC 6962); this pre-certificate shall be submitted to a minimum of three CT logs (or two CT logs if the duration of the certificate is shorter than 398 days). These logs must, at time of issuance, be mentioned in the list of well known logs available via:

Certificate Transparency Known Logs

Where possible, the logs used for publication shall not be owned and operated by the same company. However, in the event of temporary technical failure, it is permissible to have a single owner of the logs. The issuance log details shall record the failures encountered while attempting to publish to the logs.

TrustCor shall endeavor to ensure that its publication policy matches the requirements set by such browser root programs of which TrustCor CA is a member.

If an insufficient set of replies from the various CT logs is received, the pre-certificate must be held and retried (at least three times, per calendar day). If, after three calendar days of retrying, a relevant quorum of SCTs has not been compiled, the pre-certificate must be revoked, and the failure reported to the Applicant.

Once SCTs have been collected from as many logs as possible, those SCTs are embedded into the certificate as an extension. This certificate is then made available to the Applicant.

The final certificate is also submitted (by TrustCor CA) to the CT logs, such that the SCTs so gained may be made available via a TLS header or OCSP extension. The logs for the final certificate are not guaranteed to be the same as the ones used for the pre-certificate, but the publication policy regarding number and ownerships of logs remains unchanged.

Note that any external partners who own and operate subordinate CA under the External PKI program are required to follow the above CT publication policy for their DV and OV certificates.

S/MIME certificates, Timestamping Certificate and Code Signing Certificates are not published to CT logs. These are only communicated to the end users.

CA certificates are published on the online repository explained in Section 2.1

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Other than CT publication per 4.4.2, no notification to other entities is performed.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers are prohibited from engaging in conduct which compromises the integrity or confidentiality of the private key.

The certificate issued may only be used for those purposes which the Subscriber Agreement denotes, and consonant with the keyUsage and extendedKeyUsage flags present within the certificate.

For Code Signing Certificates, Subscribers are required to store the private key component on either:

- a TPM embedded into a computer owned by the Subscriber
- a FIPS-140-2 L2 or Common Criteria EAL 4+ device.

Storing the private key on a non-rated device (like a USB stick) is not permissible and constitutes a violation of the relevant Subscriber Agreement.

4.5.2 Relying Party Public Key and Certificate Usage

RPs are under a duty to rely upon the information present in a certificate only where the following conditions apply:

- the certificate chain up to a trusted root certificate has been built
- the signatures on each certificate have been verified
- each certificate below the root has been validated against a current CRL or OCSP response
- the certificate is not being used for a purpose other than allowed in its key usage specifications

Even when this information has been validated, RPs cannot use it to place any reliability on the honesty or integrity of the certificate owner, since TrustCor CA can not verify such matters.

4.6 Certificate Renewal

TrustCor CA will only renew a certificate (ie, re-issue it with the same identity and public key but with an updated validity period) under the same business offering which the certificate was first issued.

A Basic grade Certificate cannot be renewed to an Enhanced grade one, and vice versa. Similarly, a Secure Email certificate cannot be transformed into a Secure Site one (even if the identities were such as to make such a transformation meaningful).

Certificates may only be renewed for the lifetime of a certificate specified in the business offering.

4.6.1 Circumstance for Certificate Renewal

If a request for certificate renewal is lodged with TrustCor CA, it will only renew when:

- the Subscriber confirms that the details within the certificate have not altered from the original submission
- the documentation which was used to validate the original request is still current at time of renewal (for example, a driver's license is expired now, but was valid at original submission time)

4.6.2 Who May Request Renewal

Subscribers can request renewal of certificates. TrustCor CA does not renew certificates automatically.

Enterprise Subordinate CA Subscribers may accept renewal requests from agents within their enterprise if the relevant Subscriber Agreement allows this arrangement.

4.6.3 Processing Certificate Renewal Requests

The Subscriber must authenticate himself or herself to the TrustCor CA system either by:

- use of a website function for renewal after authentication via username and shared secret.
- use of secure email to send a renewal request, where the body of the email contains a signature capable of validating the request.

Both methods require a statement from the Subscriber that the details in the certificate have not altered and that any associations present in the certificate still hold. A PKCS#10 submission is not required, since the public key is not changing.

TrustCor CA will then verify that:

- the credentials demonstrated on the renewal are valid
- the original submission lives within the maximum renewal time stated by the business offering under which the certificate was issued
- that any documentation used to validate the original request are still valid, for Secure Site certificates and Enhanced Secure Mail certificates.

4.6.4 Notification of New Certificate Issuance to Subscriber

See section 4.3.2 for notification protocols.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See section 4.4.1 for acceptance criteria. Note that the 30 day period for accepting of identity information in the certificate does not apply here, since that acceptance is deemed to have happened already.

4.6.6 Publication of the Renewal Certificate by the CA

With the exception of CT logs for site certificates, end entity certificates are not published to any public resource, other than by notification to the Subscriber.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

TrustCor CA does not commit to notifying issuance of any certificate to any other party, except as named above.

4.7 Certificate Re-Key

Re-keying is defined as the re-issuance of a certificate with a new public key, but the same subject identity information.

Re-keying is not allowed to transform a certificate issued under one program to that issued under another.

TrustCor CA does not (in general) re-key after revocation of a certificate, but may credit a Subscriber such that a resubmission for a certificate does not cost the Subscriber any more.

4.7.1 Circumstance for Certificate Re-Key

Re-keying may take place by way of a renewal process. It may also take placed in the case of Enhanced Secure Site certificates, where the certified set of names has been altered.

4.7.2 Who may request certification of a new public key

Subscribers may request re-keying. TrustCor CA at its discretion may also do so.

4.7.3 Processing certificate re-keying requests

A re-key request is similar to requesting a new certificate. The Subscriber must (re-)state which subject details are to be present in the certificate, and provide a PKCS#10 document containing the public key to be certified.

If a Subscriber initiates this process, the Subscriber must authenticate to TrustCor CA by:

- website authentication using a user name and shared secret
- secure email where the re-key request body contains a valid signature from the Subscriber

Note that in the event of certificate revocation, the signature validation will fail, so this may not always be possible.

The subject DN of a re-keyed certificate cannot change in any circumstance.

For Enhanced Secure Site certificates, the new set of names must include the name on the subject DN. If any name is deleted from this list, then the original certificate is automatically revoked, and the re-key processed with the new names.

For all Secure Site certificates, the documentation regarding authority to use the FQDNs must still be valid, and a CAA check is still required. If those checks fail, the re-key is halted.

4.7.4 Notification of new certificate issuance to Subscriber

See Section 4.3.2 of this document for notification protocols.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See Section 4.4.1 of this document for acceptance criteria.

4.7.6 Publication of the re-keyed certificate by the CA

Other than Subscriber notification, the re-keyed certificate is not made public.

4.7.7 Notification of certificate issuance by the CA to other entities

Other than CT publication, TrustCor CA does not notify other entities of certificate issuance following a re-key operation.

4.8 Certificate modification

TrustCor CA operates a certification modification process for Enhanced Secure Site certificates only, where additional subjectAltNames for FQDNs can be added into the certificate, without changing the key or subject DN of the certificate.

If the additional name process requires a PKCS#10 submission to TrustCor CA. The public key must match the one currently in the certificate to which the new name is being added. However, if the public key belongs to a certificate which has been revoked, this modification will not succeed. A revocation requires a new public key to be submitted, in all cases.

Other than that, TrustCor CA does not allow certificate modification.

4.8.1 Circumstance for certificate modification

If a Enhanced Secure Site Subscriber wishes additional dNSName subjectAltNames *added* to his/her certificate, he/she can apply to TrustCor CA to have those added.

If any names are to be deleted from the certificate, then the process becomes a revoke and re-submission as per the processes described above.

4.8.2 Who may request certificate modification

Subscribers holding Enhanced Secure Site certificates may request modification.

TrustCor CA will modify end-entity certificates where the continued existence of the unmodified certificate would violate a competent court order, or because of algorithm weakness, represent an unacceptable threat to the integrity of TrustCor CA's business. All such TrustCor CA initiated modifications must be recorded as security events in the ticketing workflow system.

4.8.3 Processing certificate modification requests

Additional subjectAltNames are collected, and the request authenticated, by one of two methods:

- via a website form where the username password and two factor response code are used as proof of identity
- via an email to `requests@trustcor.ca` requesting the modification, signed by a TrustCor CA Secure Email certificate. The emailAddress in the S/MIME certificate must match that of the username on the account owning the Enhanced Secure Site certificate.

Each new name on the certificate is validated to belong to the set of already validated domains within the existing certificate. If this is not the case, additional documentation validating the certificate holders right to claim the FQDN must be supplied. Such additional names are passed through the CAA check and normal domain validation rules.

4.8.4 Notification of new certificate issuance to Subscriber

See section 4.3.2 for notification protocols.

4.8.5 Conduct constituting acceptance of modified certificate

See section 4.4.1 for acceptance criteria.

4.8.6 Publication of the modified certificate by the CA

Other than Subscriber notification, the modified certificate is not made public.

4.8.7 Notification of certificate issuance by the CA to other entities

Other than CT publication, TrustCor CA does not notify other entities of certificate issuance after a modification operation.

4.9 Certificate Revocation and Suspension

TrustCor CA offers the services to permanently revoke any certificate issued by it.

TrustCor CA does not suspend certificates (that is, revoke and then unrevoke them).

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate TrustCor CA shall revoke a Subscriber Certificate within 24 hours of any of the following events occurring:

1. The Subscriber requests in writing that TrustCor CA should revoke the Certificate;
2. The Subscriber notifies TrustCor CA that the original certificate request was not authorized, and that authorization is not being granted retroactively;

3. TrustCor CA obtains evidence (whether from the Subscriber or elsewhere) that the Subscriber's Private Key corresponding to the Public Key in the Certificate has been compromised; or
4. TrustCor CA becomes aware that the validation process for domain authorization or control for any FQDN in the Certificate should not be relied upon.

TrustCor CA will normally revoke a Subscriber Certificate within 24 hours, but certainly within five (5) days if any of the following occurs:

1. The Certificate no longer satisfies the requirements of Sections 6.1.5 and 6.1.6;
2. TrustCor CA becomes aware that the Certificate was misused;
3. TrustCor CA becomes aware that a Subscriber has violated one or more of its obligations under the CP, this CPS, Subscriber Agreement and/or Terms of Use;
4. TrustCor CA becomes aware that any FQDN or email address in a Certificate is no longer legally permitted (this can include such conditions as a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
5. TrustCor CA becomes aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name.
6. TrustCor CA becomes aware of a material change in the information contained in the Certificate;
7. TrustCor CA becomes aware that the Certificate issuance was not performed in accordance with the CP, or this CPS;
8. TrustCor CA determines that any of the information appearing in the Certificate is not accurate;
9. TrustCor CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless TrustCor CA has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by TrustCor CA's CP and/or this CPS;
11. TrustCor CA becomes aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key, or if there is clear evidence that the specific method used to generate the Private Key was flawed; or
12. TrustCor CA determines that the ongoing existence of the Certificate represents an unacceptable risk to its business operations.
13. (For code signing certificates) A third party provides information that leads TrustCor CA to believe that the certificate is compromised or is being used for Suspect Code.

TrustCor CA will revoke a Subscriber Certificate within two (2) business days of receipt of the request, if any of the following occurs:

1. (For code signing certificates) The Application Software Supplier requests revocation and where TrustCor CA decides that revocation is warranted.

In the event that, following an investigation triggered by the above, TrustCor CA decides not to revoke the Certificate, TrustCor CA will inform the Application Software Supplier of its decision within two (2) business days. If TrustCor CA decides that revocation will have an unreasonable impact on its customer base, it will propose an alternative course of action to the Application Software Supplier, based on its investigation.

4.9.1.1.1 Meaning of Revocation Reasons TrustCor CA interprets the revocation reasons from RFC 5280 as having the following meanings. For all such revoked Certificates, the private key is not deemed to be compromised unless explicitly stated.

- *unspecified* (0) : Default used by TrustCor CA
- *keyCompromise* (1) : When the Subscriber has reason to believe that the private key corresponding to the public key in the Certificate has been compromised (this will then affect any other TrustCor CA issued certificates which share this public key)
- *cACompromise* (2) : Used for CA-certificates only when the CA which issued the Certificate is no longer trusted
- *affiliationChanged* (3) : When the Subscriber needs to change organizational information in the Certificate
- *superseded* (4) : The Certificate is no longer needed by the Subscriber, but may have been replaced with another Certificate bearing a similar name (possibly from a different CA)
- *cessationOfOperation* (5) : The Certificate is no longer needed by the Subscriber due to discontinuing use of their website or no longer owning domains listed in the Certificate
- *certificateHold* (6) : Not used by TrustCor CA
- *undefined* (7) : Not used by TrustCor CA
- *removeFromCRL* (8) : Not used by TrustCor CA
- *privilegeWithdrawn* (9) : Reserved for use only by TrustCor CA admins
- *aACompromise* (10) : Not used by TrustCor CA

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate TrustCor CA will revoke a Subordinate CA Certificate within seven (7) days if any of the following occurs:

1. The Subordinate CA requests revocation in writing;

2. The Subordinate CA notifies TrustCor CA that the original Certificate request was not authorized and does not retroactively grant authorization;
3. TrustCor CA discovers that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate has been compromised or no longer complies with the requirements of Sections 6.1.5 and Section 6.1.6;
4. TrustCor CA discovers that the Certificate was misused;
5. TrustCor CA becomes aware that the Certificate was not issued in accordance with, or that the Subordinate CA has not complied with the Baseline Requirements or the applicable CP or the terms of this CPS;
6. TrustCor CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. Either TrustCor CA or Subordinate CA ceases operations, for any reason, and has not made arrangements for another CA to provide revocation support for the Certificate;
8. Either TrustCor CA or Subordinate CA loses the right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless TrustCor CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by TrustCor CA's CP and/or this CPS; or
10. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

4.9.2 Who Can Request Revocation

The Subscriber owning a certificate may request revocation.

For Enhanced grade certificates, either the business contact or technical contact for the certificate may request revocation. If TrustCor CA has issued certificates to employees/contractors of a organization, any officer of that organization may request (in writing) that such certificates be revoked, whether individually or en masse.

TrustCor CA, on its own initiative, may revoke a certificate.

Certain well trusted entities known to TrustCor CA may request revocation. These include, but are not limited to:

- representatives of the browser root certificate programs such as Microsoft, Mozilla, Apple, where TrustCor CA has been accepted into such programs.
- (For code signing), Application Software Suppliers.
- representatives of the CA/B Forum.

4.9.3 Procedure for Revocation Request

Revocation requests may come in one of the following forms:

- Via an S/MIME signed email, stating the issuer DN, serial number of the certificate and reason for revocation. This email is sent to `revoke@trustcor.ca` (the serial number and issuer DN may be fetched from the S/MIME signature, if the end-entity certificate is included);
- Via an unsigned email to `revoke@trustcor.ca`, stating issuer, serial and reason, and a stipulation that the sender is a listed officer or director of the organization represented within a certificate;
- Via signed postal mail, written to TrustCor CA at the following address:

  TrustCor CA Revocation Service, 371 Front Street West #227 Toronto, ON M5V3S8 Canada

  This mail must contain contact details (including physical address, email addresses or phone numbers) which enable TrustCor CA to contact the requester in order to validate the revocation request;
- Via API or client interface after proper account authentication; or
- Via TrustCor CA's internal ticketing system, which is authenticated via username and password. (This is restricted to requests originating from TrustCor CA itself).

For signed emails, the signature will be validated to ensure that it sufficiently identifies the requester as belonging to the authorized groups listed in Section 4.9.2.

For unsigned emails, TrustCor CA will attempt to:

- Verify that the requester named is an appropriately named officer or director of the organization involved, via reliable registries of organizations; and
- Contact the stated requester using contact information obtained from those registries. If contact cannot be gained through this method, the revocation request will be denied.

The unsigned email approach is only usable for Enhanced grade certificates, which embed organizational identity. If the request is not authenticated, then the request is denied, and the revocation ticket updated to include why no action was taken.

For web forms, this limits the client to requesting revocation for any of the certificates assigned to that user account.

Non-Subscribers, relying parties, application software vendors, and other third parties will find TrustCor CA's certificate revocation process, as well as instructions for filing a Certificate Problem Report, detailed at `https://revoke.trustcor.ca/`.

Once a request has been deemed valid, a certificate revocation request is added as a service request to TrustCor CA's internal ticketing software, which is acted upon by an agent allowed to contact the CA software and perform the revocation. Both the ticketing log and CA revocation log are audited events.

TrustCor CA maintains the ability to accept revocation requests via email, physical mail and ticket requests on a continuous 24x7 basis.

4.9.4 Revocation Request Grace Period

If a Subscriber is dissatisfied with the content of the certificate issued, that Subscriber has 30 days to request a revocation.

If the circumstances change such that a Subscriber may no longer assert the truth of certificate details, TrustCor CA must be informed of this within 4 business days.

Any private key compromise of an end-entity certificate must inform TrustCor CA of this compromise within 24 hours of discovery.

Private key compromise of a Subordinate CA must be reported to TrustCor CA within 1 hour of discovery.

4.9.5 Time within which CA Must Process the Revocation Request

Properly validated revocation requests are normally processed within 1 hour of validation. TrustCor CA will not delay processing of a revocation request for longer than 24 hours post validation.

In all end-entity certificate cases, the Subscriber for the certificate will be kept informed as to the circumstances of the revocation request, as well as the revocation requester (in the case where these identities are not the same). If the decision is made by TrustCor CA to proceed with revocation, then that date shall be communicated to the Subscriber and requester.

Should the decision to revoke be made, that proposed date of revocation will be 24 hours under the following circumstances:

- the request came in writing (the web form is deemed to be in writing) from the Subscriber, and the request was authenticated as being valid.
- the request came from the Subscriber, stipulating that the original certificate request was not authorized by him/her, and that he/she does not grant such authorization.
- TrustCor CA has reasonable grounds to believe that the private key corresponding to the certificate had been compromised.

- TrustCor CA obtains evidence that the FQDN validation method result was unreliable.

In all other circumstances, the timeframe between initiating the revocation process and either revoking, or refusing to revoke, must take no longer than 4 calendar days.

Subordinate CA revocation requests will be processed within 1 hour of validation of the request for revocation, unless a direct instruction from the TCPA states otherwise, should the disruption to business outweigh the harm from delayed revocation.

For code signing certificates where the revocation request stems from the alleged signing of malware, TrustCor CA shall follow the timeframe established in the Minimum Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates in section 13.1.5.

4.9.6 Revocation Checking Requirement for Relying Parties

Any RP must verify the validity of any subordinate certificate or end-entity certificate against the appropriate CRL or OCSP service. Failure to do so imposes the entire risk of reliance on the RP, and TrustCor CA can accept no responsibility whatsoever.

4.9.7 CRL Issuance Frequency

For the status of Subscriber Certificates, TrustCor CRL is updated and reissued routinely every 24 hours; and at minimum once every seven (7) days and the value of the nextUpdate field must not be more than ten (10) days beyond the value of the thisUpdate field and is routinely completed in four (4) days.

For the status of Subordinate CA Certificates, TrustCor CRL is updated and reissued routinely every six (6) months; and not exceeding twelve (12) months. Within twenty-four (24) hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field must not be more than twelve (12) months beyond the value of the thisUpdate field and is routinely completed in six (6) months.

4.9.8 Maximum Latency for CRLs

CRLs for Subscriber Certificates are posted automatically to the repository within a commercially reasonable time after generation. Regularly scheduled CRLs are posted prior to the nextUpdate field in the previously issued CRL of the same scope. From signing a new CRL to publishing it on the online repository, TrustCor CA will normally take no more than 1 hour to do so.

4.9.9 On-line Revocation/Status Checking Availability

TrustCor CA fields OCSP services at multiple global locations which provide current responses with low latency.

OCSP responses have validity periods of:

- 4 days for end-entity Certificates (SSL, Email and Code Signing)
- 6 months for CA Certificates and Timestamp Certificates.

New OCSP responses are produced at a minimum frequency of half the validity periods shown above (e.g. 2 days for SSL, EMail and Code Signing certificates, and 3 months for CA and Timestamping Certificates).

OCSP services are configured for failover capability and 24x7 availability.

OCSP responses may be signed by dedicated OCSP responder identities, rather than the CA identities themselves (although CA signed responses may be used as well). OCSP responder certificates have a maximum validity period of 825 days. Those delegated responder certificates contain the `id-pkix-ocsp-nocheck` extension.

TrustCor CA's OCSP conforms to RFC 6960, as well as the profile stipulations of RFC 5019. Note that TrustCor CA does not guarantee to observe all of the extensions mentioned in RFC 6960. In particular, TrustCor CA reserves the right not to honor nonce extensions present.

TrustCor CA uses the profile in RFC 5019 to restrict its OCSP responses to be suitable for use in a high capacity environment. Specifically, requests which specify multiple certificate status requests in a list may not be answered, since that precludes pre-generation of OCSP responses.

TrustCor CA's external OCSP servers are open to the public internet.

4.9.10 On-line Revocation Checking Requirements

TrustCor CA OCSP servers support both the GET and POST methods for querying over HTTP.

TrustCor CA OCSP services will not produce a `good` status reply when asked about a certificate which has not been issued.

Any RP checking TrustCor CA must conform to RFC 6960 and the client profiles established in RFC 5019, and is constrained to validate signatures by the methods described in section 3.2 of that document.

4.9.11 Other Forms of Revocation Advertisements Available

TrustCor CA does not require its customers to deploy OCSP stapling, and does not monitor that they do so.

4.9.12 Special Requirements Related to Key Compromise

The mechanisms which TrustCor CA will accept as indicating key compromise are:

1. The authorized use of the TrustCor CA API to revoke a certificate using the `key compromise` reason (the documentation for this approach can be found on docs.trustcor.com);
2. Sending an email to `revoke@trustcor.ca` which contains details of the certificate to be revoked, along with the corresponding private key in an accessible format (e.g. not encrypted, or encrypted with the key material being provided to TrustCor CA); or
3. Sending an email to `revoke@trustcor.ca` which contains details of the certificate to be revoked, along with a message, digitally signed by the private key corresponding to that within the certificate detailed, where that message carries an unambiguous intent that the key should be considered compromised. An example message could be a CMS message whose body was "The key used to sign this message is compromised", or a JWS object whose payload carried a similar meaning within it.

Where certificates must be identified for revocation, the reporting message must *uniquely* identify the certificate in question. Thus, the message may contain either the certificate itself in a well known format (DER or PEM), or sufficient detail regarding the certificate so as to make identification clear (for example, the name of the issuing CA and the serial number of the certificate). Reports which do not contain such details will not be considered sufficient to begin the 24 hour revocation window.

4.9.13 Circumstances for Suspension

TrustCor CA does not suspend certificates. Revocation is permanent.

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

CRL download and OCSP services are made available on a global basis.

4.10.1 Operational Characteristics

For Secure Site certificates, the status of certificate is retained in a CRL until 1 day after the certificate's expiry date has passed, and then it may no longer be present in the CRL (and OCSP queries may not return a known status for the expired certificate).

Secure Email certificates have their status discoverable in the OCSP repositories for 7 years after expiry. Expired certificates may be removed from secure email CRLs in order to stop the size of the CRL growing without bound.

For Code Signing certificates, CRLs will contain revoked serial numbers for a period of 10 years after the expiration of the Code Signing certificate. OCSP responses for Code Signing certificates will be available for 10 years after expiry.

OCSP responders will never yield a 'good' response to a certificate query where no certificate has been issued for that serial number.

4.10.2 Service Availability

OCSP responses and CRLs are available 24x7 over at least 4 geographical locations.

Both OCSP and CRL download services are made available via plaintext HTTP, not HTTPS.

All OCSP responses and CRLs should be discoverable within 10 seconds of enquiry, assuming no non-TrustCor CA networking problems interfere.

Should any party become aware of a severe issue arising from any TrustCor CA certificate, such parties may inform TrustCor CA by mailing `security@trustcor.ca`. This address will generate support tickets and message the Security Incident team. TrustCor CA personnel are directed to respond with urgency to such reports.

4.10.3 Optional Features

OCSP services may, at TrustCor CA's discretion, support SCT embedding.

4.11 End of Subscription

A Subscriber's subscription service ends:

- when all Certificates issued under the same Subscription Agreement are revoked;
- when all Certificates issued under the same Subscription Agreement expire and are not renewed under the same Agreement; or
- when the Subscriber Agreement expires without renewal.

4.12 Key Escrow and Recovery

TrustCor CA does not escrow keys for any party.

Enterprise Subordinate CAs are not permitted to escrow their keys.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable, as no escrow or recovery procedures are allowed.

5 Facility, Management, and Operational Controls

TrustCor CA makes every reasonable effort to protect its certification business from damage, loss, unauthorized access or disruption to its business. The controls which it uses to do so are detailed in this section.

TrustCor CA receives annual reports from its data centers confirming that the policy requirements below are being met.

5.1 Physical Controls

TrustCor CA equipment is located in data centers which are hardened against physical attack and environmental damage.

5.1.1 Site Location and Construction

TrustCor CA's primary and secondary data centers are in Phoenix, Arizona, USA.

The sites are situated in areas away from heavy industry or likely sources of biological, chemical or radiological pollution.

Sites have physically separated areas for visitor reception, clearance to enter the equipment cabinets and the equipment cabinets themselves.

Sites are solidly constructed in such a way as to prevent or inhibit physical attack or environmental hazard (fire, flood, etc.)

5.1.2 Physical Access

All exits and entrances to controlled spaces within the data centers use card entry systems.

All exits and entrances have cameras which record ingress and egress 24x7.

All areas of the data centers are monitored by data center personnel 24x7.

External entrances and exits are patrolled by trained security personnel.

All cabinets housing TrustCor CA equipment are locked, and the keys stored in a separate area of the data center under the supervision of site personnel. Each cabinet is also equipped with cameras front and back, which transmit video to off-site monitoring facilities which can be viewed by TrustCor CA personnel.

5.1.3 Power and Air Conditioning

All data centers have primary and secondary power systems and redundant HVAC systems to ensure consistent temperature and humidity levels.

All data centers have enough fuel to allow continuous powered operation in the event of mains electricity failure, and contracts in place for continuous delivery of generator fuel to allow operations to continue without restoration of mains power.

All cabinets are supplied via filtered UPS power.

5.1.4 Water Exposures

No data center is in a known flood risk area.

HVAC systems are in place to prevent humidity buildup.

All cabinets have sealed roofs to prevent water exposure.

Data centers are equipped with dry pipe sprinkler systems, rather than wet pipe.

All data centers have policies preventing the taking of liquids (e.g. drinks) into the cabinet areas.

5.1.5 Fire Prevention and Protection

Data centers are equipped with automatic fire suppression systems which do not use water to limit fire. Data centers are provided with hand held fire extinguishers suitable for use around electrical equipment, and those extinguishers are inspected regularly to ensure capacity.

Data centers have automated fire alarms linked to emergency service providers to allow rapid response to the outbreak of fire.

5.1.6 Media Storage

Long term media storage is stored in TrustCor CA business premises, and the contents of same encrypted to ensure that only TrustCor CA personnel can access the clear text data.

Media is stored away from known fire/flood hazards.

5.1.7 Waste Disposal

All data centers have secure and safe disposal and destruction facilities for all media types likely to come from the data center, including paper, hard disks, optical disks, etc.

5.1.8 Off-site Backup

Backups are taken daily, with full backups done once a week and incremental ones once a day.

Backup data access is restricted to TrustCor CA personnel. All backups are deemed to be company sensitive materials, meaning that they cannot be stored or transmitted in clear text.

5.2 Procedural Controls

5.2.1 Trusted Roles

TrustCor CA defines the follow roles for operations:

Role Name	Function
Systems Administrator	Deploying or controlling computers hosting TrustCor CA data
CA Administrator	Changing the configuration of profiles or operation of the CA software
Validation Specialist	Issuing, rekeying and revoking end-entity certificates
Auditor	Reviewing log data to ensure compliance with stated policies
Root Operator	Causing the Root CA to sign a certificate request or CRL
Remote Hands	Physically installing, altering or removing TrustCor CA equipment in a data center

At least one person occupying a Highly Trusted role must be a recorded officer of TrustCor Systems S. de R.L.

Role assignments are granted, reviewed and revoked by the TCPA.

5.2.2 Number of Persons Required per Task

Generating, or using private keys stored on an offline HSM partition is an example of a highly trusted operation that requires two people: one to activate the partition and another to perform the signing or generation. Also, transferring CA equipment into data centers requires one person to record the equipment being shipped and one to perform the supervision that the packaged equipment is as recorded.

5.2.3 Identification and Authentication for Each Role

All principals performing CA operations must authenticate themselves using internal Management PKI credentials uniquely identifying the principal and role under which he/she operates.

All Remote Hands operatives must clear their visit to site with the data center beforehand, and submit government approved photo ID to site personnel before performing their task. The maximum duration of visit must also be provided, which is then monitored by site personnel.

5.2.4 Roles Requiring Separation of Duties

Each credential shall bear the unique identity of the person given the role such that his or her logged activities can be easily discovered.

5.3 Personnel controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The TCPA shall evaluate the assignment of any role to a principal such that the body is satisfied that the principal possesses sufficient skill, qualifications and experience to perform the duties of that role without undue risk to TrustCor CA's equipment, operations or reputation.

No person appearing on the OFAC proscribed entities list may be assigned any role within TrustCor CA, and this is checked prior to role assignment.

The TCPA will also evaluate whether the principal being assigned a role has, or could reasonably be seen to have, a conflict of interest which could compromise TrustCor CAs integrity.

5.3.2 Background Check Procedures

All TrustCor CA personnel undergo background checks prior to employment. These checks may include research of previous employment and criminal records.

5.3.3 Training Requirements and Procedures

TrustCor CA shall ensure that, prior to engagement in any trusted role, a person must be trained in:

- Basic PKI knowledge
- Common threats to information verification
- All CA/B Forum policies and guidelines
- TrustCor CA's CP and CPS

Every employee is trained in TrustCor CA's business offerings as well as the basic operations of any CA/RA, and the operations of the CA software, if their duties require such operation. All training is recorded in TrustCor CA's knowledge base, which is part of its workflow software.

5.3.4 Retraining Frequency and Requirements

TrustCor CA monitors the activities of various standards/best practices bodies such as the CA/B Forum relevant to TrustCor CA's area of operations. If it emerges that new duties or requirements are likely to be forthcoming as standards, the relevant personnel will be retrained such that they possess enough knowledge to continue in their roles.

This retraining is recorded as per Section 5.3.3

5.3.5 Job Rotation Frequency and Sequence

TrustCor CA does not mandate job rotation or sequencing for its staff.

5.3.6 Sanctions for Unauthorized Actions

Personnel who are found to have performed unauthorized actions will have their role credentials revoked. These credentials can be re-issued if and when the TCPA deems that any retraining has been completed, such that it makes the risk or role recommencement an acceptable one for TrustCor CA. Should that violation of company policy encompass potential criminal wrongdoing, TrustCor CA will report the matter to the appropriate law enforcement agencies for further investigation and action.

5.3.7 Independent Contractor Requirements

Any independent contractors involved in the CA business are required to meet the requirements of Section 5.3.3 and 5.4.1. They may also receive necessary sanctions as per Section 5.3.6. The sanctions for contractors may extend to termination of contract and possible legal action to recover damages.

5.3.8 Documentation Supplied to Personnel

Personnel are granted access to such relevant training documents and governance documents as their intended roles dictate. This documentation is kept in an online knowledge base, or on the public repository (in the case of the CP and CPS documents).

5.4 Audit Logging Procedures

Auditable events are recorded on either manual or electronic logs, depending on activity. All logged events must include at a minimum:

- The date and time at which the event occurred.
- The name of the system which caused the log event to be generated.
- The identity of the user (or automated principal) which caused the log event to be generated.
- A description of the event such that a human being can read and understand it.

Any TrustCor privacy policies shall further constrain the manner in which events are logged after the date at which that policy becomes effective.

Any Qualified Auditor engaged by TrustCor for external assessment purposes shall have the ability to read any or all of the maintained audit logs by way of proof of TrustCor CA's practices.

5.4.1 Types of Events Recorded

Types of events recorded to the audit log include at a minimum, but are not restricted to, the following:

1. CA Key Life Cycle Management events, such as

- Key generation
- Key backup from a key store to any another device
- Key restoration from a device to an approved key store
- Key storage on an approved key store
- Withdrawal of key from service
- Retiring and archival of keys
- Key destruction

2. Cryptographic Device Life Cycle Management events:

- Commissioning/decommissioning of new hardware
- Erasure of data on a hardware device
- Changes in configuration of new devices
- Updates to firmware on devices
- Transportation of hardware devices
- Access control changes to hardware devices

- Activation and deactivation of a cryptographic hardware device
- Compromise of private key

3. CA/Subscriber Certificate or Time Stamp Token (TST) Life Cycle events

- Certificate/TST request events
  - All requests for a new certificate/TST
  - All requests for renewal of a certificate
  - All requests for the re-keying of a certificate
  - All requests for the revocation of a certificate
- Certificate data verification events
  - The date and times, phone number used, persons spoken to and the results of any verification telephone calls or data associated with the issuance of a certificate.
  - The dates, times and results of all verification activities stipulated in TrustCor CA's Certification Practice Statement.
- Results of certificate/TST requests
  - The successful validation of a certificate/TST request
  - The reason for the rejection of a certificate/TST request
- Certificate/TST issuance
  - The issuance of both CT pre-certificates and final certificates
  - The results of submission to CT logs of any pre-certificates and final certificates
  - Signing of data using a key stored on a hardware device
- Certificate status generation
  - The generation of CRLs for each of the CAs being managed
  - The signing of OCSP responses
  - The publication results for the above CRLs and OCSP responses (where applicable)

4. Generalized Security Events

- PKI system access attempts
  - All authentication and authorization results (successful or not) for access to any system involved in the processing or handling of PKI data
  - All lockout/clearances caused by system access protection logic
- PKI/Security system events
  - Deployment of new systems to handle PKI data

  - Decommissioning of systems which used to handle PKI data
  - Backup of PKI systems
  - Restoration of PKI systems
  - Alteration of configuration of any software involved in the processing of PKI data
  - Detection of alteration of known sensitive files, including system binaries or configuration files
  - All software packages/patches (with version numbers and identified source) installed or removed from the systems
  - System clock correction events
  - Alteration of the control profiles for the system configuration management subsystems
  - Alteration of logged information for any subsystem

- Security profile changes
  - Addition of new authorized users/principals to a host
  - Removal of authorized users/principals from a host
  - Alteration of privileges associated with a user or principal
  - Alteration of privilege groups within any host or application involved in the processing of PKI data

- System availability events
  - System crashes (both operating system level and application)
  - Systems becoming non-responsive
  - Systems being restarted
  - Anomalous results emanating from possible hardware faults

- Firewall and router activities
- CA facility access
  - Entries to the facility where CA hardware is maintained
  - Exits to the facility where CA hardware is contained
  - Access to CA components

5.4.2 Frequency for Processing and Archiving Audit Logs

All audit logs are reviewed at least quarterly to inform future security and operational policies.

These periods reflect the normal log review process: events which trigger security incidents have much shorter processing times as detailed in Section 5.7.

5.4.3 Retention Period for Audit Log

Audit logs are maintained onsite until review is complete. All Audit logs (as specified in Section 5.4.1) are retained for at least two (2) years. In the event of audit log information pertaining to certificates, that log retention period starts from the expiration date of the certificate.

Audit logs are supplied to the Qualified Auditor engaged by the company.

5.4.4 Protection of Audit Log

Log permissions on systems are set to restrict read-only access to authorized personnel; similarly, archival of log data is restricted to authorized personnel.

All system which generate audit log data host intruder detection software which alerts on log shrinkage or unexpected alteration.

Logs stored offsite reside in facilities which have protections at least equivalent to the TrustCor CA originating systems. Offsite logs are digitally signed to make tampering of the logs evident. Offsite logs are verified periodically to ensure that their integrity has been maintained.

5.4.5 Audit Log Backup Procedures

Multi-site audit log backup happens every day. Logs are encrypted both in transit to their destination and at rest. Logs may not be rotated off their originating systems until log review is complete.

5.4.6 Audit Collection System (internal vs. external)

Systems are configured to begin their audit logging at startup, running continuously until system shutdown.

All automated audit logs send their results to a central logging service for collation and review.

If that central logging service is no longer receiving logs from a CA system, that CA system becomes suspect. The TCPA shall determine whether CA operations shall be suspended, depending on the severity of the outage of the system which has failed to log.

5.4.7 Notification to Event-Causing Subject

TrustCor CA is not required to notify subjects that they have caused auditable events in TrustCor's logging systems, though it may choose to do so.

5.4.8 Vulnerability Assessments

At least once a year, TrustCor CA conducts a threat assessment review which collates the potential threats (both internal and external) to the confidentiality, integrity or availability to the systems and data operated by TrustCor CA.

Each threat is assessed with a view to: * how harmful would the threat be to the company and the public should the threat materialize * how difficult it is to translate the threat to an active exploit * what mitigations are in place to counteract the efficacy of the threat.

For each identified risk above, an entry is made in the internal risk assessment document, which is reviewed by an internal audit process to either accept the risk as being sufficiently well mitigated, or whether changes are required to the policies, procedures, security postures or other security arrangements in order to constrain risk to acceptable levels.

5.5 Records Archival

5.5.1 Types of Records Archived

The following data forms part of the records archived:

- All logs generated in the audit log section (5.4)
- All records related to the commissioning and decommissioning of computer or network equipment
- The engagement and disengagement of all personnel having contractual employment with TrustCor CA
- All policies (security, operational, certificate, etc.) controlling TrustCor CA's operations
- All Subscriber Agreements adopted by TrustCor CA
- The records of certificate validation, issuance and revocation
- Reports of auditors generated for compliance purposes
- All security incident reports and their resolutions (this includes detected policy violations of CP/CPS documents)

5.5.2 Retention Period for Archive

TrustCor CA retains archived audit logs (as specified in Section 5.5.1), including but not limited to all documentation relating to certificates, in accordance with its CP and Baseline Requirements for at least two (2) years from their record creation timestamp, or at least two (2) years after the expiration of the Certificate based on that documentation, whichever is longer.

5.5.3 Protection of Archive

Archive records are stored in secure, off-site locations. Access to those records is restricted to authorized personnel.

Logging data on systems which feed the archive is configured not to be mutable by anyone except system administrators. Since log data is also monitored for unexpected shrinkage (corresponding to the unauthorized removal of audit data), TrustCor CA asserts that this protects the integrity of the archive data and process.

5.5.4 Archive Backup Procedures

System administrators operate (either by scheduled operation or manual) the backup process using software approved for such purposes by the TCPA.

A default backup process is configured to take a full dump of archive data every seven days, and transfer that data automatically to a data repository. Every day, an incremental backup is scheduled.

Backups are signed and encrypted using keys which the system administrators keep secure. Backup files are transferred to their target locations using protocols which are cryptographically authenticated and protected.

5.5.5 Requirements for Time-stamping of Records

Every system which archives records is required to run NTP in order to synchronize its clocks to a well known accurate time source.

All logs collected, whether email, or system log must carry a timestamp.

System logs and application logs are configured to use UTC on their timestamps, to allow easy ordering of time sequence data.

Physical site visit logs must also record time of entry and exit to the controlled facility. Such logs are maintained by the data center itself.

5.5.6 Archive Collection System (internal or external)

All archives of data which are generated by TrustCor CA systems or software are collected internally to form its primary archive.

5.5.7 Procedures to Obtain and Verify Archive Information

Electronic archive data is cryptographically signed, so its integrity can be validated (although not necessarily read) by anyone possessing the signing public key, which is made available to TrustCor CA personnel.

At its discretion, TrustCor CA may allow Subscribers to access a copy of their archived information. It may also charge fees to offset costs of this archive recovery process.

Plaintext backup data is only made available to TrustCor CA personnel with a business need to see that data (including auditors). It is not disclosed to any other party, except where a properly formed instrument has been presented, issued by legally competent authority.

5.6 Key Changeover

As any CA certificate owned by TrustCor CA approaches the end of its life shall have new keys generated and a new certificate issued in its place. From the moment of the replacement being published, all new certificate requests which would have been signed by the old private key will be signed by the new key.

The old certificate is still published on the online repository until the expiry of the last certificate issued under it. CRLs will still be generated under the old certificate until the expiry of the last certificate issued under it.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

All TrustCor CA high security devices must be equipped with intruder detection system which watches for such anomalies as might indicate compromise of the system.

In the event of an apparent security incident, a security incident ticket is created in the ITIL workflow software and passed onto the security team to investigate. The security team will triage the incident report, and will act to:

- withdraw from service any component which might compromise the integrity of TrustCor CA operations
- assign appropriate resources to identification, mitigation and resolution of the incident
- before bringing a remediated component back into service, a person in the System Administrator role shall record in the security incident report that the incident is believed resolved and that operations using that component can continue.

5.7.2 Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

TrustCor CA hosts are built and maintained by a consistent configuration management process. If such systems are corrupted (by accident rather than malice), the configuration management system is used to restore the system binaries, libraries and configurations to a known state.

System administrators shall restore files not managed by the configuration management software via backup snapshots.

If there is reason to believe that certificates have been issued during such time as the integrity of the software and processes might have been compromised, TrustCor CA may choose to revoke such certificates, and notify the Subscribers of this action and the reasons for doing so. TrustCor CA will credit Subscribers such that new certificates may be issued in place of the revoked certificates.

5.7.3 Recovery Procedures After Key Compromise

Any CA keys held by TrustCor CA are deemed to be of critical importance. In the event of compromise actions may include but is not limited to:

- Revocation of the affected key pair
- Revocation of all active certificates issued under that key pair
- Deployment of a new CA program
- Notification to all Subscribers and Relying Parties
- Generation of new certificates for all affected Subscribers

5.7.4 Business Continuity Capabilities after a Disaster

TrustCor CA operates in (at least) two distinct geographies, so that services can be operated in the event of loss of a host providing that service.

HSMs operate in a paired configuration, meaning that CA signing operations can continue in the event of hardware failure.

As described above in Sections 5.1 and 5.2, sufficient data center capability exists to minimize the risk of outage of TrustCor CA services.

A certain amount of outage, detailed in Section 2.1 is allowed, for emergency maintenance or unplanned unavailability of services. Such minor outage should be published by TrustCor CA once it is resolved.

However, should major outage happen - such that the Section 2.1 guarantees cannot be met - TrustCor CA shall publish an ongoing record of what the outage is, what is being done to rectify it, and what the likely time of restoration shall be.

The priority for reestablishment of function is the certificate status services (OCSP/CRLs) and the time stamping (TSA) function.

If there is any reason to believe that the outage has resulted in the loss of integrity of the CA's assets (including private keys), TrustCor CA shall immediately inform the CA/B Forum of this, as well as the operators of the browser root certificate programs to which TrustCor CA belongs. Restoration of services will not be permitted unless the TCPA can be assured of the integrity of the CA function.

5.8 CA or RA Termination

Should TrustCor CA be about to cease operations, it shall make the best efforts to provide timely communication of this state of affairs to all affected parties including but not limited to:

- The operators of the browser root certificate programs
- The CA/B Forum
- Relying Parties
- Subscribers to current certificates

This communication of cessation of operations will explain that current certificates will not remain valid after cessation of operations. The last act of the CA shall be the revocation of its existing certificate base and the publication of those CRLs.

If a successor CA is found which can adopt all of TrustCor CA's responsibilities under its governing documentation, notification to the above shall also be provided explaining this succession. In such a case, the mass revocation may not be warranted.

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 All CA key pairs for TrustCor CA are generated and stored on FIPS 140-L3 or EAL 4+ (or higher) rated Hardware Signing Modules (HSM).

For Root level CAs, a commissioning script must be made and archived, showing the personnel involved in the Root Certificate generation as well as the validation of the script. All participants must physically sign that script and it forms part of TrustCor CAs foundational documents.

6.1.1.2 RA Key Pair Generation Not applicable.

6.1.1.3 Subscriber Key Pair Generation TrustCor CA does not perform key generation on behalf of Subscribers - such key generation and storage is entirely the responsibility of the Subscriber.

Certificate requests are presented to TrustCor CA as PKCS#10 documents.

6.1.2 Private Key Delivery to Subscriber

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

Subscribers must deliver their public keys (as PKCS#10 documents) over HTTPS or encrypted (and possibly signed) S/MIME email.

6.1.4 CA Public Key Delivery to Relying Parties

TrustCor CA publishes all CA certificates on its online repository.

The browser root certificate programs of which TrustCor CA is a member will also publish the root certificates for TrustCor CA.

6.1.5 Key Sizes

The minimum key size allowed for RSA keys in any business offering is 2048 bits. After Jan 1, 2021, the minimum size of RSA key allowed within a Code Signing certificate is 4096 bits.

DSA keys are not used anywhere in TrustCor CA's certification operations.

The minimum key size for any ECC key is 256 bits. ECC keys are not accepted for Enterprise Subordinate CAs. ECC keys must use either the P-256 or P-384 curves.

The minimum digest size used is 256 bits. All digests used are from the SHA-2 family. The digest minimum applies to signatures on signatures on certificates, OCSP responses and CRLs.

6.1.6 Public Key Parameters Generation and Quality Checking

TrustCor CA generates its CA private and public keys from inside a FIPS 140-L3 or EAL 4+ (or higher) HSM.

Weak keys are checked for (and rejected if found) prior to further processing. In particular, RSA public key exponents must be an odd integer greater than or equal to 3.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

CA certificates contain the keyUsage identifiers cRLSign and keyCertSign as well as digitalSignature (in case TrustCor CA wishes to use directly signed OCSP, which it currently does not).

OCSP responses may be signed by separate OCSP agents, if not by the CA key directly. As such, OCSP certificates have a digitalSignature key Usage, and extendedKeyUsage set to id-kp-OCSPSigning. As required, they also embed the id-pkix-ocsp-nocheck OID, but not as a KU/EKU value)

See Section 7.1.2 for further details regarding end entity keyUsage and extendedKeyUsage values.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

For Subscriber keys, TrustCor CA requires that the private key holder uses reasonable steps to protect the key, such as restrictive permissions and possibly key encryption using a strong passphrase.

6.2.1 Cryptographic Module Standards and Controls

For all CA keys storage, HSMs rated at FIPS 140-L3, or at least EAL4+ are used.

For Basic grade keys, no controls are placed upon the user (other than those behavioral ones above).

For Enhanced grade keys, keys should be generated and stored according to FIPS 140 Level 1 requirements, whether in hardware or software.

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

For recovery of keys which are used to encrypt backups and logs, the private key components are split into multiple shares via the Shamir secret sharing scheme, and must be brought together to recover the key. The shares are distributed securely to TCPA approved personnel, with the requirement that no one person can have enough shares to recover a key.

Changes to HSM security policies must be performed by at least two persons using separate hardware keys.

6.2.3 Private Key Escrow

Not applicable. TrustCor CA does not escrow its keys, nor permit subordinate CAs to do so.

6.2.4 Private Key Backup

CA keys are backed up to a specific HSM backup hardware, issued by the same vendor which makes the main HSM.

Subscriber keys are not available to TrustCor CA, and are thus not backed up.

6.2.5 Private Key Archival

TrustCor CA does not archive its private keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Private keys are transferred between HSMs according to manufacturers specifications, and only leave the originating device in encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

Private keys are generated and stored in partitions on TrustCor CA's HSMs. All HSMs are rated to FIPS 140-L3 or EAL4+ (or greater levels of assurance of those standards).

6.2.8 Activating Private Keys

Private keys are activated by bringing the partition which contains them online. This requires authentication to the HSM itself and use of trusted remote device.

A partition (and its keys) stays active until explicitly deactivated.

Partitions containing Root CA keys may not be held active for unattended operations. Activation data is required to be entered via trusted devices for each use of the Root CA key (e.g. signing subordinate CA CSR or issuance of CRLs).

6.2.9 Deactivating Private Keys

Private keys are deactivated by deactivating their containing partition. Any system administrator is permitted to take a partition offline.

Individual hosts may have their rights to use a partition (and thus the keys within such partitions) removed. Any system administrator can do this by deregistering host key information on the HSM.

6.2.10 Destroying Private Keys

Keys are securely destroyed using the HSMs manufacturer's instructions.

6.2.11 Cryptographic Module Rating

See Section 6.2.1 of this document.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

See Section 5.5 of this document regarding archival of public keys (embedded in certificates).

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

TrustCor CA certificates have a maximum validity period of:

Certificate Type	Maximum Validity Period
Root CA	15 years
Subordinate CA	15 years

End entity certificates have the following certificate validity periods:

Certificate Type	Maximum Validity Period
DV SSL	398 days
OV SSL	398 days
Email	825 days
Time Stamping Authority	3655 days
Document Signing	3655 days
Code Signing	1128 days

OCSP responder certificates have a maximum validity period of 825 days.

Note that the maximum validity of a Timestamp Certificate's associated Private Key is 450 days, or 15 months, whichever is the shorter period of time.

TrustCor CA may retire any key and certificate in its control prior to the expiry date for rollover purposes.

TrustCor CA does not issue certificates with a notAfter date which exceeds the Issuer CA certificate's notAfter date.

6.4 Activation Data

Activation data in this section refers to the process by which partitions containing HSM keys may be used by authorized parties (usually the CA signing software for CRL generation and certificate issuance).

6.4.1 Activation Data Generation and Installation

HSM Activation data is generated according to the specifications of the HSM manufacturer. Devices which are used to enter activation data are initialized when the HSM is installed in the data center.

Registration information regarding which hosts may communicate with which HSM partitions are securely copied and encrypted in transit according to the specifications of the HSM manufacturer.

6.4.2 Activation Data Protection

Activation data is protected via FIPS 140 Level 2 devices and may only be used via registered data entry devices. Repeated attempts to wrongly enter PIN data will cause the activation devices to lock out, and new device issuance to be required.

6.4.3 Other Aspects of Activation Data

TrustCor CA describes, in its security policy, all aspects of activation policy, roles and assignments.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

TrustCor CA software runs on software that is designated high sensitivity, according to TrustCor CA's security policy.

The validation server (containing OCSP responders and hosting CRLs internally) is a medium sensitivity host.

The publicly facing website which contains a proxy web server to the CRL repository and OCSP responders is deemed normal sensitivity (it contains no private key or sensitive information).

High sensitivity hosts are administered under the security policy which means at least:

- all shell accounts on the host must use 2 factor authentication (public key and OTP code) to access it
- accounts failing 5 attempts at access are locked out for at least 10 minutes
- HIDS software is running on the host, watching for known compromises, and unexpected file variations.

Medium sensitivity hosts must exhibit at least the following controls:

- accounts failing 5 attempts at access are locked out for at least 10 minutes
- HIDS software is running on the host, watching for known compromises, and unexpected file variations.

Normal sensitivity hosts are controlled using:

- HIDS software is running on the host, watching for known compromises, and unexpected file variations.

In all cases, system security logs still generate security incident reports which are filed in TrustCor CA's SIEM system.

6.5.2 Computer Security Rating

TrustCor CA is not required to have its computer systems formally rated to any particular standard.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

All software coming from external vendors must be either in a package form which is signed by a key known to be under that vendor's control; or have a binary distribution which has a SHA-512 integrity code known to TrustCor CA's development team and recorded in the configuration management database. Direct deployment of software to any host inside TrustCor CA is not allowed, and is detected via HIDS monitoring.

Software developed in house is peer reviewed, and may only be commissioned from developers having signed contracts with TrustCor CA.

All changes to the production environment must be as the result of ITIL workflows which have been signed off by the TrustCor CA Change Management function. Such approval is not granted unless the change has been developed, tested and deployed on TrustCor CA's parallel test infrastructure.

Systems are not deployed by hand, but deployed via the configuration management software, which ensures that the system profile is consistent with a declared configuration. The same management software is used to revert any local changes on a host.

All systems are required to run software which continually scans for alteration of executable software which is not performed through the normal configuration and package management processes. This includes anti-virus scanning for systems which are at risk of such malware.

6.6.2 Security Management Controls

Intruder detection systems and rootkit detection systems are deployed on all TrustCor CA systems.

Changes to the database which controls system configuration itself is logged under a source code control system, such that changes can be identified and reverted if need be.

6.6.3 Life Cycle Security Controls

TrustCor CA is not required to follow any particular methodology in the development of its software.

6.7 Network Security Controls

Changes to DNS, IP namespacing, routing and network fabric configuration are stored in the same configuration management software as for host deployment. The same change controls are in place to ensure auditability of changes.

All network connectivity for each host flows through firewalls controlled by TrustCor CA. Direct public facing network connectivity is prohibited.

All IP ports open on high risk systems are controlled by whitelisting the addresses which may access them. Those addresses reside in the TrustCor CA controlled network space.

6.8 Time-Stamping

All hosts run NTP to synchronize their clocks to reliable time providers.

Any changes to TrustCor CA's Timestamp signing process are an auditable event.

Clock adjustments of one second or greater are auditable events.

TrustCor CA's TSA ensures that clock synchronization is maintained when a leap second occurs.

The TSA facility operated by TrustCor CA uses a time source synchronized to a GPS receiver and three unauthenticated NTP sources at Stratum 3 or better. If any source falls below Stratum 3, this is an auditable event, and another source will be used.

TrustCor CA's TSA facility operates according to the protocol specified in RFC 3161.

TST Requesters are required to inform TrustCor CA as soon as possible if any of the information in the TST cannot be verified.

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

TrustCor CA issues certificates compliant with the Baseline Requirements, ITU X.509 standard, as well as RFC 5280. TrustCor CA meets the technical requirements set forth in Sections 2.2, 6.1.5 and 6.1.6 of this CPS.

TrustCor CA certificate serial numbers are randomly generated, and incorporate a **minimum** of 64 random value bits. The randomness comes from algorithms designed for cryptographic purposes. TrustCor CA's software will not permit a value of zero to be used as a serial number, even if so generated.

7.1.1 Version Number(s)

TrustCor CA certificates are X.509v3 certificates.

7.1.2 Certificate Content and Extensions; Application of RFC 5280

The extensions covering the various types of certificate are described below.

7.1.2.1 Root CA Certificate

- The basicConstraints extension does appear as a critical extension. The cA field is set true. The pathLenConstraint field is not be present.
- The keyUsage extension is present and marked critical. Bit positions for keyCertSign and cRLSign are set. The digitalSignature bit is set.
- Root CA certificates do not contain any certificatePolicies or extendedKeyUsage extension.

7.1.2.2 Subordinate CA Certificate

- The certificatePolicies extension is present and not marked critical.
- The following certificatePolicies fields are present:
  - certificatePolicies:policyIdentifier – OID of the Certificate Policy adhering to and compliant with the Baseline Requirements
  - certificatePolicies:policyQualifiers:policyQualifierId – id-qt-cps
  - certificatePolicies:policyQualifiers:qualifier:cPSuri – HTTP URI for the Certification Practice Statement
- The cRLDistributionPoints extension is present and not marked critical. It contains the HTTP URI of TrustCor CA's CRL service.
- The authorityInformationAccess extension is present and not marked critical. It contains the HTTP URI of TrustCor CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2) and the HTTP URI of TrustCor CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).
- The basicConstraints extension is present and marked critical. The cA field is set true. The pathLenConstraint field is not present.
- The keyUsage extension is present and marked critical. Bit positions for keyCertSign, cRLSign and digitalSignature are set.
- If present, the nameConstraints extension may be marked critical.
- The extKeyUsage extension is present and marked critical. Subordinate CA certificates created after January 1, 2019 contain an EKU extension; they do not include the anyExtendedKeyUsage KeyPurposeId.

  For Subordinate CA certificates which contain the extendedKeyUsage, they must be a non-strict superset of all the values of any certificate (Subordinate CA or end-entity certificate) issued under them. That is, no end-entity certificate can contain an extendedKeyUsage value, unless that value appears in all of the extendedKeyUsage values of its superior CA certificates, if those CA certificate contain such an extension. No Subordinate CA Certificates that are not used to issue TLS certificates, contain the id-kp-serverAuth [RFC5280] value. No multiple independent key purposes are combined in any Subordinate CA Certificates.
- The authorityKeyIdentifier extension is present and not marked critical. It contains a keyIdentifier field and it does not contain a authorityCertIssuer or authorityCertSerialNumber field.

7.1.2.3 Subscriber Certificate

- The certificatePolicies extension is present and not marked critical.
- The following certificatePolicies fields are present:
  - certificatePolicies:policyIdentifier – OID of the Certificate Policy adhering to and compliant with the Baseline Requirements
  - certificatePolicies:policyQualifiers:policyQualifierId – id-qt-cps
  - certificatePolicies:policyQualifiers:qualifier:cPSuri – HTTP URI for the Certification Practice Statement
- The cRLDistributionPoints extension is present and not marked critical. It contains the HTTP URI of TrustCor CA's CRL service.
- The authorityInformationAccess extension is present and not marked critical. It contains the HTTP URI of TrustCor CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2) and the HTTP URI of TrustCor CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).
- The basicConstraints extension is present and not marked critical. The cA fields are not set to true.
- The keyUsage extension may be present and marked critical. When present, bit positions for keyCertSign and cRLSign are not set.
- The extKeyUsage extension is present and not marked critical. Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values must be present. id-kp-emailProtection [RFC5280] MAY be present. The value anyExtendedKeyUsage is not present.
- The authorityKeyIdentifier extension is present and not marked critical. It contains a keyIdentifier field and it does not contain a authorityCertIssuer or authorityCertSerialNumber field.

7.1.2.4 All Certificates All end-entity certificates must contain the extendedKeyUsage extension. No certificate contains the anyExtendedKeyUsage value in its extendedKeyUsage section.

7.1.2.5 Application of RFC 5280 Any Precertificate generated by TrustCor CA is not considered to be a "certificate" subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile under this CPS.

7.1.3 Algorithm Object Identifiers

All signing algorithms are either sha256WithRSAEncryption or sha512WithRSAEncryption.

TrustCor CA does not, and never has, used SHA-1 as a component of any signature algorithm on a certificate.

7.1.3.1 SubjectPublicKeyInfo The following requirements apply to the subjectPublicKeyInfo field within a Certificate or Precertificate. No other encodings are permitted.

7.1.3.1.1 RSA TrustCor CA certificates contain an Algorithm of rsaEncryption (OID: 1.2.840.113549.1.1.1) with parameters set to NULL.

7.1.3.2 Signature AlgorithmIdentifier All objects signed by a TrustCor CA Private Key conform to Baseline Requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier derived type in the context of signatures.

7.1.3.2.1 RSA TrustCor CA uses the following signature algorithms and encodings:

- RSASSA-PKCS1-v1_5 with SHA-256: Encoding: 300d06092a864886f70d01010b0500.
- RSASSA-PKCS1-v1_5 with SHA-512: Encoding: 300d06092a864886f70d01010d0500.

7.1.4 Name Forms

Each certificate contains a serial number, unique within the scope of its issuing CA.

All CA certificates have a commonName attribute within their subject DNs which is meaningful to the purpose of the CA, and is not a generic name. All CA certificates operated by TrustCor have the organization attribute set to `TrustCor Systems S. de R.L.` and the countryName attribute set to `PA`.

For Subordinate CA certificates issued after January 1, 2020, no attributes are allowed in the subject DN other than commonName, organization or countryName.

For all certificates, the contents of the Issuer DN field shall, octet for octet, match the subject DN value of its issuing CA certificate. This will comply with the name chaining rules of RFC 5280, section 4.1.2.4.

7.1.4.1 Name Encoding The Issuer Distinguished Name shall in all cases match the Subject Distinguished Name present within the issuing certificate.

7.1.4.2 Subject Information - Subscriber Certificates No field within the subject of an end-entity certificate may be present unless it has been validated to be true by TrustCor CA.

No certificate subject can contain metadata such as '.', '-' and ' ' characters, and/or any other indication that the value/field is absent, incomplete, or not applicable.

7.1.4.2.1 Subject Alternative Name Extension

a. **Certificate Field:** extensions:subjectAltName

   Required/Optional: Required for SSL

   Contents for SSL Server Certificates: This extension must contain at least one entry. Each entry must be a dNSName containing the Fully-Qualified Domain Name or Wildcard Domain Name. Underscore characters ("_") are not permitted in dNSName entries. TrustCor CA will validate the dNSName in accordance with sections 3.2.2.4 and 3.2.2.6 of this CPS.

   The Fully-Qualified Domain Name or the FQDN portion of the Wildcard Domain Name contained in the entry will be composed entirely of LDH Labels joined together by a U+002E FULL STOP (".") character and consist solely of Domain Labels that are P-Labels or Non-Reserved LDH Labels.

7.1.4.2.2 Subject Distinguished Name Fields

a. **Certificate Field:** subject:commonName (OID 2.5.4.3)

   When present, the value is a value contained in the Certificate's subjectAltName extension. This value is a Fully-Qualified Domain Name or Wildcard Domain Name and is encoded as a character-for-character copy of the dNSName entry value from the subjectAltName extension. All Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name are encoded as LDH Labels, and P-Labels which are never converted.

b. **Certificate Field:** subject:organizationName (OID 2.5.4.10)

   TrustCor CA requires this field for OV SSL.

   When provided, this field must contain either the official name of the organization or the DBA name as verified in Section 3.2.2.2. TrustCor CA may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that such variations are documented and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", "Company Name Inc." or "Company Name" may be used. Because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly

supported by application software, TrustCor CA may use the subject:organizationName field to convey a natural person Subject's name or DBA.

TrustCor CA does not issue DV SSL certificates that contain this certificate field.

c. **Certificate Field:** subject:givenName (2.5.4.42) and subject:surname (2.5.4.4)

TrustCor CA does not issue certificates that contain this certificate field.

d. **Certificate Field:** Number and street: subject:streetAddress (OID: 2.5.4.9)

TrustCor CA does not issue certificates that contain this certificate field.

e. **Certificate Field:** subject:localityName (OID: 2.5.4.7)

TrustCor CA requires this field for OV SSL when subject:organizationName field contains verified information and the subject:stateOrProvinceName field is not provided.

This field is optional for OV SSL when subject:organizationName field and subject:stateOrProvinceName field contains verified information.

When provided, this field must be the locality of the organization as it appears in the documents used to verify that organization. Verification of this field is completed as specified in this CPS in section 3.2.2.1. Note that while locality or state/province must be present, a certificate need not include both attributes and values.

TrustCor CA does not issue DV SSL certificates that contain this certificate field.

f. **Certificate Field:** subject:stateOrProvinceName (OID: 2.5.4.8)

TrustCor CA requires this field for OV SSL when subject:organizationName field contains verified information and the subject:localityName field is not provided.

This field is optional for OV SSL when subject:organizationName field and subject:localityName field contains verified information.

When provided, this field must be the state or province of the organization as it appears in the documents used to verify that organization. Verification of this field is completed as specified in this CPS in section 3.2.2.1. Note that while locality or state/province must be present, a certificate need not include both attributes and values.

TrustCor CA does not issue DV SSL certificates that contain this certificate field.

g. **Certificate Field:** subject:postalCode (OID: 2.5.4.17)

TrustCor CA does not issue certificates that contain this certificate field.

h. **Certificate Field:** subject:countryName (OID: 2.5.4.6)

TrustCor CA requires this field for OV SSL when the subject:organizationName field is present. Contents: If the subject:organizationName field is present, the subject:countryName will always contain the two-letter ISO 3166-1 country code associated with the location of the Subject verified under Section 3.2.2.1.

TrustCor CA will not issue an OV SSL Certificate if a Country is not represented by an official ISO 3166-1 country code.

TrustCor CA does not issue DV SSL certificates that contain this certificate field.

i. **Certificate Field:** subject:organizationalUnitName (OID: 2.5.4.11)

TrustCor CA does not issue certificates that contain this certificate field.

j. Other Subject Attributes

Other attributes MAY be present within the subject field. If present, other attributes will contain information that has been verified by TrustCor CA.

7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates

By issuing a Subordinate CA Certificate, TrustCor CA followed the procedures set forth in this Certification Practice Statement and Certificate Policy to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.4.3.1 Subject Distinguished Name Field

For Root Certificates issued after January 1, 2021, the format of all Subject DNs shall be:

- subject:commonName (OID: 2.5.4.3): Unique Name of Root CA
- subject:organizationName (OID: 2.5.4.10): TrustCor Systems S. de R.L.
- subject:countryName (OID: 2.5.4.6): PA

For Subordinate Certificates issued after January 1, 2020, the format of all Subject DNs shall be:

- subject:commonName (OID: 2.5.4.3): Unique Name of Subordinate CA
- subject:organizationName (OID: 2.5.4.10): TrustCor Systems S. de R.L.
- subject:countryName (OID: 2.5.4.6): PA

7.1.5 Name constraints

Name constraints are only present in Enterprise Subordinate CA certificates, and are described in Section 7.1.2.2.

7.1.6 Certificate Policy Object Identifier

The Certificates issued by TrustCor CA containing specified policy identifier(s) are managed in accordance with Baseline Requirements. TrustCor CA Subscriber Certificates contain, within the Certificate's certificatePolicies extension, one or more policy identifier(s) that are specified beneath the CA/Browser Forum's reserved policy OID arc. The OIDs used by TrustCor CA in its end-entity certificates and time stamp tokens are as follows:

Certificate/TST type	OID
DV SSL certificates	2.23.140.1.2.1
OV SSL certificates	2.23.140.1.2.2
Object Signing	2.23.140.1.4.1
OV Object Signing	2.23.140.1.4.1
OV Email certificates	2.23.140.1.2.2
TSA tokens	1.3.6.1.4.1.44031.5.{1,2}

Any certificate bearing the Object Signing policy identifier denotes that it is managed in accordance with the MRCS.

TrustCor CA's Root CA Certificates do not contain any certificatePolicies extension.

TrustCor CA Subordinate CA certificates do not contain Certificate Policy Identifiers.

7.1.7 Usage of Policy Constraints Extension

No certificate contains a policy constraints extension.

7.1.8 Policy Qualifiers Syntax and Semantics

TrustCor CA does not currently add explicit text into the policy extensions of its certificate.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Processing semantics for the critical Certificate Policies extension shall be done in accordance with the X.509 certification path processing rules.

7.2 CRL Profile

7.2.1 Version Number(s)

CRLs are issued as version 2 CRLs, as defined in RFC 5280.

7.2.2 CRL and CRL Entry Extensions

The CRL number is a monotonically increasing integer.

The Authority Key Identifier matches that in the signing certificate.

The Invalidity date is given as a UTC date.

7.3 OCSP Profile

TrustCor CA operates an Online Certificate Status Profile (OCSP) responder in compliance with RFC 5019 and RFC 6960 and highlights this via an OCSP responder URL.

7.3.1 Version Number(s)

The OCSP responder conforms to the specifications of RFC 6960, and uses v1 as its version number.

7.3.2 OCSP Extensions

TrustCor CA OCSP will not honor nonce extensions, but will accept them. TrustCor CA may use the Extended Revoked Definition of RFC 6960, 4.4.8 to denote non-issued certificates, or may return an `unauthorized` error should a request be entered for a non-existent certificate.

TrustCor CA OCSP will issue errors if the requests come with critical extensions which are not understood by the responder. The OCSP responders are not guaranteed to honour any extensions in the OCSP request.

TrustCor CA OCSP may opt to use certificate SCTs as an extension to the OCSP response. Such extensions will not be marked as critical.

8 Compliance Audit and Other Assessments

This document is designed to meet the standards required of the Baseline Requirements as well as Webtrust's "Principles and Criteria for Certification Authorities" (WebTrust for CAs).

8.1 Frequency or Circumstances of Assessment

TrustCor CA is audited according the requirements above at least once per year. TrustCor CA may elect to begin its audit assessment earlier at its discretion.

8.2 Identity/Qualifications of Assessor

The audit of TrustCor CA is performed by a Qualified Auditor selected from the list of WebTrust's licensed practitioners, and possesses the following qualifications and skills:

- Independence from the subject of the audit;
- Ability to conduct an audit that addresses the criteria of the audit schemes specified in section 8.4;
- Employs individuals who have proficiency in examining PKI technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
- Licensed by WebTrust;
- Bound by law, government regulation, or professional code of ethics; and
- Maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

TrustCor CA has selected an auditor/assessor who is completely independent from TrustCor Systems S. de R.L. or any of its affiliated companies. The auditor selected will not have any interest which would cause a bias in any direction regarding audit findings.

8.4 Topics Covered by Assessment

The audit will test compliance of TrustCor CA against the policies and procedures set forth, as applicable in:

- This Certificate Practice Statement;

- TrustCor CA Certificate Policy;
- The latest required version of WebTrust for Certification Authorities;
- The latest required version of WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security;
- The latest required version of WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements

8.5 Actions Taken as a Result of Deficiency

In the event of deficiencies being discovered, this must be reported to the TCPA as soon as is reasonably practical. The TCPA directs the appropriate personnel to devise a plan to remediate the deficiencies.

Once the plan has been implemented, TrustCor CA will call for an auxiliary audit to verify that the noted deficiencies have been remediated.

TrustCor CA may revoke certificates if the deficiencies were such that the issuance process is likely to have been faulty.

If the deficiency is deemed so serious, or the time to remediate so long as to call into question the integrity of certificates issued, TrustCor CA will inform the relevant browser root certificate program managers that a serious deficiency in practice has been uncovered, and that they should take such steps as to mitigate the risk to their program's integrity.

8.6 Communication of Results

The results of all compliance audits will be communicated to the TCPA and to any third party entities which are entitled by law or regulation to receive a copy of the audit results.

The results of the most recent compliance audit will be posted within three months from the end of the audit period to the Repository and linked via the relevant WebTrust seal on TrustCor's main website.

In the event of a delay greater than three months, and if so requested by an Application Software Supplier, TrustCor CA will provide an explanatory letter signed by the Qualified Auditor.

8.7 Self-Audits

TrustCor CA monitors adherence to the Certificate Policy, This Certificate Practice Statement, and the Baseline Requirements and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one Certificate

or at least three percent of the Certificates issued during the period commencing immediately after the previous self-audit sample was taken.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

TrustCor CA charges fees for certificate issuance and renewal. All fees and any associated terms and conditions are made clear to the Applicant during the application process. Such fees are subject to change at any time, in accordance with the applicable customer agreement, and any such changes shall become effective immediately after posting in such web sites.

9.1.2 Certificate Access Fees

TrustCor CA may charge a reasonable fee for access to its certificate databases.

9.1.3 Revocation or Status Information Access Fees

TrustCor CA does not charge a fee for certificate revocation or a fee for a Relying Party to check the validity status of an issued Certificate using CRLs or OCSP.

TrustCor CA may charge added fees for providing customized CRLs, OCSP services, or other value-added revocation and status information services outside the scope of a normal request.

9.1.4 Fees for Other Services

TrustCor CA may elect to charge fees for its other services. Such fees will be outlined in the applicable customer agreement.

9.1.5 Refund Policy

All payments for certificates or services provided in respect to certificates are non-refundable, except in the case where a formal written refund policy states otherwise, if any, applies. A refund will not be issued if the Subscriber has used the Certificate, or if 30 days have exceeded past the date the certificate was issued.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

TrustCor Systems S. de R.L. maintains Commercial General Liability insurance coverage and Professional Liability/Errors & Omissions insurance coverage.

9.2.2 Other Assets

This CPS does not describe any other assets. However, any warranty documentation issued by TrustCor CA may do so.

9.2.3 Insurance or Warranty Coverage for End-entities

TrustCor CA provides a limited warranty to Relying Parties in TrustCor CA's Relying Party Agreement. Complete terms and conditions are found in the applicable Relying Party Agreement located on TrustCor's website.

9.3 Confidentiality of Business Information

TrustCor CA makes commercially reasonable efforts to maintain the integrity and confidentiality of information it receives from being used or disclosed for purposes other than those set forth in the CPS, a Subscriber Agreement, or a Relying Party Agreement.

9.3.1 Scope of Confidential Information

TrustCor CA keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel. Confidential information includes, but is not limited to:

- Subscriber Agreements and Relying Party Agreements
- Contingency, Disaster Recovery, And Business Continuity Plans
- Any certificate application records and documentation submitted in support of certificate applications, which is not in relation to an issued certificate, whether successful or rejected.
- External or internal audit trail records and reports, which are not required to be openly published.
- Transaction records, financial audit records, and internal records on the operations of TrustCor CA's infrastructure, certificate management, services and data.

9.3.2 Information Not Within the Scope of Confidential Information

Certificate status information and information that is included in a certificate or a certificate revocation list, including without limitation personal information, shall not be considered confidential. Certificates themselves are deemed public.

9.3.3 Responsibility to Protect Confidential Information

TrustCor CA personnel are trained in handling and responsible for protecting confidential information. All personnel in trusted positions are contractually obligated to protect confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

TrustCor CA personnel are required to follow the company Privacy Policy, maintained and published on its website, when handling personal or private information.

9.4.2 Information Treated as Private

TrustCor CA treats all personal information about an individual that is not publicly available in the contents of a Certificate, CRL, or OCSP as private information in accordance with the Privacy Policy.

9.4.3 Information Not Deemed Private

Certificates, CRLs, and OCSP and the personal or corporate information appearing in them are not considered private information.

9.4.4 Responsibility to Protect Private Information

TrustCor CA personnel are expected to handle personal information in compliance with legal requirements and the company Privacy Policy. All private information is securely stored and protected against accidental disclosure.

9.4.5 Notice and Consent to Use Private Information

Personal information obtained from an applicant during the application or identity verification process is considered private information if the information is not contained in a certificate. TrustCor CA includes any required consents in the Subscriber Agreement and will only use private information after obtaining the subject's consent or as required by law.

All Subscribers consent to the global transfer of any personal data contained in the Certificate.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

TrustCor CA may disclose private information, without notice, when disclosure is required by law or regulation, or in response to judicial or other administrative orders.

9.4.7 Other Information Disclosure Circumstances

Should TrustCor CA elect to disclose any non-public information other than covered in the sections above, it shall post to the public lists operated by the CA/B Forum to detail such disclosure, to whom the disclosure was made and when the disclosure was made. The actual information disclosed may, or may not, be repeated in the mailing list posting, depending on the sensitivity that TrustCor CA assesses the information to hold.

9.5 Intellectual Property Rights

TrustCor CA owns all intellectual property rights in TrustCor's services, including the Certificates, databases, websites, and any and all associated software embedded therein; as well as trademarks used in the provisioning of these services, and all documentation originating from TrustCor CA including this CPS.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Except where specifically stated in this CPS or a Subscriber Agreement, TrustCor CA represents and warrants that:

- TrustCor CA complies with its company policies, the CP and this CPS;
- Certificates issued will comply and be verified in accordance with this CPS;

- To the best of TrustCor CA's knowledge, there are no misrepresentations of fact in the Certificates;
- TrustCor CA's revocation services, including its repositories, are in accordance with the terms and conditions of this CPS;
- A repository of public information will be maintained on TrustCor's website; and
- Upon receipt of a request from an RA operating under such CA, issue an Certificate in accordance with the terms and conditions of this CPS.

9.6.2 RA Representations and Warranties

Any RA operating under TrustCor CA represents and warrants to conform to the policies and practices detailed in this CPS and to the obligations found in the associated Reseller Agreement.

The RA warranties include, but are not limited to:

- Perform all Certificate issuance and management services in accordance to the CP and this CPS;
- Certify that all information provided to TrustCor CA does not contain any false or misleading information; and
- All Certificates requested by the RA meet the requirements of this CPS.

9.6.3 Subscriber Representations and Warranties

Subscribers represent and warrant to TrustCor CA and Relying Parties that:

- All information material to the issuance of a Certificate Subscriber provides, is both accurate and complete;
- Subscriber retains control of, and takes all reasonable measures to keep confidential and properly protect their Private Key at all times;
- Subscriber has reviewed and verified the information in each Certificate prior to installing and using the Certificate, and will promptly notify TrustCor CA of any errors;
- Subscriber will only use the Certificate for authorized and legal purposes, consistent with this CPS and the relevant Subscriber Agreement, and only on those end points consistent with the Certificate itself;
- In the event of any actual or suspected misuse or compromise of the Private Key associated with the Certificate, or if any information in the Certificate is or becomes incorrect or inaccurate, Subscriber will immediately cease using the Certificate and its associated Private Key and promptly request TrustCor CA to revoke the Certificate;

- Subscriber shall cease use of the Private Key corresponding to the Certificate if reliably informed via any method that the private key has become compromised, or after the expiry date on the Certificate has passed;
- Subscriber must respond to TrustCor CA in a time period of seven (7) business days regarding any matter of reported misuse of the Certificate or apparent Private Key Compromise; and
- Subscriber acknowledges and accepts that TrustCor CA is entitled to revoke the certificate immediately, and without notice, should TrustCor CA discover that the Certificate is being used outside of the terms of the Subscriber Agreement, Terms of Use, or in furtherance of the goals of any criminal activity.
- Subscriber shall not use a private key corresponding to a TrustCor CA code signing certificate to sign malicious code.

9.6.4 Relying Party Representations and Warranties

Prior to relying on a TrustCor CA Certificate, each Relying Party must:

- Understand and obtain sufficient information on the use of Certificates and PKI
- Not rely on or use a TrustCor CA Certificate which has expired, been revoked or is being used for any purpose other than contained in the Certificate itself
- Verify both the TrustCor CA Certificate and the Certificates in the certificate chain by referring to the relevant CRLs and OCSP responder
- Read and agree to all terms and conditions of this CPS and Relying Party Agreement

9.6.5 Representations and Warranties of Other Participants

TrustCor CA shall detail any such representation or warranties in its various business agreement documents and/or Terms of Use documentation.

9.7 Disclaimers of Warranties

All Certificates and any related services and software are provided on an "as is" and "as available" basis. To the maximum extent permitted by law, TrustCor CA disclaims all express and implied warranties, including warranties of merchantability, fitness for a particular purpose, satisfactory quality and non-infringement. TrustCor CA does not warrant that any service or product will meet any expectations, be uninterrupted or that access to Certificates will be timely or error-free. TrustCor CA does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time.

9.8 Limitations of Liability

To the extent TrustCor CA has issued the Certificate or service in compliance with this CPS and/or CP, TrustCor CA shall not be liable to the Subscriber, Relying Party or any third parties for any claims, damages or losses suffered as a result of use or reliance on such Certificate or service provided by TrustCor CA. Otherwise, TrustCor CA's total liability to the Subscriber, Relying Party or any third party is limited as set forth in the relevant Subscriber Agreement and Relying Party Agreement.

9.9 Indemnities

9.9.1 Indemnification by CAs

TrustCor CA shall indemnify each Application Software Supplier against any and all third party claim, damage or loss suffered by such Application Software Supplier related to a Certificate issued by TrustCor CA that is not in compliance with the Baseline Requirements effective at the time the Certificate was issued, regardless of the cause of action or legal theory involved.

This does not apply, however, where such claim, damage or loss was directly caused by such Application Software Supplier's software displaying either a valid and trustworthy Certificate as not valid or trustworthy, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a revoked Certificate where the revocation status is available from TrustCor CA's repositories online, and the application software either failed to check such status or ignored an indication of revoked status.

9.9.2 Indemnification by Subscribers

Subscriber shall release, indemnify and hold harmless TrustCor CA, its partners, all RAs operating under TrustCor CA and any Resellers, and all respective directors, shareholders, officers, agents, employees, contractors and successors of the foregoing, against any and all liabilities, third party claims, proceedings, judgments, damages, losses, expenses and costs (including reasonable attorney's fees and court costs) that, directly or indirectly, arise from:

- Subscriber's breach of warranties, representations and obligations under the Subscriber Agreement, this CPS or applicable law;
- Any error, misrepresentation or omission made by Subscriber in using or applying for the Certificate;
- Any infringement of an Intellectual Property Right of any person or entity in information or content provided by Subscriber;

- Compromise, unauthorized use, or misuse of the Certificate or Private Key arising from Subscriber's negligence or intentional act.

9.9.3 Indemnification by Relying Parties

Each Relying Party shall release, indemnify and hold harmless TrustCor CA against any and all liabilities, third party claims, proceedings, judgments, damages, losses, expenses and costs, damage, or expense (including reasonable attorney's fees and court costs) that, directly or indirectly, arise from:

- the Relying Party's breach of the Relying Party Agreement, this CPS, or applicable law;
- reliance on a Certificate outside the terms; or
- failure to check the Certificate's status prior to use

9.10 Term and Termination

9.10.1 Term

The terms of this CPS begins from the publication in the online repository, and remains in effect until this document is replaced by a TCPA approved CPS.

9.10.2 Termination

The terms of this CPS and any amendments remain in effect until replaced by the issuance of a properly approved newer version. Changes become effective immediately upon publication.

9.10.3 Effect of Termination and Survival

Changes to this version, and all versions of the CPS, are published to TrustCor CA's online repository. Regardless of such changes, the following rights, responsibilities and obligations will survive termination:

- All Subscriber Agreements and any Relying Party Agreements;
- All payment obligations;
- All responsibilities and obligations related to confidential information, including those stated in section 9.3 of this CPS;
- All responsibilities and obligations to protect private information, including those stated in section 9.4.4 of this CPS;

- All representations and warranties, including those stated in section 9.6 of this CPS;
- All warranties disclaimed in section 9.7 of this CPS;
- All limitations of liabilities as described in section 9.8 of this CPS; and
- All indemnities described in section 9.9 of this CPS.

9.11 Individual Notices and Communications with Participants

TrustCor CA accepts notices related to this CPS, by means of digitally signed emails or in paper form sent to the TCPA, at the locations specified in section 1.5.1 (electronic and physical are given). All such notices are deemed effective upon receipt of a valid and digitally signed acknowledgement from TrustCor CA. The sender must receive such acknowledgment within ten (10) business days, or else written notice must then be sent in paper form through a courier service that confirms delivery.

9.12 Amendments

Amendments to this document are classified by severity:

- minimal - no changes to conditions to any party is involved. Typically used when correcting grammar, clarifying meaning or reformatting the appearance of text.
- small - additional business offerings or minor changes to existing business offerings are made which have minimal impact on any party's obligations
- large - major changes to rights or responsibilities are entailed. Major new business offerings, withdrawal of existing lines of business (where premature revocation of certificates might be needed) would be classified as major.

9.12.1 Procedure for Amendment

Any proposed change to this CPS is made in a source code controlled repository operated by TrustCor CA. Controls are in place to reasonably ensure that this CPS is not amended and published without the prior review and authorization of the TCPA. If accepted for inclusion, the TCPA will issue incremented numbering to the CPS version based on the severity of the change.

The version of the document will change as follows:

- minimal: the micro version of this document is incremented. No new OID is generated. (e.g. 1.0.1 -> 1.0.2)

- small: the minor version of this document is incremented, a new OID is generated, and included in all future certificates issued pursuant to the new CPS. (e.g. 1.2.4 -> 1.3.0)
- large: the major version of this document is incremented, and a new OID is generated. (e.g. 1.3.5 -> 2.0.0)

Updated versions of the CPS are posted to the online repository of the TrustCor CA website.

9.12.2 Notification Mechanism and Period

TrustCor CA provides notice of CPS revisions by publication of the CPS to the online repository. Amendments become effective on the date provided in the document. TrustCor CA reserves the right to make changes to this CPS without prior notice and at any time.

9.12.3 Circumstances Under Which OID Must be Changed

The TCPA has the sole authority to determine whether an amendment to the CPS requires an OID change. Circumstances for new OID changes are listed in section 9.12.1 of this CPS.

9.13 Dispute Resolution Provisions

Before filing suit, initiating an administrative claim, or resorting to any other dispute resolution mechanism, all parties agree to notify TrustCor CA for the purpose of seeking a dispute resolution.

If the dispute is not resolved within sixty (60) days after the initial confirmed notice, then the disputing party may proceed as permitted under applicable law as specified under the relevant Subscriber Agreement or Relying Party Agreement.

9.14 Governing Law

The substantive laws of the Republic of Panama govern the interpretation, construction and enforcement of this CPS and all matters related to it, including tort claims, without regards to any conflict-of-law provisions. The law of Panama applies to all TrustCor CA commercial or contractual relationships in which this CPS may apply, quoted implicitly or explicitly, in relation to TrustCor CA products and services where TrustCor CA acts as a provider, supplier, beneficiary receiver or otherwise.

Each party, including Subscribers, Relying Parties and all other related parties, hereby agree to the exclusive jurisdiction of the courts of the Republic of Panama.

9.15 Compliance with Applicable Law

Each party acknowledges and agrees to comply with all applicable national, state, local and foreign laws, regulations and export requirements. TrustCor CA shall have the right to refuse issuance or revoke a Certificate, without any prior notice, if Applicant or Subscriber fails to comply with this provision.

With regard to the PII provisions of Section 9.4.5, TrustCor CA meets the requirements of the data protection regulations of the European Union regarding access, disclosure and destruction of personal data.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CPS, the CP, the applicable Subscriber Agreement and Relying Party Agreement represent the entire agreement between the parties, superseding any and all agreements and representations that may exist pertaining to its subject matter.

In the event of any inconsistency between the provisions of this CPS and the provisions of any Subscriber Agreement or any Relying Party Agreement, the terms and conditions of this CPS shall govern.

9.16.2 Assignment

Entities operating under this CPS may not assign their rights or obligations to any other party without the prior written consent of TrustCor Systems S. de R.L.

9.16.3 Severability

If any provision of this CPS is found to be invalid, illegal or unenforceable by a court of competent jurisdiction, the provision affected will be construed so as to be enforceable to the maximum extent permissible by law; and the validity, legality and enforceability of the remaining provisions contained in this CPS shall not, in any way, be affected or impaired thereby.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

If a party violates the terms of any agreement with TrustCor CA, including but not limited to this CPS, TrustCor CA may seek indemnification and any fees (including reasonable attorney's

fees and court costs) from such party for damages, losses and expenses related to that party's conduct.

TrustCor CA's failure to enforce a provision of this CPS does not waive TrustCor CA's right to enforce the same provision later, or right to enforce any other provision of this CPS (except where a waiver is granted of explicit written permission by TrustCor CA).

9.16.5 Force Majeure

TrustCor CA shall not be liable for any interruption in performance or failure to perform an obligation under the this CPS, where such interruption or failure is caused by an event outside TrustCor CA's reasonable control.

9.17 Other Provisions

All Certificates issued by TrustCor CA are the property of TrustCor CA. Permission is given to reproduce and distribute on a non-exclusive, royalty-free basis **provided** that the reproduction is performed in full.

Private keys for Subscriber Certificates are **not** owned by TrustCor CA, but remain the property and responsibility of the Subscriber.