

SEP 19, 2016

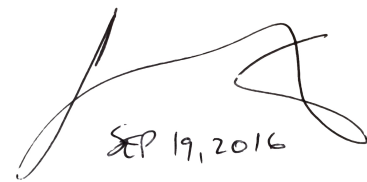
TrustCor Systems S. de R.L.

Certificate Policy

Version: 1.3.0

This document is PUBLIC

Generated on September 15, 2016 at 16:22 UTC.



SEP 19, 2016

Contents

1. INTRODUCTION

1.1 Overview

1.2 Document name and identification

1.3 PKI participants

1.3.1 Certification authorities

1.3.2 Registration authorities

1.3.3 Subscribers

1.3.4 Relying parties

1.3.5 Other participants

1.4 Certificate usage

1.4.1 Appropriate certificate uses

1.4.2 Prohibited certificate uses

1.5 Policy administration

1.5.1 Organization administering the document

1.5.2 Contact person

1.5.3 Person determining CPS suitability for the policy

1.5.4 CPS approval procedures

1.6 Definitions and acronyms

1.6.1 Definitions

1.6.2 Acronyms

1.6.3 References

1.6.4 Conventions

2. PUBLICATION AND REPOSITORY

RESPONSIBILITIES

2.1 Repositories

2.2 Publication of certification information

2.3 Time or frequency of publication

2.4 Access controls on repositories

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

3.1.2 Need for names to be meaningful

3.1.3 Anonymity or pseudonymity of subscribers

3.1.4 Rules for interpreting various name forms

3.1.5 Uniqueness of names

3.1.6 Recognition, authentication, and role of trademarks

3.2 Initial identity validation

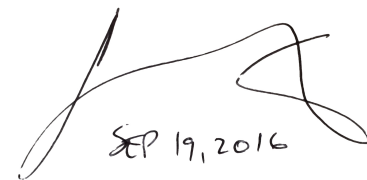
3.2.1 Method to prove possession of private key

3.2.2 Authentication of organization identity

3.2.2.1 Identity

3.2.2.2 DBA/Tradename

3.2.2.3 Verification of Country



SEP 19, 2016

3.2.2.4 Authorization by Domain Name Registrant

3.2.2.4.1 Validating the Applicant as a Domain Contact

3.2.2.4.2 Email, Fax, SMS or Postal Mail to Domain Contact

3.2.2.4.3 Phone Contact with Domain Contact

3.2.2.4.4 Constructed Email to Domain Contact

3.2.2.4.5 Domain Authorization Documents

3.2.2.4.6 Agreed-Upon Change to Website

3.2.2.4.7 DNS Change

3.2.2.4.8 IP Address

3.2.2.4.9 Test Certificates

3.2.2.4.10 TLS Using a Random Number

3.2.2.5 Authentication for an IP Address

3.2.2.6 Wildcard Domain Validation

3.2.2.7 Data Source Accuracy

3.2.3 Authentication of individual identity

3.2.4 Non-verified subscriber information

3.2.5 Validation of authority

3.2.6 Criteria for interoperation

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

3.3.2 Identification and authentication for re-key after revocation

3.4 Identification and authentication for revocation request

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

4.1.2 Enrollment process and responsibilities

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

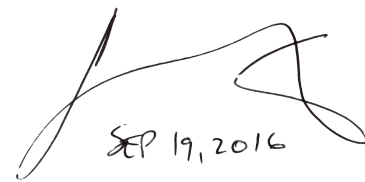
4.2.2 Approval or rejection of certificate applications

4.2.3 Time to process certificate applications

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

4.3.2 Notification to subscriber by the CA of issuance of certificate



SEP 19, 2016

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

4.4.2 Publication of the certificate by the CA

4.4.3 Notification of certificate issuance by the CA to other entities

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

4.5.2 Relying party public key and certificate usage

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

4.6.2 Who may request renewal

4.6.3 Processing certificate renewal requests

4.6.4 Notification of new certificate issuance to subscriber

4.6.5 Conduct constituting acceptance of a renewal certificate

4.6.6 Publication of the renewal certificate by the CA

4.6.7 Notification of certificate issuance by the CA to other entities

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

4.7.2 Who may request certification of a new public key

4.7.3 Processing certificate re-keying requests

4.7.4 Notification of new certificate issuance to subscriber

4.7.5 Conduct constituting acceptance of a re-keyed certificate

4.7.6 Publication of the re-keyed certificate by the CA

4.7.7 Notification of certificate issuance by the CA to other entities

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

4.8.2 Who may request certificate modification

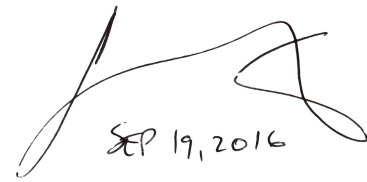
4.8.3 Processing certificate modification requests

4.8.4 Notification of new certificate issuance to subscriber

4.8.5 Conduct constituting acceptance of modified certificate

4.8.6 Publication of the modified certificate by the CA

4.8.7 Notification of certificate issuance by the CA to other entities



SEP 19, 2016

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

4.9.2 Who can request revocation

4.9.3 Procedure for revocation request

4.9.4 Revocation request grace period

4.9.5 Time within which CA must process the revocation request

4.9.6 Revocation checking requirement for relying parties

4.9.7 CRL issuance frequency (if applicable)

4.9.8 Maximum latency for CRLs (if applicable)

4.9.9 On-line revocation/status checking availability

4.9.10 On-line revocation checking requirements

4.9.11 Other forms of revocation advertisements available

4.9.12 Special requirements re key compromise

4.9.13 Circumstances for suspension

4.9.14 Who can request suspension

4.9.15 Procedure for suspension request

4.9.16 Limits on suspension period

4.10 Certificate status services

4.10.1 Operational characteristics

4.10.2 Service availability

4.10.3 Optional features

4.11 End of subscription

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

4.12.2 Session key encapsulation and recovery policy and practices

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

5.1.2 Physical access

5.1.3 Power and air conditioning

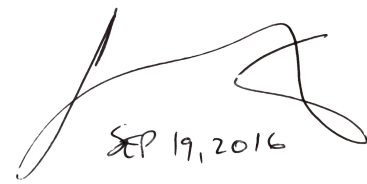
5.1.4 Water exposures

5.1.5 Fire prevention and protection

5.1.6 Media storage

5.1.7 Waste disposal

5.1.8 Off-site backup



SEP 19, 2016

5.2 Procedural controls

5.2.1 Trusted roles

5.2.2 Number of persons required per task

5.2.3 Identification and authentication for each role

5.2.4 Roles requiring separation of duties

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

5.3.2 Background check procedures

5.3.3 Training requirements

5.3.4 Retraining frequency and requirements

5.3.5 Job rotation frequency and sequence

5.3.6 Sanctions for unauthorized actions

5.3.7 Independent contractor requirements

5.3.8 Documentation supplied to personnel

5.4 Audit logging procedures

5.4.1 Types of events recorded

5.4.2 Frequency of processing log

5.4.3 Retention period for audit log

5.4.4 Protection of audit log

5.4.5 Audit log backup procedures

5.4.6 Audit collection system (internal vs. external)

5.4.7 Notification to event-causing subject

5.4.8 Vulnerability assessments

5.5 Records archival

5.5.1 Types of records archived

5.5.2 Retention period for archive

5.5.3 Protection of archive

5.5.4 Archive backup procedures

5.5.5 Requirements for time-stamping of records

5.5.6 Archive collection system (internal or external)

5.5.7 Procedures to obtain and verify archive information

5.6 Key changeover

5.7 Compromise and disaster recovery

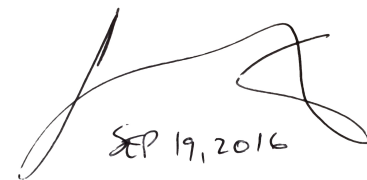
5.7.1 Incident and compromise handling procedures

5.7.2 Computing resources, software, and/or data are corrupted

5.7.3 Entity private key compromise procedures

5.7.4 Business continuity capabilities after a disaster

5.8 CA or RA termination



SEP 19, 2016

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

6.1.1.2 Subscriber Key Pair Generation

6.1.2 Private key delivery to subscriber

6.1.3 Public key delivery to certificate issuer

6.1.4 CA public key delivery to relying parties

6.1.5 Key sizes

6.1.6 Public key parameters generation and quality checking

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

6.2.2 Private key (n out of m) multi-person control

6.2.3 Private key escrow

6.2.4 Private key backup

6.2.5 Private key archival

6.2.6 Private key transfer into or from a cryptographic module

6.2.7 Private key storage on cryptographic module

6.2.8 Method of activating private key

6.2.9 Method of deactivating private key

6.2.10 Method of destroying private key

6.2.11 Cryptographic Module Rating

6.3 Other aspects of key pair management

6.3.1 Public key archival

6.3.2 Certificate operational periods and key pair usage periods

6.4 Activation data

6.4.1 Activation data generation and installation

6.4.2 Activation data protection

6.4.3 Other aspects of activation data

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

6.5.2 Computer security rating

6.6 Life cycle technical controls

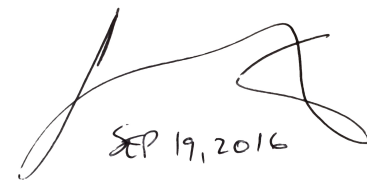
6.6.1 System development controls

6.6.2 Security management controls

6.6.3 Life cycle security controls

6.7 Network security controls

6.8 Time-stamping



SEP 19, 2016

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

7.1.1 Version number(s)

7.1.2 Certificate extensions

7.1.2.1 Root CA Certificate

7.1.2.2 Subordinate CA Certificate

7.1.2.3 Subscriber Certificate

7.1.2.4 All Certificates

7.1.2.5 Application of RFC 5280

7.1.3 Algorithm object identifiers

7.1.4 Name forms

7.1.4.1 Issuing CA Certificate Subject

7.1.4.2 Subject Information for Standard Server Authentication certificates

7.1.4.3 Subject Alternative Names for Standard Server Authentication certificates

7.1.5 Name constraints

7.1.6 Certificate policy object identifier

7.1.6.1. Reserved Certificate Policy Identifiers

7.1.6.2. Root CA Certificates

7.1.6.3 Subordinate CA Certificates

7.1.6.4 Subscriber Certificates

7.1.7 Usage of Policy Constraints extension

7.1.8 Policy qualifiers syntax and semantics

7.1.9 Processing semantics for the critical Certificate Policies extension

7.2 CRL profile

7.2.1 Version number(s)

7.2.2 CRL and CRL entry extensions

7.3 OCSP profile

7.3.1 Version number(s)

7.3.2 OCSP extensions

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

8.2 Identity/qualifications of assessor

8.3 Assessor's relationship to assessed entity

8.4 Topics covered by assessment

8.5 Actions taken as a result of deficiency

8.6 Communication of results

8.7 Self-Audits

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

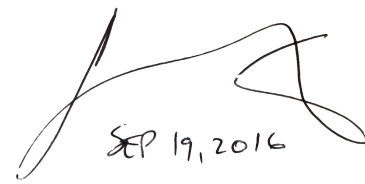
9.1.1 Certificate issuance or renewal fees

9.1.2 Certificate access fees

9.1.3 Revocation or status information access fees

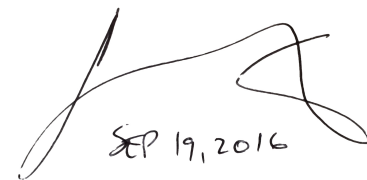
9.1.4 Fees for other services

9.1.5 Refund policy



SEP 19, 2016

- 9.2 Financial responsibility
 - 9.2.1 Insurance coverage
 - 9.2.2 Other assets
 - 9.2.3 Insurance or warranty coverage for end-entities
- 9.3 Confidentiality of business information
 - 9.3.1 Scope of confidential information
 - 9.3.2 Information not within the scope of confidential information
 - 9.3.3 Responsibility to protect confidential information
- 9.4 Privacy of personal information
 - 9.4.1 Privacy plan
 - 9.4.2 Information treated as private
 - 9.4.3 Information not deemed private
 - 9.4.4 Responsibility to protect private information
 - 9.4.5 Notice and consent to use private information
 - 9.4.6 Disclosure pursuant to judicial or administrative process
 - 9.4.7 Other information disclosure circumstances
- 9.5 Intellectual property rights
- 9.6 Representations and warranties
 - 9.6.1 CA representations and warranties
 - 9.6.2 RA representations and warranties
 - 9.6.3 Subscriber representations and warranties
 - 9.6.4 Relying party representations and warranties
 - 9.6.5 Representations and warranties of other participants
- 9.7 Disclaimers of warranties
- 9.8 Limitations of liability
- 9.9 Indemnities
- 9.10 Term and termination
 - 9.10.1 Term
 - 9.10.2 Termination
 - 9.10.3 Effect of termination and survival
- 9.11 Individual notices and communications with participants
- 9.12 Amendments
 - 9.12.1 Procedure for amendment
 - 9.12.2 Notification mechanism and period
 - 9.12.3 Circumstances under which OID must be changed
- 9.13 Dispute resolution provisions
- 9.14 Governing law
- 9.15 Compliance with applicable law



SEP 19, 2016

9.16 Miscellaneous provisions

9.16.1 Entire agreement

9.16.2 Assignment

9.16.3 Severability

9.16.4 Enforcement (attorneys' fees and waiver of rights)

9.16.5 Force Majeure

9.17 Other provisions

1. INTRODUCTION

1.1 Overview

This certificate policy (CP) contains the policy adopted by the CA managed by TrustCor Systems S. de R.L. ("TrustCor CA") for the issuance and management of publicly trusted SSL certificates, as adopted by the CA/ Browser forum and is designed to be compliant with the criteria stated in Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") version 1.3.0 (available at <https://cabforum.org>).

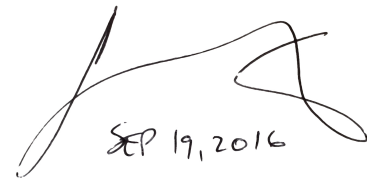
TrustCor CA's certificate policies are controlled by the TrustCor Policy Authority (TCPA). The TCPA determines how this CP applies to the entities which make up TrustCor CA's business: the Certificate and Registration Authorities (CAs and RAs respectively), the Subscribers and Relying Parties.

Client certificates follow the identity assurance frameworks documented in NIST 800-63 and the Kantara Initiative. Qualified Certificate law from the European Union (EU) also governs the identity assurance practices of TrustCor CA.

Other documents which govern the activities of TrustCor CA include, but are not limited to:

- TrustCor CA Certificate Practice Statements (CPS)
- TrustCor CA Privacy Policy
- TrustCor CA Security Policy
- TrustCor CA Subscriber Agreements

This document is formatted according to the IETF RFC3647 CP/CPS framework. Sections which do not apply to TrustCor CA, or where TrustCor CA makes no authoritative statement, will have either the text "No stipulation" or "Not Applicable".



SEP 19, 2016

1.2 Document name and identification

This document is the “TrustCor Systems S. de R.L. Certificate Policy” and was approved by the TCPA on 2016-01-23. Changes to other released certificate policies are:

Date	Changes	Version
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	1.2.1
2016-01-23	This version 1.2.1 corrects the incorrect policyID root 1.3.6.1.4.4 to 1.3.6.1.4.1	1.2.1
2015-11-16	This version 1.2.0 replaces the TrustCor Certificate Policy, dated 2015-08-15, being reformatted into RFC3647 form.	1.2.0

TrustCor CA designates its OIDs with the prefix 1.3.6.1.4.1.44031 (TC-OID)

The OID arc for objects approved by the TCPA and released to production has the prefix 1.3.6.1.4.1.44031.1

Documents governing policy and practices for TrustCor CA have the prefix 1.3.6.1.4.1.44031.1.1

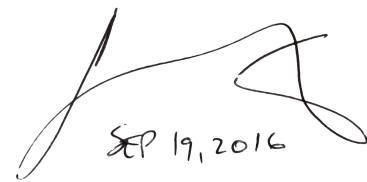
This document has the OID 1.3.6.1.4.1.44031.1.1.4

1.3 PKI participants

1.3.1 Certification authorities

The TCPA establishes the policies which govern the TrustCor CA operations, namely the installation and operation of its Root and Subordinate CAs. The TCPA defines the business requirements for TrustCor CA as well as the usage policies for digital certificates issued under the auspices of TrustCor CA. The TCPA is comprised of members from senior management, security and CA operations teams.

The TrustCor CPS shall denote the list of Root and Subordinate CAs operated under TrustCor CA’s brand.

A handwritten signature in black ink is located in the top right corner of the page. Below the signature, the date "SEP 19, 2016" is written in a similar cursive style.

1.3.2 Registration authorities

Registration Authorities (RAs) collect and validate subscriber details which can then be submitted to TrustCor CA for signing into a certificate. TrustCor CA requires any external RA (that is, one not run directly by TrustCor CA) to submit policy and practice documentation which is then reviewed by the TCPA to ensure that it meets the same policy and practice requirements which govern TrustCor CA's own registration processes.

1.3.3 Subscribers

A subscriber is an entity which applies for the right to have the expression of particular identity (the *subject*) bound to a particular public key and have that binding digitally signed by TrustCor CA. Note that the subscriber is not necessarily the same as the subject.

TrustCor CA requires all subscribers to be bound by the terms of a subscriber agreement which imposes duties owing to TrustCor CA on the subscriber. Once the identity validation process is complete, the subscriber is entitled to use the resulting certificate to support secure transactions and communication pursuant to the provisions of the relevant subscriber agreement.

1.3.4 Relying parties

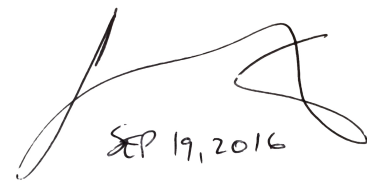
Relying Parties (RP) are those entities which rely on the subject identity and public key information present in a TrustCor CA issued certificate, in order to effect secure communications and/or transactions.

All RPs are required to use the revocation publishing services detailed in the CPS to be assured that a presented certificate is still fit to be trusted.

TrustCor CA shall ensure that, at a minimum, highly available CRL download and OCSP services are available for all certificates issued under its roots.

1.3.5 Other participants

No stipulation



SEP 19, 2016

1.4 Certificate usage

A digital certificate (Certificate) is a binding between an expression of a subject's identity and a public key, whose private component is held by the subject. This binding is cryptographically signed by TrustCor CA, and can be used by the private key holder subject to certain restrictions as expressed via the subscriber agreements and CPS.

TrustCor CA shall ensure that all certificate holders are bound by an agreement which sets out the permitted uses of the certificate.

1.4.1 Appropriate certificate uses

Each certificate contains a set of designators (OIDs) which state the purposes to which a certificate may be put (the "key usage" and "extended key usage" segments of the certificate).

1.4.2 Prohibited certificate uses

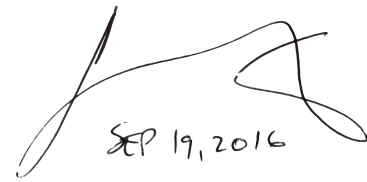
TrustCor CA gives no assurance that the subscriber controlling use of a certificate is reputable or that the subscriber will comply with any local laws governing the use of cryptographic materials. TrustCor CA's guarantees extend only to an assurance that the subscriber presented sufficient identifying information as to satisfy the relevant validation criteria for the type of certificate issued, at or near the time of issuance.

TrustCor CA specifically states that its certificates may not be used where such use is prohibited by law binding on the subscriber.

TrustCor CA further prohibits the use of its certificates in applications which require failsafe operation and whose failures carry risk of injury, death or damage to the environment. Such applications include, but are not limited to:

- Operation of nuclear power facilities
- Air traffic control systems
- Weapons control systems

- Aircraft navigation systems



SEP 19, 2016

1.5 Policy administration

1.5.1 Organization administering the document

This CP and any documents to which this document makes reference are maintained under the authority of the TCPA, which can be contacted at:

TrustCor Policy Authority, 371 Front Street West #123, Toronto ON M5V3S8 Canada
--

1.5.2 Contact person

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

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

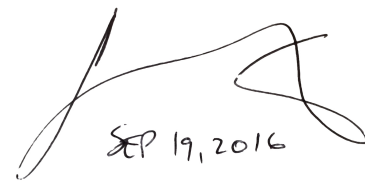
1.5.3 Person determining CPS suitability for the policy

The TCPA determines suitability of any CPS required to conform to this policy. The TCPA solicits the advice of an independent auditor in order to guide such deliberation, and is required to act on such guidance to ensure compliance with such audits that TrustCor CA requires to be satisfied.

1.5.4 CPS approval procedures

The TCPA will review such changes as are required to the CP, and/or any CPS which must conform to it, and update both CP and CPS versioning accordingly. The version of any document has three components: Major, Minor and Micro.

Micro release changes are there to indicate minor syntactic changes (e.g. spelling errors, grammatical clarity, etc.). Micro releases do not require a new OID issue.



SEP 19, 2016

Minor release changes indicate new or altered information which has a bearing on TrustCor CA's processes, or imposes altered duties on PKI participants). Such changes will be accompanied by a new OID issue.

Major release changes indicate significantly altered information, such as entirely new business offerings, major liability changes, or significant changes to the duties imposed upon subscribers. A new OID issues is required for such major changes.

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

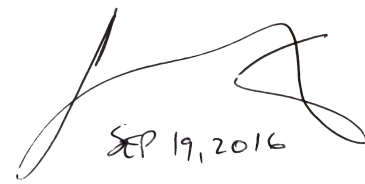
The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if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



SEP 19, 2016

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.

CAA Record

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."

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 Policy

This document.

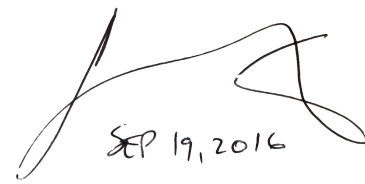
Certificate Problem Report

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

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



SEP 19, 2016

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

Certification Practice Statement

One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

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.

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

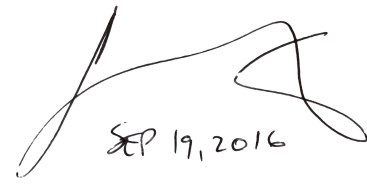
Documentation provided by, or a CA’s documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant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

Domain Name

The label assigned to a 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



SEP 19, 2016

(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 Namespace

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

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

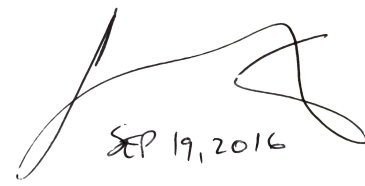
A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

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.



SEP 19, 2016

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.

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.

Legal Entity

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

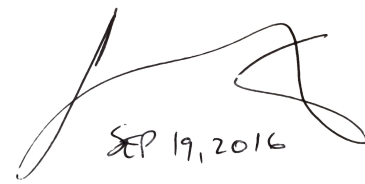
Object Identifier

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



SEP 19, 2016

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.

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

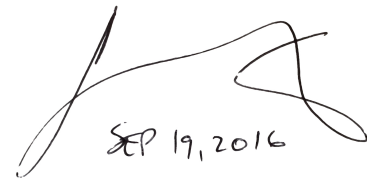
A natural person or Legal Entity that meets the requirements of Section 8.2 (Identity/Qualifications of Assessor).

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



SEP 19, 2016

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

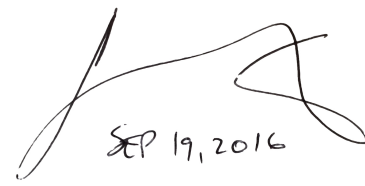
Reserved IP Address

An IPv4 or IPv6 address that the IANA has marked as reserved: <http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml> (<http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml>) <http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml> (<http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml>)

Root CA

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

Root Certificate



SEP 19, 2016

The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

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

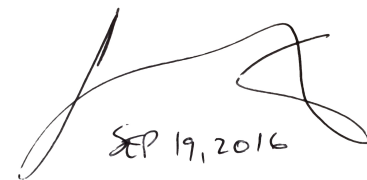
A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

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.

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



SEP 19, 2016

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 Specialists

Someone who performs the information verification duties specified by these Requirements

Validity Period

The period of time measured from the date when the Certificate is issued until the Expiry Date.

Wildcard Certificate

A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

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

DNS

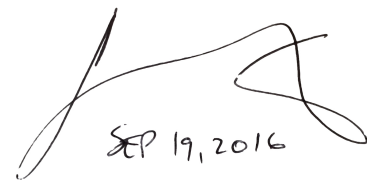
Domain Name System

EU

The European Union

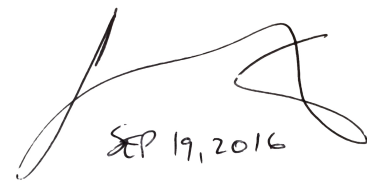
FIPS

(US Government) Federal Information Processing
Standard



SEP 19, 2016

- FQDN
Fully Qualified Domain Name
- IANA
Internet Assigned Numbers Authority
- ICANN
Internet Corporation for Assigned Names and
Numbers
- IM
Instant Messaging
- ISO
International Organization for Standardization
- NIST
(US Government) National Institute of Standards
and Technology
- OCSP
Online Certificate Status Protocol
- OID
Object Identifier
- 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



SEP 19, 2016

1.6.3 References

1.6.4 Conventions

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

All TrustCor CAs will publish all trusted CA certificates; any revocation data for certificates issued under those CA certificates and all policy documentation including this CP, the CPS and all public subscriber agreements on online repositories.

TrustCor CA is required to ensure that the repository is available on a 99% uptime basis (e.g. a total of no more than 3 overall days unplanned downtime per year). Planned maintenance may not cause more than 36 hours of downtime in any given year. Note that the repositories may be geographically replicated and that the outage constraints apply to the repository service as a whole, not an individual part while other instances of the repository may field external requests for published information.

2.2 Publication of certification information

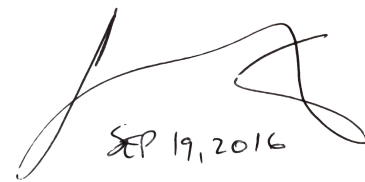
TrustCor CA will make the following information publicly available via HTTP:

- All trusted root certificates
- All currently used Subordinate CAs directly signed by the root certificates above
- All CRLs issued by any of the CAs mentioned above
- All current Certificate Policy documents
- All current Certificate Practice Statements

Any end-entity certificate which references a CPS, CRL or issuing certificate will also contain a URI reference which will resolve to the appropriate document.

2.3 Time or frequency of publication

All CAs under TrustCor CA's control will publish their CA certificates as soon as possible after issuance.



SEP 19, 2016

CRLs for CAs issuing end-entity certificates must generate and publish their revocation data at least every four days (whether or not any new revocation data is available).

CRLs for Root CAs will re-issue and re-publish their CRLs every 6 months, but must issue a new CRL within 24 hours if a subordinate CA has been revoked.

CP and CPS documents must be made publicly available no more than seven (7) days after approval by the TCPA.

2.4 Access controls on repositories

TrustCor CA is required to provide unrestricted read access to its online repositories, and is further required to impose such technical and management controls as to prevent any unauthorized party from altering the contents of its repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

TrustCor CAs must issue certificates with have a subject distinguished name (DN) compliant with the requirements of the ITU X.500 standards documents.

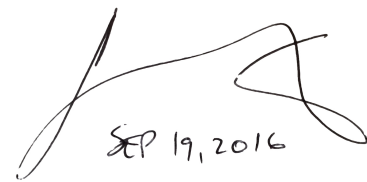
TrustCor CAs must not issue names which correspond to private IP address spaces as per RFC 1918 and RFC 4193.

Common Names whose value differ only in terms of whitespace are not to be treated as different from an identity perspective.

3.1.2 Need for names to be meaningful

The names which appear in any TrustCor end entity certificate must reflect a canonical form of the names submitted as part of the certificate application process.

TrustCor CA shall take such reasonable steps to ensure that the name present in a certificate is not an attempt to mislead relying parties owing to visual similarity to already issued certificates (e.g. anti-phishing, or identity fraud)



SEP 19, 2016

TrustCor CA may not issue certificates containing names components which have not been validated as part of the validation process leading the certificate issuance. That is, all components of any subject names in a certificate must have accompanying documentary evidence which satisfies the relevant validation criteria.

Organizational names must reflect exactly the text which appears in the accompanying validation evidence. The only exception for this is where an abbreviation may be used for a company's trading definition. For example, "Limited Liability Company" may be abbreviated to "LLC"; "Limited" may be abbreviated to "Ltd.", and so on. In no case may the company name itself be altered from the validation evidence.

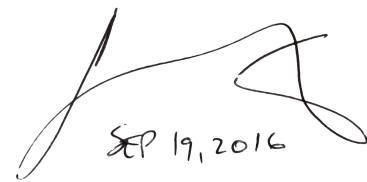
Internal organizational units may not be represented in certificates directly issued by TrustCor CA subordinate CAs. Organizational unit names may be issued via enterprise level subordinate CAs (ie, which are technically restricted to constrain certificates to a particular organization's name space); such issuance must be governed by a particular subscriber agreement for enterprise level CAs.

State, locality and country information may only be included when validation evidence supports their inclusion (e.g. via governmentally issued company directories, national charity registries, etc.)

3.1.3 Anonymity or pseudonymity of subscribers

TrustCor CA may issue certificate to end-entities who choose to remain anonymous or pseudonymous subject to the restriction that the validation evidence supports the use of the pseudonym, that the grade of certificate chosen does not prohibit such use, and that the name chosen is canonically unique (eg, whitespace is insignificant, case is insignificant, etc.)

TrustCor shall make reasonable effort to ensure that an anonymous/pseudonymous certificate issuance is not likely to confuse or mislead any relying party.



SEP 19, 2016

3.1.4 Rules for interpreting various name forms

The X.500 standards set defines the interpretation of any DN. The syntax used to express names inside a certificate is governed according to RFC 4514 (obsoleting RFC 2253).

3.1.5 Uniqueness of names

TrustCor CA may not have two concurrently valid certificates issued by the same CA which have an identical subject DN.

Where name collisions for organizationally validated subjects could occur, the subject DN topology must include a globally unique field, such as an email address, or Kerberos principal name.

3.1.6 Recognition, authentication, and role of trademarks

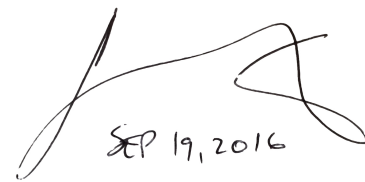
TrustCor CA does not validate the authority to use a particular trademark which forms part of a subject DN. However, subscriber agreements must make clear that subscribers are not permitted to assert a trademark to which they have no authority. Furthermore, TrustCor CA reserves the right to refuse or revoke any and all certificates where the trademark stated is in dispute.

3.2 Initial identity validation

TrustCor CA may use a variety of communication methods to begin a validation process, including, but not limited to:

- Telephone Calls
- SMS messages
- E-mail
- Postal Service

TrustCor CA shall provide a method for a user to register a principal name together with such credentials as can be used to further identify that principal to TrustCor CA, for the purposes of certificate requesting, revocation, re-keying, modification and renewal.



SEP 19, 2016

3.2.1 Method to prove possession of private key

TrustCor CA must verify that the subscriber requesting a certificate possesses a private key corresponding to the public key submitted during application.

3.2.2 Authentication of organization identity

Any domain name which is to form part of a subject DN or a subjectAltName must pass validation checks stated in BR Section 3.2.2.

If an application is made to have a subject DN or subjectAltName include an organization's name, then TrustCor CA must use such reliable databases to be assured that the organization is:

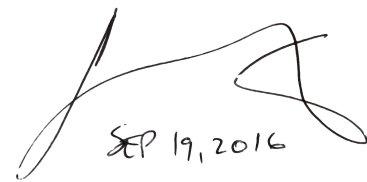
- Legally registered in a reliable government database, or
- Registered via a reliable third party aggregator which sources reliable government databases directly.
- Entitled to conduct operations (e.g. the company is not dormant, has been dissolved, etc.)

As an alternative to the above, TrustCor CA may directly communicate with a relevant government department to be assured that the criteria of legal incorporation and ability to conduct business are met.

3.2.2.1 Identity

TrustCor CA must only include such identity information in its certificates as has been established via direct communication with a subscriber (e.g. email address, or telephone number); or via communication with a government body issuing a credential which can be used to substantiate identity.

TrustCor CA shall establish processes as per the BR section Third party databases can be used to establish identity assuming that they meet the criteria established in section 3.2.2.7 of integrity, liveness and authority.



SEP 19, 2016

3.2.2.2 DBA/Tradename

If a requestor wishes to assert the use of a tradename within a certificate, TrustCor CA will have a process to obtain a list of trading bodies within a given national jurisdiction.

If TrustCor CA does not have a valid process for obtaining such a reliable list of incorporated bodies, then it will refuse to issue a certificate asserting such an identity.

3.2.2.3 Verification of Country

Country identity assertions must be validated to exist within ISO-3166-1. Organizational identities will have their country set depending on which national register of organizations is used to validate the identity (e.g. if Companies House in the UK is used to validate a British trading institution, then the country will be set to be GB).

TrustCor CA will not include country code designations for DV only certificates.

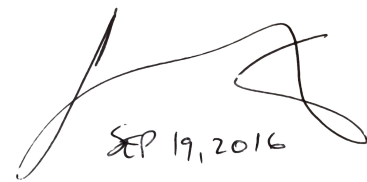
TrustCor CA does not issue certificates for IP identity assertions, therefore no stipulation with regard to country is required.

Where individual identity information is considered, and where national government issued ID is used as proof, the country code will be set to that of the issuing nation.

3.2.2.4 Authorization by Domain Name Registrant

If any certificate request needs an FQDN within a certificate (subject DN or subjectAltName with a dNSName marker), TrustCor CA will use the process outlined in BR 3.2.2.4 to ensure that the requestor is entitled to request the FQDN.

In all cases, random value challenges must contain at least 128 bits of entropy, and may not live longer than 7 days. After a random value challenge expires, the application must be restarted.



SEP 19, 2016

3.2.2.4.1 Validating the Applicant as a Domain Contact

TrustCor shall use authoritative databases to fetch domain contact information.

3.2.2.4.2 Email, Fax, SMS or Postal Mail to Domain Contact

TrustCor may use any of the headlined methods to contact applicants for email or domain certificates.

3.2.2.4.3 Phone Contact with Domain Contact

TrustCor must ensure that only the phone number as presented in the authoritative databases for contacts is used to telephone for validation reasons.

3.2.2.4.4 Constructed Email to Domain Contact

TrustCor shall maintain a list of approved mailboxes for constructing emails. It must be a subset of those allowed in the BR's for this corresponding section.

3.2.2.4.5 Domain Authorization Documents

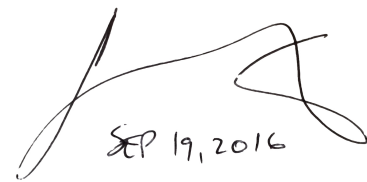
TrustCor shall not use DADs to validate requests

3.2.2.4.6 Agreed-Upon Change to Website

TrustCor may supply and observe the installation of a random value challenge under a well known URI, using the observation as completion of validation.

3.2.2.4.7 DNS Change

TrustCor may check for TXT record changes within the domain requested to complete domain control validation.



SEP 19, 2016

3.2.2.4.8 IP Address

IP changes are not to be used by TrustCor as a validation method.

3.2.2.4.9 Test Certificates

Test Certificates are not to be used by TrustCor as a validation method.

3.2.2.4.10 TLS Using a Random Number

This method is not yet approved for validation of TrustCor certificates.

3.2.2.5 Authentication for an IP Address

TrustCor CA shall not issue identities based on either IPv4 or IPv6 addresses.

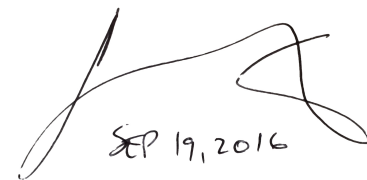
3.2.2.6 Wildcard Domain Validation

TrustCor CA shall not issue wildcard domain certificates.

3.2.2.7 Data Source Accuracy

Before allowing a data source to be used as part of any validation process, the TCPA must make a judgement that the source is:

- properly constituted to perform such a function
- refreshed regularly (e.g. by receiving company filings regularly)



SEP 19, 2016

- likely to produce information of sufficiently high integrity for the purposes of TrustCor CAs business needs.

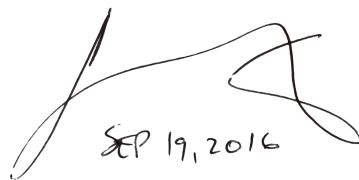
3.2.3 Authentication of individual identity

Where individual identity certificates are issued as part of a business offering, TrustCor CA shall establish a process in its CPS which meets the following criteria for validation (levels are described in the Kantara Initiative levels of assurance).

- Level 1 S/MIME - The certificate requestor must demonstrate control over the email address being requested.
- Level 1 Client - The requestor must either provide in-person proof of identity by use of government issued photo ID (drivers license, passport, etc.) at a place suitable to TrustCor CA; or proof of the ability to receive mail at the billing address of a payment card which is submitted as part of the subscription process.
- Level 2 S/MIME or Client - Apart from the email address requirement for level 1, the requestor must also provide valid forms of identification which combine to yield:
 1. his/her date of birth;
 2. his/her current physical address
 3. A valid telephone number.

If the requestor has not previously had a relationship with TrustCor CA at this level of assurance, then TrustCor CA must then validate that the person can receive information sent to the physical address and respond with that information via a telephone call.

In addition, TrustCor must validate the forms of identification using either remote verification checks against reliable government databases suitable to establish identity checks, or arrange to have the credentials checked in person by an authorized agent of the state which issued the credential.

Handwritten signature and date: SEP 19, 2016

If the requestor has an existing relationship at this level, the demonstration of knowledge of a passphrase shall suffice to prove identity.

At the time of this document, TrustCor CA defines no protocols, and shall not issue certificates based upon, Level 3 or Level 4 identity assurance. Future versions of this document will define such protocols.

If a requestor is not legally competent to complete an application, a designated representative may accompany the requestor to a face to face identity validation session. The representative must present sufficient information as would be required to grant said representative a certificate of the same level being obtained on behalf of the requestor.

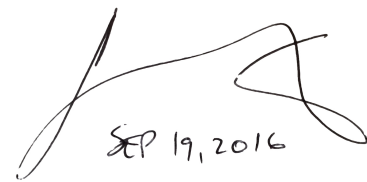
3.2.4 Non-verified subscriber information

TrustCor CA shall not include any subscriber information in a certificate which is not validated as part of the subscription process. Thus, for example, Level 1 S/MIME certificates may not have common name components in their subjects, since there is no requirement to validate that information.

3.2.5 Validation of authority

TrustCor CA, or any authorized external RA, must verify the evidence accompanying a certificate request according to the following certificate types:

- DV SSL Certificates - the domain name registrar must list the applicant as part of the WHOIS record; or effective control of the domain shall be demonstrated by the applicant or communication satisfying BR 3.2.2.4 shall be obtained.
- OV SSL Certificates - In addition to the communications as per DV SSL Certificates, the CA/RA must also be satisfied that such assurances as per BR 3.2.2.2 and BR 3.2.2.3 have been completed. Specifically, reliable data sources such as government registries of incorporation shall be consulted to verify that the organizational identity can be reasonably asserted in the certificate subject.



SEP 19, 2016

- S/MIME Certificates - the requestor must demonstrate control over receiving and sending messages from the specified email address.
- Level 2 Individual-Organizational Certificates - the CA must possess communication delivered using a reliable method that the individual has an ongoing association with the organization; and that this communication must be sourced from someone in the organization with the ability to speak authoritatively for its associations (e.g. an HR representative, the signatory to a contract of employment, etc.)

3.2.6 Criteria for interoperation

If TrustCor CA enters into any cross signing relationship, the CA shall make the cross-signed certificate paths available on its website under the same conditions of availability as its own Root and Subordinate CAs as noted under Section 2.2.

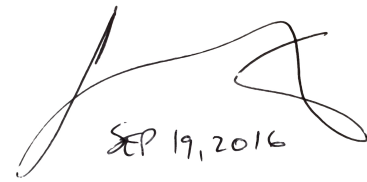
3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Upon the premise that validation documentation (ie, that which allowed a certificate to be issued in the first place) is no older than thirty-nine (39) months, TrustCor CA may permit a certificate to be re-issued using the same names and identity assurance level as the original certificate. A certificate so issued may not be valid for longer than the 39 months from initial validation.

The level of authentication required will depend on the type of certificate issued. The 'levels' in this list correspond to the Kantara Initiative levels of assurance.

- Level 1 S/MIME certificates - challenge/response to an encrypted email is enough to demonstrate continued private key possession and ability to receive email at the certified address.
- Level 1 Client certificates - a username and password, set at subscription time is sufficient to allow re-key.



SEP 19, 2016

- Level 1 DV SSL server certificates - a username and password, set at subscription time will suffice to allow re-key.
- Level 2 Client certificates - demonstration of a pre-shared key and OTP validation as described in Section 3.2.3 is sufficient to allow re-key.
- Level 2 S/MIME certificates - challenge/response to an encrypted email is sufficient. Alternatively, authentication to a TrustCor CA certificate management website may suffice, using multi-factor authentication.
- Level 2 OV SSL certificates - a multi-factor authentication is needed (e.g. username/password plus OTP authentication) to allow re-key
- External subordinate CA certificates - re-key is only possible when the original documentation and policies regarding treatment have been re-validated and certified to still hold. This process will be manual rather than amenable to automated re-key.

3.3.2 Identification and authentication for re-key after revocation

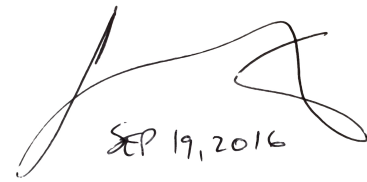
If a certificate is revoked, TrustCor CA will not re-key a certificate with the same name set and issuer CA. A new application process must take place to re-issue a certificate with the same subject names.

There is one exception to the above statement: if a subjectAltName which **does not** form part of the subject DN in a certificate is no longer needed, the certificate may be revoked and a new certificate issued using the same public key, but without the unneeded subjectAltName. The stipulations of lifetime validity and validation requirements from Section 3.3.1 still apply.

3.4 Identification and authentication for revocation request

Revocation requests must be authenticated to ensure they emanate from authorized personnel. Demonstration of knowledge of a certificate's corresponding private key is sufficient evidence as to validate a revocation request. Other methods (e.g. out

of band communications from trusted parties) may also be used to establish the identity of a revocation requestor.



SEP 19, 2016

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

If an applicant has had a certificate revoked by virtue of breach of a subscriber agreement, or has had a certificate revoked by an externally originating request because of fraudulent behaviour (either in application for the certificate or in its usage), TrustCor CA shall record this information in its issuance database. TrustCor CA will not then process an application from such an applicant.

If an entity - corporate or individual - has been placed on a list of prohibited persons or institutions, or an application emanates from a embargoed territory as stated by the government of the United States of America, then an application from such a person will be rejected.

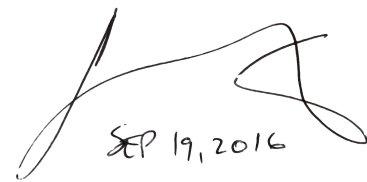
4.1.2 Enrollment process and responsibilities

TrustCor CA is responsible for communicating to the requesting entity the identity evidence required to issue a particular type of certificate, as well as the terms and conditions for submission.

TrustCor CA is responsible for validating the identity evidence supplied by the certificate requestor to ensure that it is:

- current
- properly formed
- genuine
- complete
- meets the standards required for the certificate type requested

The certificate requestor is solely responsible for supplying the required information in a timely manner and in accordance with the stated terms and conditions.



SEP 19, 2016

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

TrustCor CA must ensure that any application contains all the data to complete a certificate application as per Section 4.1.2

TrustCor CA will check any domain names against published DNS CAA records to ensure it is not prohibited (or indeed, is expressly allowed) to issue certificates for the domain name which forms part of any SSL Server certificate. This check must be performed for **all** names which will be included in the certificate.

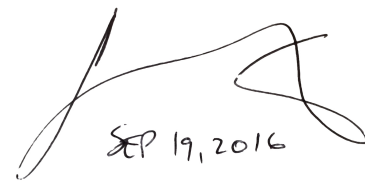
TrustCor CA will check that any domain name requested is a valid one, using the ICANN public suffix lists sourced from any reliable data source.

Any applicants known to have made fraudulent applications, or had certificates revoked because of fraudulent behaviour will have their identities stored in TrustCor CA's database; this database will be consulted prior to processing continuing after identity checking.

4.2.2 Approval or rejection of certificate applications

TrustCor CA must reject any application where the accompanying evidence of identity does not meet the standards laid down in Section 4.1.2. If further third party processing cannot attest to the identity asserted by the application, TrustCor CA must reject the application.

TrustCor CA is not under any obligation to provide a reason for rejection of an application, and may choose to do so for any reason whatsoever.



SEP 19, 2016

4.2.3 Time to process certificate applications

TrustCor CA will ensure that all applications are completed (either successfully or not) within 30 days of the first request. The result of this application will be communicated to the requestor using such contact details as were provided in the application.

The CPS shall state more detailed time limits depending on which type of certificate is being requested.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The action of signing a certificate request must be done by a user expressly authorised to carry out this action. A secure and tamper evident log is required to log both the action and the principal who authorized it.

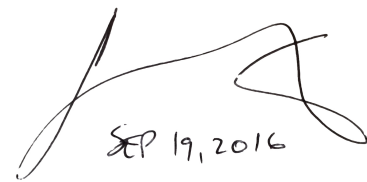
Serial numbers on certificates must not be predictable - that is they must contain sufficient entropy as to make guessing serial numbers to be computationally infeasible.

4.3.2 Notification to subscriber by the CA of issuance of certificate

TrustCor CA will send the certificate to the requestor directly, or place the certificate in a location where the certificate can be obtained and communicate that to the requestor, using the contact details supplied on certificate application.

In all cases the certificate must be sent in a standard electronic form which renders it easy to use for the requestor. Examples are PEM encoded X.509 sent within an email, or DER encoded X.509 available via URI which the user can access.

The means of communication is not stipulated, but must be done via a reliable communications protocol.



SEP 19, 2016

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The subscriber agreement requires a requestor to validate that the details present in the certificate match his or her requirements, and to notify TrustCor CA if such requirements have not been met. This notification of dissatisfaction must be performed within a reasonable time frame, and in no case may exceed 30 days.

If the certificate is placed into use, such as by fronting an SSL endpoint or being used to sign email, then the certificate is deemed to have been accepted by the requestor.

4.4.2 Publication of the certificate by the CA

End entity certificates shall not be published by TrustCor CA in a fashion which allows general searching for certificates (from non TrustCor sources). CA certificates must be published by TrustCor CA.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

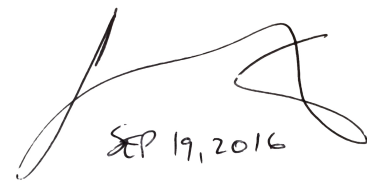
4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The subscriber is required by subscriber agreement not to release to unauthorized parties any private key corresponding to an issued certificate.

Any restrictions on how the private key may be stored (e.g. in a FIPS 140 compatible manner) must be expressed within the subscriber agreement.

The certificate may only be used for the purposes designated by the `keyUsage` and `extendedKeyUsage` flags, and consistent with any provisions within the subscriber agreement.



SEP 19, 2016

4.5.2 Relying party public key and certificate usage

RPs may only trust the certificate issued when the signing chain to a trusted Root CA has been established **and** where all certificates up to the root have been verified to be valid, by use of CRLs or OCSP responses.

TrustCor CA gives no guarantee to a relying party other than that the requestor of a certificate has provided sufficient evidence to warrant issue of a certificate bearing the identifiers presented.

4.6 Certificate renewal

Renewal means the re-issuance of a certificate with the same public key information, same identity details but with a new validity period.

4.6.1 Circumstance for certificate renewal

TrustCor CA may renew certificates when:

- the details present in the certificate have not altered
- it possesses no information that the private key has been compromised
- any stipulated public key validity has not expired
- verification of identity documentation is not required (see Section 3.3.1)

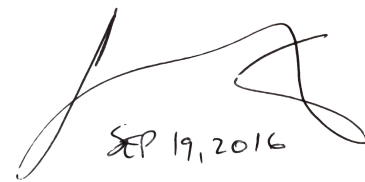
4.6.2 Who may request renewal

The requestor identified in a certificate's subject may request renewal.

Any authorized representative of the certificate subject (e.g. a domain name holder, or organizational representative) may request renewal.

4.6.3 Processing certificate renewal requests

The renewal process must be validated on the CA by the same means as issuance was granted (ie, by an authenticated and authorized principal, and the resulting action logged).



SEP 19, 2016

4.6.4 Notification of new certificate issuance to subscriber

The same communications methods satisfying Section 4.3.2 may be used to communicate the renewed certificate.

4.6.5 Conduct constituting acceptance of a renewal certificate

Since the details within the certificate do not change, the window to reject the certificate, on the grounds on unsatisfactory details in the certificate, may no longer be open to the user.

As per Section 4.4.1, demonstrated use of the certificate constitutes acceptance by performance.

4.6.6 Publication of the renewal certificate by the CA

The publication requirements are as per Section 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

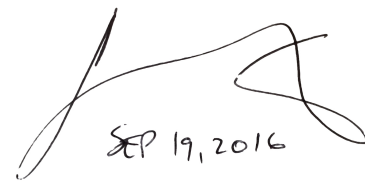
4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

If a new certificate is being requested under the same certificate program as an older one with the same details, and the identity evidence is still current, then the authentication methods in Section 3.3.1 can be used to re-key.

Otherwise a new issuance process must be undertaken.

If a re-key'ed certificate has been issued, any existing older certificates for the same subscriber may not be renewed.



SEP 19, 2016

4.7.2 Who may request certification of a new public key

The entity identified by the certificate (if a natural person) can request re-key. Otherwise a representative authorized to make certificate requests for the subject in the certificate may make a re-key request.

4.7.3 Processing certificate re-keying requests

The constraints of Section 3.3.1 obtain while processing re-key requests.

4.7.4 Notification of new certificate issuance to subscriber

The requirements of Section 4.3.2 must be met for issuance notification.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

The stipulations of Section 4.4.1 obtain for a re-keyed certificate, including the right to reject if any new details in the certificate are not to the subscriber's satisfaction.

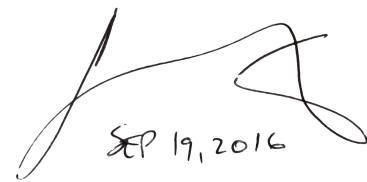
As before, demonstrated use of the certificate constitutes acceptance.

4.7.6 Publication of the re-keyed certificate by the CA

Section 4.4.2's requirements must be satisfied for re-keyed certificates.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.



SEP 19, 2016

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

TrustCor CA may be required to modify a certificate as a result of trademark dispute, court order in a competent jurisdiction, or by technical requirements changing for the handling of certificates (e.g. a critical flaw being discovered in the signing algorithm within a certificate)

TrustCor CA may only modify a certificate which lists multiple dnsNames as a subjectAltNames, such that the new set does not change any dnsName which is present as part of the subject DN.

In the case where the new dnsNames form a strict superset of the old ones, this process is equivalent to a re-key, maintaining the same public key as the old certificate. In the case where a name present in the old set of dnsNames does not appear in the new set, then the old certificate is revoked and a new one issued as per the normal certificate issuance rules: the “ongoing relationship” criterion is deemed to apply.

In the case where the principal name (ie, present in the subject DN) needs to be altered, the certificate must be revoked and a new subscriber agreement entered into, in order to publish the new certificate.

4.8.2 Who may request certificate modification

TrustCor CA may institute certificate modification.

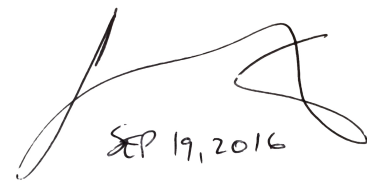
The subscriber may request certificate modification.

4.8.3 Processing certificate modification requests

The constraints of Section 3.3.1 obtain while processing modification requests.

4.8.4 Notification of new certificate issuance to subscriber

The requirements of Section 4.3.2 must be met for modification notification.



SEP 19, 2016

4.8.5 Conduct constituting acceptance of modified certificate

The stipulations of Section 4.4.1 obtain for a modified certificate, including the right to reject if any new details in the certificate are not to the subscriber's satisfaction.

As before, demonstrated use of the certificate constitutes acceptance.

4.8.6 Publication of the modified certificate by the CA

Section 4.4.2's requirements must be satisfied for modified certificates.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

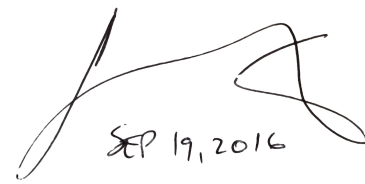
4.9 Certificate revocation and suspension

TrustCor CA will make its certificate revocations public through the use of publicly issued CRLs and publicly available OCSP responder services.

4.9.1 Circumstances for revocation

TrustCor CA will revoke certificates if:

- The subscriber makes an authenticated request that his/her certificate be revoked
- The subscriber chooses not to accept a certificate as not being satisfactory
- A certificate has been not been issued according to the policies described in this CP, or in the CPS which satisfies it.
- It is brought to TrustCor CA's attention that the private key for the certificate is no longer in the sole control of the subscriber
- The subscriber no longer has the right to assert any of the details described in the certificate, such as trade names, trademarks, association with an organization noted in the certificate, etc.



SEP 19, 2016

- TrustCor CA has received a properly issued, legally binding order to revoke a certificate from a competent legal authority
- TrustCor CA ceases operations and no successor organization has taken over its obligations
- The details present in the certificate is deemed to mislead or confuse relying parties
- The subscriber engages in behavior which is in material breach of the relevant subscriber agreement
- The subscriber appears, subsequent to issue, on a blacklist of entities or embargoed nations issued by the government of the United States of America
- The subscriber does not take delivery of the certificate within a reasonable time frame (where the certificate is delivered by request to TrustCor CA).

Since it is part of the subscriber agreement that a subscriber must notify TrustCor CA of any changes in circumstance which would prevent the details of the certificate being accurate, failure to so inform constitutes a material breach of the subscriber agreement, and thus revocation is warranted.

4.9.1.1 Reasons for Revoking a Subscriber Certificate

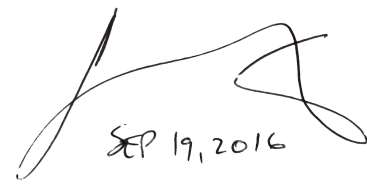
No stipulation above those in Section 4.9.1

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

In addition to the reasons in Section 4.9.1, a subordinate CA may be revoked if it is not possible for its operations to be conducted in a way which is compliant with the Baseline Requirements standards, or any other conditions imposed upon it by the subscriber agreement.

Reasons for this could be:

- loss of FIPS-140 L3 certification for the HSM holding the subordinate CA's private key.
- inability of the Subordinate CA to validate details according to the terms of this CP



SEP 19, 2016

TrustCor CA shall revoke its own CA certificates if it discovers an exploited threat to the confidentiality and/or integrity of its private key material.

4.9.2 Who can request revocation

The subscriber owning a certificate can request revocation.

An authorized representative of any organization represented in a certificate can request revocation of any certificate which contains that organizational identity.

TrustCor CA can, on its own initiative, request revocation.

Entities trusted by TrustCor CA can request revocation, including, but not limited to:

- Representatives of the various browser Root Certificate inclusion programmes
- Representatives of the CA/B Forum

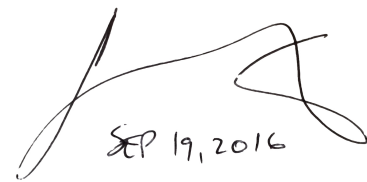
4.9.3 Procedure for revocation request

Any request for revocation must:

- Clearly identify the source of the requests
- Clearly identify the target certificate of revocation (e.g. with Issuer DN and Serial Number)
- State the reason for revocation
- State the capacity in which the requestor is operating (subscriber, organizational representative, etc.)

TrustCor CA must then authenticate the request, and record it.

Assuming the request is warranted, an agent of TrustCor CA will then have the CA software issue a revocation for the targetted certificate. This revocation is an auditable event.



SEP 19, 2016

4.9.4 Revocation request grace period

Subscribers not accepting a certificate must make their non-acceptance known to TrustCor CA within thirty (30) days of certificate issuance. Actual use of the certificate cancels this grace period.

A subscriber who loses the right to assert any of the details contained within a certificate must make this known to TrustCor CA within four (4) days.

Any end-entity key holder who detects private key compromise must make this information known to TrustCor CA within 24 hours.

Any holder of a Subordinate CA private key must make compromise known to TrustCor CA within 1 hour.

4.9.5 Time within which CA must process the revocation request

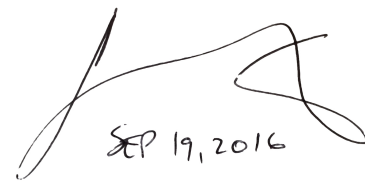
Subordinate CAs which require revocation must be processed as a matter of urgency by TrustCor CA. No more than two hours should elapse between possessing an authenticated and authorized revocation request and the request being processed. If this revocation will cause major business disruption, the TCPA must be informed immediately and a decision given on the revocation timeframe by the TCPA. This decision is binding on TrustCor CA.

For end-entity CAs, the request must be processed prior to the next scheduled release of the CRL for the issuing CA. Under no circumstances should a revocation request take longer than twenty-four (24) hours to process.

4.9.6 Revocation checking requirement for relying parties

A certificate issued by TrustCor CA can **not** be considered trustworthy unless all certificates in the chain (excluding the trusted root) are checked against current CRLs or OCSP responses.

If no such validation information can be obtained, the certificate should not be relied upon by the RP.



SEP 19, 2016

4.9.7 CRL issuance frequency (if applicable)

Subordinate CAs which issue end entity certificates must issue CRLs at least every twenty-four (24) hours.

Offline Root CAs which issue subordinate CA certificates must issue CRLs at least every six (6) months.

The normal issuance period does not relieve TrustCor CA of the burden to produce CRLs in a timely manner as per Section 4.9.5.

4.9.8 Maximum latency for CRLs (if applicable)

Each CRLs must be published at least ten (10) minutes before the nextUpdate field on the previous CRL for the issuing CA.

4.9.9 On-line revocation/status checking availability

TrustCor CA shall provide OCSP servers configured in a high availability mode such that the uptime guarantees of Section 2.1 can be met. Every certificate apart from a Root CA certificate shall be able to be validated in an OCSP via a URI published within the certificate.

4.9.10 On-line revocation checking requirements

RPs must have OCSP client software which adheres to RFC2560 specifications in order to use the OCSP services.

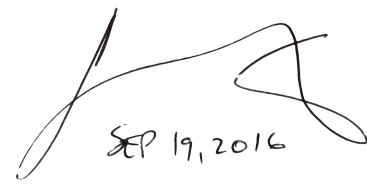
4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

In the event that TrustCor CA discovers that private keys under its ownership have become compromised, TrustCor CA shall make all reasonable efforts to

communicate this information to any Relying Parties as well as those contacts within browser root certificate programmes to which TrustCor CA is a member.



SEP 19, 2016

4.9.13 Circumstances for suspension

TrustCor CA does not suspend certificates, therefore this part of the CP is not applicable.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

CRLs and OCSP responders will list revocation status for all certificates currently in a revoked state until the certificates expiry period has elapsed. After the publication of a subsequent CRL, the serial number of the certificate may be removed from the published CRL.

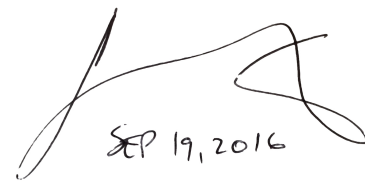
OCSP services may also reflect this archive cutoff in their responses.

4.10.2 Service availability

TrustCor CA is required to provide a globally available OCSP and CRL service availability at all times, with outages constrained to be within the limits expressed in Section 2.1

4.10.3 Optional features

No stipulation.



SEP 19, 2016

4.11 End of subscription

Subscriber agreements terminate upon revocation of a certificate, unless the subscriber elects to request new certificates under the same subscription agreement.

4.12 Key escrow and recovery

TrustCor CA shall not escrow private key information in its possession, nor shall it operate key escrow services for subscribers.

Enterprise Subordinate CAs must not be permitted per their subscriber agreements to escrow 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.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

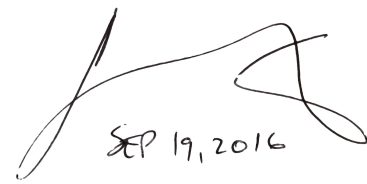
5.1 Physical controls

5.1.1 Site location and construction

TrustCor CA sites its operations within secure data centers exhibiting the following features:

- Not located in areas likely to exhibit hazard of environmental damage, chemical, biological or radiological pollution
- Possessed of redundant stable electricity supplies from at least two separate providers
- Physically separated areas for visitor reception, clearance and computer equipment hosting

- Capable of safely storing, separate to any computer equipment, fuel to power facilities in the event of loss of mains power



SEP 19, 2016

5.1.2 Physical access

TrustCor CA shall ensure that its CA and RA services are hosted within data centers which limit physical access using at least the criteria:

- A log in durable form is kept of every visitor to the facility listing their affiliation, name, purpose of visit and area of visit
- Segmented physical access which limits the ingress and egress of visitors to site equipment through manned checkpoints
- Closed circuit video surveillance equipment, operating 24x7, recording all areas around and within the data center.
- Security personnel stationed on-site with sufficient training to recognize, alert and/or escalate in the event of unauthorized attempts to gain access to the facility.
- Policies in place to prevent single person access to any areas where CA and RA facilities are maintained.

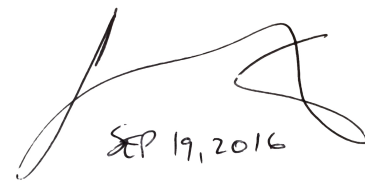
In addition to this, TrustCor CA must station its CA and RA equipment in locked cabinets, where the keys are securely stored on site facilities, separate from the cabinets themselves, under the supervision of trained site security personnel.

TrustCor CA shall ensure that the cabinets have live video feeds covering the front and rear of the cabinets. Those video feeds shall be viewable from remote computers under the control of TrustCor CA. Such feeds must limit viewing of their content to authenticated principals.

5.1.3 Power and air conditioning

Any data center housing TrustCor CA services must have:

- A filtered mains power supply



SEP 19, 2016

- Auxiliary generators capable of sustaining all TrustCor CA computer systems in the event of mains power failure
- Sufficient local storage of fuel capable of transitioning the data center to auxiliary supply
- In place contractual agreements to deliver fuel to the data center on an ongoing basis in the event of prolonged unavailability of mains power supply
- A UPS system in place providing power to every cabinet hosting TrustCor CA equipment
- A regular testing schedule to ensure proper operation of emergency power supply systems

Air conditioning facilities must be present at all sites, and emergency power supplies sufficient to maintain their operation in the event of main power outage.

Secure telecommunications systems must also exist in the facility. Such communications systems must not depend on mains power to operate.

5.1.4 Water exposures

Data center policies should prevent the taking of food and drink into the facility.

In any case, no-one shall be permitted to visit TrustCor CA equipment carrying liquid which could spill onto the equipment.

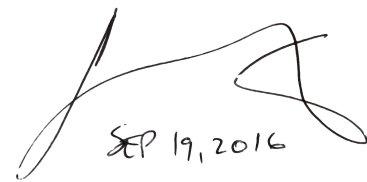
Cabinets hosting TrustCor CA equipment must be sealed at the top to prevent water exposure from potential leaks or drips. Louvres on cabinet doors must prevent drips from entering the cabinet.

5.1.5 Fire prevention and protection

The data center provide regularly tested, reliable fire suppression systems

5.1.6 Media storage

All logs, databases and audit information collected on one site must be securely and regularly transferred to off-site facilities, also owned by TrustCor CA. Such information is deemed company sensitive, and must be encrypted whilst in transit to prevent unauthorized access.



SEP 19, 2016

5.1.7 Waste disposal

Any paper which has been generated from Trustcor CA equipment must be permanently destroyed according to standard business practices.

Any storage devices being retired from TrustCor CA equipment must be securely destroyed either using on-site data destruction equipment, or as soon as practical thereafter. Such devices must be rendered into a state which puts their contents permanently beyond use (e.g angle-grinding, crushing, etc.)

5.1.8 Off-site backup

Backups of system data shall be taken daily and transferred to at least 2 geographically distinct locations. No backup location may be located in the same data centre as TrustCor CA equipment.

Backups are deemed company sensitive information and must be encrypted during transit.

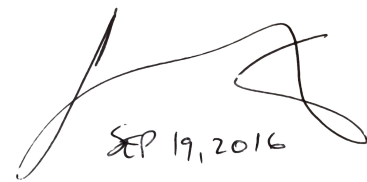
5.2 Procedural controls

5.2.1 Trusted roles

The following abilities are deemed to be trusted roles:

- The ability to issue certificates from subordinate CAs
- The ability to revoke subordinate CA certificates
- The ability to validate an applicant's certificate request
- The ability to configure or deploy computer systems or networking equipment under TrustCor CA's ownership into a production mode
- The ability to admit new personnel into TrustCor CA's employ
- The ability to collate TrustCor log telemetry for audit purposes

Trusted role personnel must have binding contracts of engagement with TrustCor CA, be vetted such that the TCPA does not doubt their trustworthiness and provide such proofs of identity to TrustCor CA (prior to engagement) as gives TrustCor CA confidence that the person engaged can assert that identity.



SEP 19, 2016

The following abilities are deemed to be highly trusted roles:

- The ability to cause the root certificate key store to sign a certificate request
- The ability to cause the root certificate key store to sign a CRL
- The ability to transfer an HSM stored private key to another HSM
- The ability to physically access the equipment of TrustCor CA

Those personnel executing highly trusted roles must, of course, have the trust level to perform trusted roles. At least one person occupying a highly trusted role must be a registered officer of TrustCor CA.

5.2.2 Number of persons required per task

Operations which require a trusted role may be performed by one person.

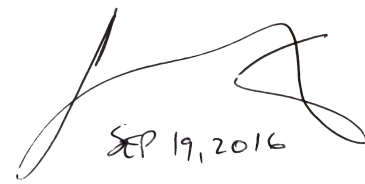
Operations which are highly trusted require two people to conduct the operation, and the operation must be designed in such a way as to make the conduct of one operator visible to the other. Under no circumstances may a highly trusted operation be delegated to a purely automated system: two human beings must perform the operation.

5.2.3 Identification and authentication for each role

Any CA operations require individual authentication using management issued credentials to perform the operation. Generic administrative users accounts **must not** be used for such purposes. The logs must show which actual principal performed the operation.

5.2.4 Roles requiring separation of duties

Every person in TrustCor CA's employ who is authorized to perform duties within a trusted role shall be given such credentials as allows them to act in exactly one of the roles listed in Section 5.2.1. The person having the audit role may not be in possession of credentials allowing him or her to act in any other role.



SEP 19, 2016

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

TrustCor CA shall ensure that, prior to engagement in any trusted role, a person has the qualifications and necessary experience to perform such duties.

TrustCor CA shall ensure that no person engaged has any conflict of interest which would pose a threat to TrustCor's operations.

No person appearing on a prohibited list of persons, or affiliated to any proscribed organization, issued by the government of the United States of America may be engaged into any role on behalf of TrustCor CA.

5.3.2 Background check procedures

TrustCor CA shall verify the identity of any potential employee or contractor prior to engagement, using an approved government issued photo identification.

TrustCor CA shall validate that the person has no declarable criminal record prior to engagement (notwithstanding the existence of appropriate laws regarding rehabilitation of offenders).

TrustCor CA shall check the residences of the potential employee covering a period of five years.

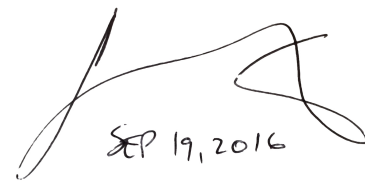
Prior to engagement, the highest educational qualification claimed shall be verified by TrustCor CA.

The TCPA will then decide as to whether the person can be admitted to various trusted roles depending on the outcome of the previous checks.

5.3.3 Training requirements

Each person engaged in CA operations must be trained in, at minimum:

- Knowledge of basic computer security



SEP 19, 2016

- Knowledge of TrustCor CA's system software
- Common identity fraud methods and their detection
- Verification of identity information for individuals and organizations
- Generic CA and RA operating principles
- TrustCor CA's business goals and partnerships

The receiver and level of training is recorded for every person in TrustCor CA's internal knowledge base. No person may be admitted to any role without at least some covering documentation detailing either:

- the formal training received
- the relevant experience being relied upon instead of formal training

5.3.4 Retraining frequency and requirements

All persons in CA operations are expected to be familiar with the directions proposed by industry bodies such as the CA/B Forum. If the TCPA deems that new training is required for any personnel as a result of actual or likely changes in CA/RA behavior, TrustCor CA shall provide that training and document in the internal knowledge base accordingly.

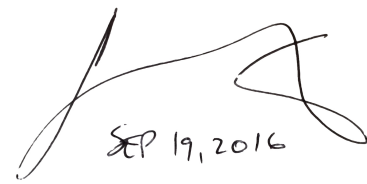
5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

All persons operating under TrustCor CA's employ must be made aware that unauthorized activities can attract different grades of sanction, including, but not limited to:

- Removal of privileges and demotion of job grade
- Diminution of compensation received
- Termination of employment
- Recovery of losses by legal action
- Reporting to law enforcement officials for possible criminal sanctions



SEP 19, 2016

If unauthorized activity is suspected by TrustCor CA, the person under suspicion will have their relevant credentials revoked while the matter is investigated. If no unauthorized activity is deemed to have taken place, new credentials will be issued.

5.3.7 Independent contractor requirements

While contractors are not directly employed by TrustCor CA, they are under the same obligations for background checking, training and conduct as documented above for employees. The sanctions for contractors can include termination of contract instead of termination of employment.

5.3.8 Documentation supplied to personnel

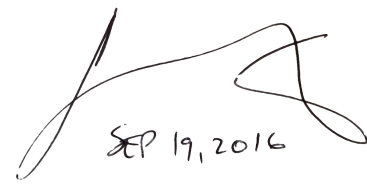
TrustCor CA shall provide all such documentation to its personnel as is needed to perform their duties.

5.4 Audit logging procedures

5.4.1 Types of events recorded

Auditable events are divided into several categories and described below:

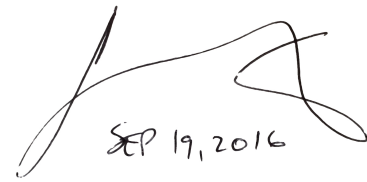
- Host Level Events
 - Deployment of a new host
 - Reconfiguration of a host software via configuration management system
 - Addition of a user account to a host
 - Removal of a user account to a host
 - Modification of user authentication/ authorization data
 - Patching of system level software to a new version
 - Reboot of a host
 - Host level firewall rule changes
 - Detection of modification of system binaries (programs, libraries, etc)
 - Detection of modification of application configuration files
 - Connection/disconnection of a device to a host level bus
 - Restoration from a backup of a host
 - Host clock synchronisation



SEP 19, 2016

- Commissioning/decommissioning of host hardware
- Audit subsystem failure
- Log file shrinkage (not caused by normal log rotation)
- Log archiving
- Network Level Events
 - Firewall rule changes
 - Anomaly detection
 - Commissioning/decommissioning of firewall/switch hardware
- Certificate Authority Internal Events
 - Addition of a new CA management principal
 - Authentication of a principal to the CA software
 - Modification of an authorization profile
 - Alteration of a principal's profile assignment
 - Addition, alteration or deletion of an end-entity
 - Modification of the validity period of a CRL
 - Modification of the validity period of OCSP responses
 - Snapshotting the CA software database
 - Restoration of the CA software database from a snapshot
- Certificate Authority Publishing Events
 - Generation of a certificate
 - Generation of CRL/OCSP data
 - Publication of CRLs/certificates to online repositories
- Key Storage Events
 - Partition of an HSM
 - Import of a private key to an HSM
 - Export of a private key to another HSM
 - Signing data via a private key stored in an HSM
 - Decrypting data via a private key stored in an HSM
 - Transfer of an HSM from one site to another
 - Zeroizing an HSM
 - Recovering a split secret from multiple shares
- Site Events
 - Scheduling of a visit to site
 - Arrival at site for scheduled visit
 - Unauthorized access attempt to site
 - Opening of a CA/RA equipment cabinet

- Power failure (Mains/Generator/UPS) at site
- Operational Events
 - Admission of a new hire into TrustCor CA
 - Existing personnel leaving TrustCor CA
 - Revocation of credentials pending investigation



SEP 19, 2016

5.4.2 Frequency of processing log

Internal log auditing is performed quarterly. Anomalies, suspicions of loss of confidentiality or integrity are documented and treated as actionable events for TrustCor CA personnel.

Events deemed to be security sensitive and will automatically generate action items via security incident reporting software.

5.4.3 Retention period for audit log

Logs must be maintained on each system for at least 3 months, when they can be reviewed.

5.4.4 Protection of audit log

Except where strictly necessary for system administrative purposes, log services are read-only for users. Intruder detection systems are configured to report log file shrinkage.

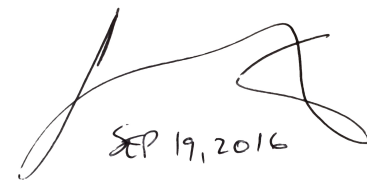
Auditors are capable of examining any of TrustCor CA's logs upon demand.

5.4.5 Audit log backup procedures

System and CA software logs are saved and stored offsite daily; the information within is deemed sensitive and must be encrypted in transit, and the end point for the transfer must be cryptographically authenticated.

5.4.6 Audit collection system (internal vs. external)

Automated audit logs must send their telemetry to a central logging system, configured in a high availability mode. If a node is no longer sending reports to the central logs, it becomes suspect, and the TCPA shall



SEP 19, 2016

determine whether it must be withdrawn from service or whether the system can be rebooted in order to restart the audit subsystem.

External auditors are given either live (read-only) access to log systems or are given the logs themselves, as the auditor demands.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

TrustCor CA operational personnel shall receive updates on discoveries of software vulnerabilities, and ensure that each system can report on whether any security related updated is applicable to it.

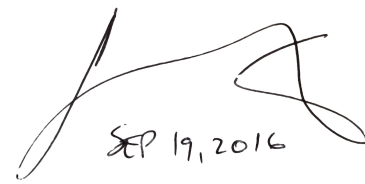
Security related updates are regarded as mandatory unless a specific case can be made for not updating the targetted software. Such an exception must be documented and approved by the TCPA.

Based on CVE scoring metrics, or the scoring of the producer of the update, an update will be rated as mitigating vulnerabilities classed as:

- Low Risk
- Medium Risk
- High Risk
- Critical Risk

If an update is rated as critical, it must be deployed with TrustCor CA test systems within 24 hours of publication, and then on production platforms (assuming the test systems show no evidence of breakage) within at most 72 hours of publication. The update shall be performed via an emergency change order.

If an update is rated as high, it must be deployed with TrustCor CA test systems within 48 hours of publication, followed by production deployment within 5 days of publication. The update shall generate an emergency change order.



SEP 19, 2016

Low or medium risks must be deployed with on test equipment within 1 week of publication of update; followed by deployment to production equipment on a normal monthly schedule. This update will be performed via a normal change order.

Annually, the TCPA will conduct a security review of its policies and security posture, with a view to altering the security policy of the company.

5.5 Records archival

Legally mandated record retention will be conducted only as required by competent authorities with respect to TrustCor CA's areas of operations.

5.5.1 Types of records archived

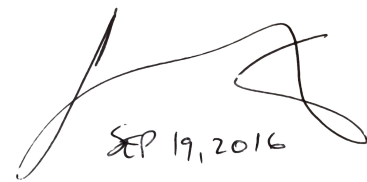
Records archived will include:

- 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
- All certificates issued by TrustCor CA
- The records of validation and certificate issuance
- All CRLs issued by TrustCor CA
- Reports of auditors generated for compliance purposes
- All security incident reports and their resolutions (this includes detected policy violations of CP/CPS documents)
- Changes to the configuration of HSMs

5.5.2 Retention period for archive

TrustCor CA shall retain archives for any record for seven years after the record has ceased to be valid (e.g. after the expiry of a certificate, a CRL, etc.)

For certificate data, verification documentation is deemed to have a validity period the same as any certificate which arose from that documentation.



SEP 19, 2016

5.5.3 Protection of archive

Archives are stored in an off-site location on a durable medium which does not allow modification. Archives may also be stored on the system of generation of the archive data, and normal user accounts are configured to have no capability to modify or destroy archive data.

5.5.4 Archive backup procedures

Archive packaging and transfer methods must be described in TrustCor CA's CPS.

5.5.5 Requirements for time-stamping of records

All systems producing archive data are required to synchronize their internal clocks at least every eight hours, to a recognized UTC(k) participating laboratory, or reliable national standards institution which produces timestamp data.

If a host is a virtual machine, it is permitted to use the hypervisor's clock, on the understanding that the hypervisor synchronizes its clock using the method above.

5.5.6 Archive collection system (internal or external)

Archive data shall be collected by TrustCor CA.

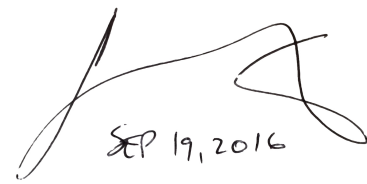
5.5.7 Procedures to obtain and verify archive information

TrustCor CA will not divulge archive information to any external party except as follows:

- where a competent legal authority presents a properly formed instrument compelling the release of archive data
- where an audit requires archive data in order to complete a compliance report

Where archive data is electronically generated, archive generating systems shall use integrity codes to establish that the archive data has not been altered. Document

control systems shall also use integrity coding to ensure that changes to documents can be checked as being valid.



SEP 19, 2016

5.6 Key changeover

Prior to the end of a private key's validity period, TrustCor CA shall generate (and document) new CA keys and certificates to be used to sign new certificates. From point of issuance onwards, a replaced private key/certificate cannot be used to sign new certificate requests. The replaced certificate shall still be retained and published until its last subordinate certificate has expired.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

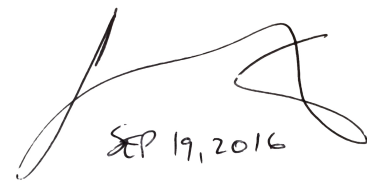
TrustCor CA must have processes in place which detect unauthorized entry and or modification of systems in its domain. ITIL processes regarding security incident reports must be followed, including categorization, assignment, resolution and verification steps.

TrustCor CA must have a business continuity plan and a stated security policy governing the operations and responses to security events.

5.7.2 Computing resources, software, and/or data are corrupted

Computing hosts must be provisioned via well established configuration management solutions such that core functionality can be restored in the event of corruption.

Databases must be backed up and stored off-site from the platform such that they can be restored quickly in the event of damage. "Quickly" in this instance means that the availability constraints of Section 2.1 must be met.



SEP 19, 2016

Private Keys must be backed up and stored on hardware equivalent in security to the primary store. It is expected that every HSM has a twin unit maintained as a warm standby, able to take over the role of the primary in the event of corruption.

5.7.3 Entity private key compromise procedures

Since TrustCor CA does not generate or hold private key data for end-entities, this section only pertains to CA keys held by TrustCor CA.

If a subordinate CA is discovered to have a compromised key, TrustCor CA must revoke the certificate as described in Section 4.9.5 and proceed with notification described in Section 4.9.12.

5.7.4 Business continuity capabilities after a disaster

TrustCor CA is required to have a business continuity plan outlining recover scenarios for:

- the loss of the database used by the CA software
- the loss of the hardware hosting CA software
- the loss of the cabinets hosting all the CA software at a site
- the loss of an entire site

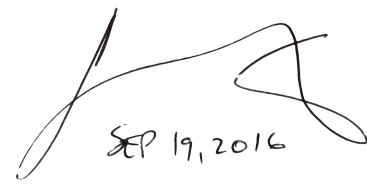
The result of the BCP should be that the constraints on availability detailed in Section 2.1 are maintained. In the event that the disaster is such that the availability can no longer be met, TrustCor CA must make all reasonable efforts to notify any RPs of the disruption of service.

That notification must contain a statement of TrustCor CA's level of confidence regarding both the likelihood and timeframe for restoration of service. It must also state TrustCor CA's belief regarding the continued integrity of its CA offerings - especially the state of its private keys and the HSMs storing them.

Further notification must be made to:

- The operators of any browser root certificate programmes

- The CA/B Forum



SEP 19, 2016

5.8 CA or RA termination

In the event that TrustCor CA ceases operations, notification to interested parties as detailed in Section 5.7.4; if a successor organization is found then TrustCor CA must provide it with all details as are needed to maintain trusted status with the browser root certificate programmes and any other entities with which TrustCor CA has established a trusted relationship.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA Key Pair Generation

CA private keys must be only be generated on HSMs rated to FIP-140 L3 or EAL 4 or higher.

A written, signed, script of commissioning for any Root CA certificate must be made and archived. This record must show evidence of multi-person involvement regarding generation, installation and validation of the script.

6.1.1.2 Subscriber Key Pair Generation

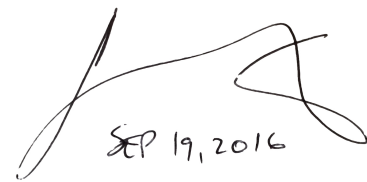
TrustCor does not generate private key materials for subscribers.

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 in a standard format and transferred over a medium which is reliable and secure. The delivery of the public key must be authenticated so as to provide confidence that it issues from the subscriber.



SEP 19, 2016

6.1.4 CA public key delivery to relying parties

TrustCor CA delivers its own public key CA certificates to RPs by:

- inclusion in a browser root certificate programme
- the provision of a CA URI within the end entity certificate which yields the signing CA certificate.

6.1.5 Key sizes

The minimum RSA modulus size used for TrustCor CA keys is 2048 bits.

The minimum ECDSA key size used for TrustCor CA keys is 384 bits.

The minimum hash used for any certificate embedded signature is SHA-256, although SHA-512 is also rated as acceptable. OCSP responses may respond using the SHA-1 hash if the request used SHA-1, but must support a minimum of SHA-256 or better.

End entity certificates must be a minimum of 2048 bit RSA/DSA/DH key size, or 224 bit elliptic curve size. TrustCor CA reserves the right to increase those minima as its business needs dictate.

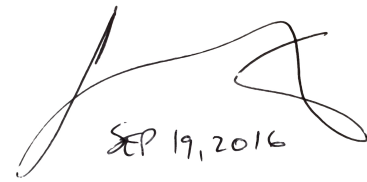
Transmission of information over secure channels must use TLS v1.2 with a symmetric session key of AES-128, or any longer key size which uses the AES cipher. Alternatively, SSHv2 may be used to transmit information, again on the assumption that the session key used is at least of AES-128 strength.

6.1.6 Public key parameters generation and quality checking

Any software deployed by TrustCor CA shall enforce the mandates of BR (v1.3.0) 6.1.6 regarding public key parameters generation. TrustCor CA must not sign any certificate request which contains known weak keys.

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

CA certificates must contain only the key usage identifiers for certificate signing and CRL signing.



SEP 19, 2016

CA certificates are not to be used for generating OCSP responses. Dedicated OCSP responder certificates must contain only digital signature key usage, with an extended key usage containing the OCSP signing purpose. OCSP responder certificates must also contain the id-pkix-ocsp-nocheck extension.

S/MIME end entity certificates may contain the key usage purposes of digital signature and key encipherment, with an extended key usage of email protection.

TLS server certificates may contain key usages of digital signature and key encipherment, with extended key usages of TLS client and TLS server.

TLS client certificates may contain key usages of digital signature and key encipherment, with extended key usages of TLS client.

A certificate may not be issued for both S/MIME and TLS purposes.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

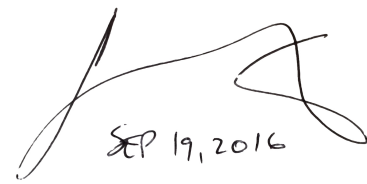
6.2.1 Cryptographic module standards and controls

Any CA run at or under TrustCor CA's Root CA certificates must store their private keys in hardware modules which are validated as satisfying the requirements of FIPS-140 Level 3, or Common Criteria for Information Technology Security Evaluation Assurance Level (EAL) 4 or above.

For each end entity certificate issued by TrustCor CA, the minimum subscriber private key storage profile is described as:

- Level 1 - No stipulation

- Level 2 - FIPS 140 Level 1 (Hardware or Software)



SEP 19, 2016

6.2.2 Private key (n out of m) multi-person control

TrustCor CA shall ensure that any activity which requires direct access to the HSM stored keys (for example, introducing a new key, or exporting keys for backup) requires at least two trusted persons to conduct the activity.

Recovery keys for rare operations (for example root database passwords, or non-individual administration keys) may be split using any secret sharing algorithm with security properties at least equivalent to the Shamir secret sharing scheme, where the workload of establishing the secret remains the same until a threshold number of shares are gathered together.

Such split keys must have their secrets then encrypted under a individual shareholder's certificate before distribution. Under no circumstances can one person be allowed to reconstruct a split secret. Recovering a split secret is an auditable event.

6.2.3 Private key escrow

TrustCor CA does not escrow its private keys, and does not allow any subordinate CA to escrow its keys.

6.2.4 Private key backup

All CA private keys are backed up to a device which has at least the same system protections as the originating device (See Section 6.2.1)

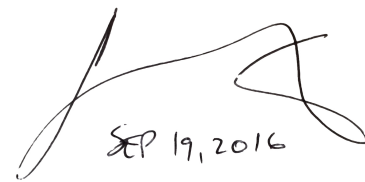
TrustCor does not back up, store or generate subscriber private keys.

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

All CA keys must be generated by, and stored in a cryptographic module as per Section 6.2.1. Export (for key backup procedures) may only be done using an



SEP 19, 2016

encrypted transfer to another cryptographic module providing the same guarantees of security. The exported data for transfer must be encrypted in such a way as to protect the private key from exposure.

No plain text private key data may ever leave any cryptographic module.

6.2.7 Private key storage on cryptographic module

All CA keys are stored on HSMs rated to least FIPS 140-L3 or EAL 4.

6.2.8 Method of activating private key

CA Private Keys may only be activated using the protocols defined by the HSM manufacturer. Authentication to the HSM must be required to activate a private key for signing purposes.

Subscriber private keys are in the control of subscribers and TrustCor CA makes no stipulation beyond the requirements of any applicable subscriber agreement regarding protection of private key material.

6.2.9 Method of deactivating private key

When not required for actual immediate need, the private key storage module must be set to be offline. It must not be possible for the private key store to be reactivated without authentication to the HSM.

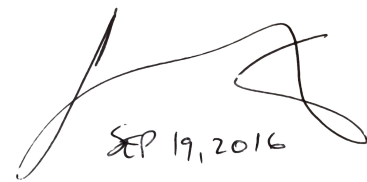
6.2.10 Method of destroying private key

Private keys which are no longer in use (because their relevant certificate has expired, or been revoked) shall be destroyed and this destruction noted in an audit log.

Keys which are stored in the HSM must be zeroized using the HSM manufacturer's instructions.

6.2.11 Cryptographic Module Rating

See Section 6.2.1



SEP 19, 2016

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public keys, in the form of certificates and certificate requests shall be archived as per Section 5.5.1

6.3.2 Certificate operational periods and key pair usage periods

The certificate and key validity period of the TrustCor CA keys are at most:

- Root CA: 15 years
- Subordinate CA: 15 years (may not live longer than the Root CA cert)
- Level 1 end-entity certificate: 1 year (12 months)
- Level 2 end-entity certificate: 2 years (24 months)
- OCSP responder certificate: 2 years (24 months)
- External Subordinate CA: 3 years (36 months)

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

6.4 Activation data

6.4.1 Activation data generation and installation

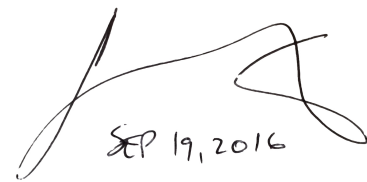
For CA keys, all private keys must have activation data associated with them. That activation data must be entered via trusted devices registered with the HSM.

6.4.2 Activation data protection

Any activation data must be securely communicated to the trusted personnel registered to possess it via trusted courier methods.

The channel used for communication must be such that no unauthorized person could obtain the activation data without outlay of sufficient resources as to be beyond the value of the private key itself.

Neither the sender nor receive of private key activation codes may be the same person who knows the credentials which bring the HSM online.



SEP 19, 2016

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

As per the TrustCor CA security policy, each computer is assigned a zone (high, medium and normal). Certificate issuing systems are considered high security devices. Systems hosting OCSP services and published CRLs are deemed to be medium security devices.

No person capable of administering a high security device may log into it without using multi-factor authentication.

No person capable of issuing a certificate may authenticate without using multi-factor authentication.

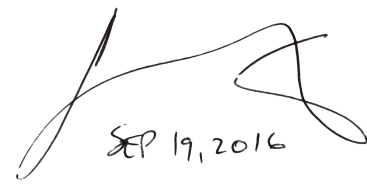
All high security devices shall lock out accounts after observing five (5) unsuccessful attempts and generate a security incident report following this lockout.

All high and medium security devices must limit the ability to obtain elevated privileges to the minimum such that any principal can perform his/her/its duties. The obtaining of elevated privileges is an auditable event.

All computers under TrustCor CAs control must be registered in its CMDB, and be configured and administered under its automated configuration management systems. All high and medium rated systems must be configured to deploy the intruder detection systems which feed a centralised incident reporting system. The logs of that incident reporting system form part of the archive data set.

6.5.2 Computer security rating

No stipulation.



SEP 19, 2016

6.6 Life cycle technical controls

6.6.1 System development controls

If any software is developed in-house, that software must undergo review by the TCPA prior to deployment in production stage equipment. The authors of any custom developed software must be made known to TrustCor CA, and their credentials to generate such software established to the satisfaction of the TCPA.

The TCPA is solely authorized to approve the deployment of any software into production equipment.

All systems in a high or medium security zone must be periodically scanned for malicious software and the results of that scan published to a central security incident logging system.

6.6.2 Security management controls

Security management is detailed in the TrustCor CA security policy document, but the central points relevant to CA operations are mentioned here.

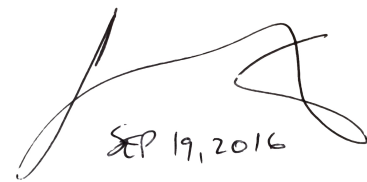
Configuration changes to production systems may only be performed using the configuration management systems approved by the TCPA.

All high and medium security systems must deploy intruder detection software capable of detecting the modification of any binary files in common system locations, or application configuration files. Such modification shall form a security incident report filed via the central monitoring system.

All changes to the configuration management database must be logged with the change data itself and the author and date of change. Any change to the database must be able to be reviewed prior to deployment, or if necessary, reverted by TrustCor CA personnel.

6.6.3 Life cycle security controls

No stipulation.



SEP 19, 2016

6.7 Network security controls

Changes to network configuration policy must go through the same configuration management changes as host devices, and be similarly documented, reviewed and approved.

No TrustCor CA system may be connected to the public internet without going through a TrustCor CA firewall, configured and run as per the TrustCor CA security policy.

No high security system may yield service to arbitrary IP addresses: sufficient controls must exist to either authenticate each connection by cryptographic means, or serve only a whitelist of TCPA approved IP addresses.

6.8 Time-stamping

All clocks in TrustCor CA systems are synchronized to known reliable time service providers, and must log all clock adjustments.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

7.1.1 Version number(s)

TrustCor CA issues X.509 version 3 certificates.

7.1.2 Certificate extensions

Such extensions which are used must concur with established industry standards, most notably RFC 5280.

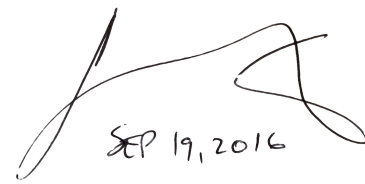
7.1.2.1 Root CA Certificate

Root Certificates must contain the following extensions:

- Basic Constraints: CA = True, set critical
- Key Usage: keyCertSign, cRLSign

The subject of the certificate must contain the following fields in addition to its Subject DN CN field:

- O [Organization] = TrustCor Systems S. de R.L.
- L [Location] = Panama City



SEP 19, 2016

- ST [State] = Panama
- C [Country] = PA

7.1.2.2 Subordinate CA Certificate

Subordinate Certificates must contain the following extensions:

- Basic Constraints: CA = True, set critical
- Key Usage: keyCertSign, cRLSign
- Authority Information Access:
 - CA Issuers: URI: <http://www.trustcor.ca/certs/{path to issuing CA certificate}>
 - OCSP: <http://ocsp.trustcor.ca/{path to relevant OCSP service}>
- CRL Distribution Points:
 - URI: <http://crl.trustcor.ca/{path to relevant CRL}>

The subject of the certificate must contain the following fields in addition to its Subject DN CN field:

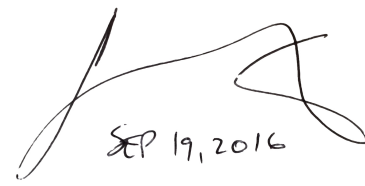
- O [Organization] = TrustCor Systems S. de R.L.
- L [Location] = Panama City
- ST [State] = Panama
- C [Country] = PA

Name constraints are not present in TrustCor CA operated subordinate CAs, but may be present in externally operated subordinate CAs, as prescribed by their individual subscriber agreements.

7.1.2.3 Subscriber Certificate

All subscriber end-entity certificates contain the following extensions

- Basic Constraints: CA = False, set critical
- Certificate Policies:
 - id-qt 1:cPSuri: <http://www.trustcorsystems.com/resources/cps.pdf>
- Authority Information Access:
 - CA Issuers: URI: <http://www.trustcor.ca/certs/{path to issuing CA certificate}>
 - OCSP: <http://ocsp.trustcor.ca/{path to relevant OCSP service}>



SEP 19, 2016

- CRL Distribution Points:
 - URI: `http://crl.trustcor.ca/{path to relevant CRL}`

For S/MIME certificates:

- `keyUsage`: `digitalSignature`, `keyEncipherment`
- `extendedKeyUsage`: `emailProtection`
- `subjectAltName`: `emailAddress`: {address of subject}

For SSL Server certificates:

- `keyUsage`: `digitalSignature`, `keyEncipherment`
- `extendedKeyUsage`: `serverAuthentication`, `clientAuthentication`
- `subjectAltName`: `dnsName`: {FQDN of subject}

For SSL Client certificates:

- `keyUsage`: `digitalSignature`, `keyEncipherment`
- `extendedKeyUsage`: `clientAuthentication`
- [optionally - `subjectAltName`: `dnsName`: {FQDN of subject}]

SSL certificates may have multiple `subjectAltNames` for multiple DNS entries.

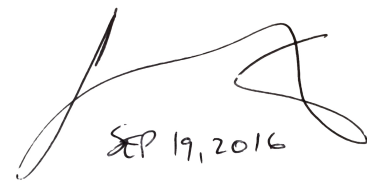
7.1.2.4 All Certificates

In addition to any specific extensions noted above, all certificates must contain X.509 extensions denoting a X509v3 subject key identifier, as well as an authority key identifier containing a keyid field.

No subject DN data shall be included which has not been verified during the application validation process.

No `subjectAltName` shall be included which has not been verified during the applicant validation process.

Given any end entity certificate, it must be possible to construct the entire chain of trust to a root certificate as well as to fetch the current validity of every certificate under the root, starting purely with the content of the end entity certificate and fetching objects (certificates/CRLs/OCSP responses) as described in the extension URIs.



SEP 19, 2016

7.1.2.5 Application of RFC 5280

Under this current CP, TrustCor CA does not issue precertificates, thus this section is not applicable.

7.1.3 Algorithm object identifiers

All CAs must sign certificates using the following algorithms:

- sha256withRSAEncryption
(1.2.840.113549.1.1.11)
- sha512withRSAEncryption
(1.2.840.113549.1.1.13)

Other algorithms (e.g. elliptic curve) may be allowed in future releases of this CP.

7.1.4 Name forms

The attributes allowable in name forms are defined in RFC 5280 and include:

- emailAddress
- commonName (CN)
- organizationalName (O)
- stateOrProvinceName (ST)
- localityName (L)
- countryName (C)

External enterprise subordinate CAs may include the organizationalUnitName (OU) in their end entity certificates subject names.

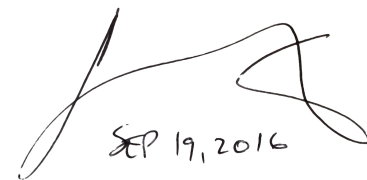
7.1.4.1 Issuing CA Certificate Subject

The Issuer DN shall in all cases match the subject DN present within the issuing certificate.

7.1.4.2 Subject Information for Standard Server Authentication certificates

For Level 1 certificates, the subject shall be entirely:

- CN={fqdn of subject}



SEP 19, 2016

For Level 2 certificates, the subject shall be entirely:

1. CN={fqdn of certificate}
2. O={validated organization name}
3. L={locality of organization's place of business}
4. ST={province name of organization's place of business}
5. C={ISO-3166-1 country code of organization's place of business}

7.1.4.3 Subject Alternative Names for Standard Server Authentication certificates

TrustCor CA will only append subjectAltNames with a dnsName tag followed by an FQDN for a domain which was validated during application. IP addresses are not to be used, and wildcard names are not to be used.

7.1.5 Name constraints

For any external enterprise subordinate CA, the CA certificate will contain a name constraint which contains the following in the permittedSubtree value:

- a dnsName for each domain which has been validated to belong to the applying organization
- a dirName which stipulates the:
 - organizationalName value
 - stateOrProvinceName
 - localityName
 - countryName

(all of the above must be set to the validated organizational details which were verified during application)

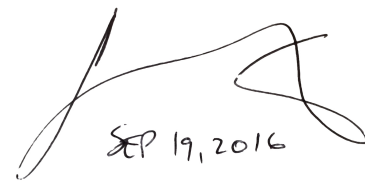
In addition to this, the name constraints contains an excludedSubtrees value of: * IP: 0.0.0.0/0.0.0.0 * IP: 0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0

to prevent issuance of ipAddress certificates.

7.1.6 Certificate policy object identifier

7.1.6.1. Reserved Certificate Policy Identifiers

Level 1 SSL client and server certificates shall contain a CPI of 2.23.140.1.2.1 (DV identifier)



SEP 19, 2016

Level 2 certificates for SSL must contain a CPI
2.23.140.1.2.2 (OV identifier)

Level 2 S/MIME certificates must contain a CPI of
2.23.140.1.2.3 (IV identifier)

7.1.6.2. Root CA Certificates

Root CA certificates do not contain any
certificatePolicies extension, therefore do not have
policy identifiers in them.

7.1.6.3 Subordinate CA Certificates

TrustCor Subordinate CA certificates shall not contain
CPIs. Enterprise Subordinate CA certificates may do so.

7.1.6.4 Subscriber Certificates

In addition to the validation OIDs noted in Section
7.1.6.1, end-entity certificates will contain the OID
beginning with 1.3.6.1.4.1.44031 to indicate the correct
version of the CPS which governs the certificate (as well
as the URI to that CPS).

7.1.7 Usage of Policy Constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

TrustCor CA may put explicit text statements in the
relevant policy extension sections of its certificates.

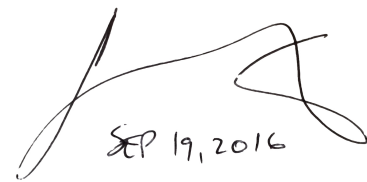
7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

7.2.1 Version number(s)

All CRLs issued will be version 2, as noted in RFC 5280.



SEP 19, 2016

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP profile

7.3.1 Version number(s)

OCSP requests and responses are at version 1, defined in RFC 2560.

7.3.2 OCSP extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The policies described in this document are designed to satisfy the requirements of the AICPA/CPA Canada WebTrust Program for Certification Authorities and the CA/B Forum's Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (BR v1.3.0).

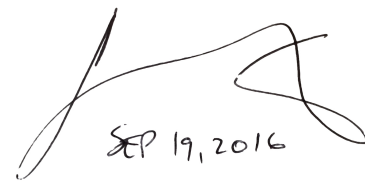
8.1 Frequency or circumstances of assessment

Audits are completed at least annually. TrustCor CA reserves the right to bring forward audits at its discretion. TrustCor CA will also conduct audits if requested to do so by trusted entities with which it has contractual relationships, including, but not limited to:

- any company operating a root certificate programme for browser of which TrustCor CA has joined
- the CA/B Forum

8.2 Identity/qualifications of assessor

Any auditor must belong to a body recognized as a part of WebTrust's licensed WebTrust practitioners (<http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx>).



SEP 19, 2016

8.3 Assessor's relationship to assessed entity

No auditor may have any financial interest in or business relationship with TrustCor CA which could create the appearance of a bias favorable towards (or unfavorably against) TrustCor CA.

8.4 Topics covered by assessment

Any audit must cover TrustCor CA's compliance with its business practices as disclosed within this CP, the attendant CPS and such other documents as TrustCor CA uses to describe its business operations and policies.

8.5 Actions taken as a result of deficiency

Where substantive deficiencies between actual performance and business description have been noted, or where the business description does not meet the compliance requirements of the standards documents in Section 8 above, the auditor must list such deficiencies and promptly notify the TCPA.

It is then incumbent upon the TCPA to devise such remediation as is necessary to address all of the auditor's findings. The plan shall then be delivered to TrustCor CA for implementation, and a post-plan re-audit shall be performed. If any notifications to contractual partners are required, TrustCor CA shall perform such actions as soon as is practical.

8.6 Communication of results

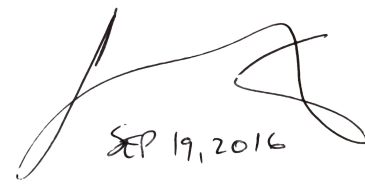
Audit results are sent to the TCPA, and will then be communicated to such third party entities as are required by law or contract to be so notified. Such parties will include WebTrust, the browser root certificate programme maintainers and possibly the CA/B Forum.

8.7 Self-Audits

TrustCor CA is required to perform regular audits of its operations, personnel (and their assignments).

TrustCor CA must also select a random sample of some three percent of its end-entity certificates (IV, DV and OV) issued since the last full audit and perform a self-audit to ensure compliance with the certificate policies

and practices in force at the time of certificate issuance. The result of this log (together with any notes regarding the likely effect of applying audit-time CP and CPS) shall be noted in the company's audit log and form part of the company archives.



SEP 19, 2016

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

TrustCor CA may charge such fees for issuance and renewal as its business offerings dictate.

9.1.2 Certificate access fees

TrustCor CA may charge such fees for access to its certificate database as its business offerings dictate.

9.1.3 Revocation or status information access fees

TrustCor CA must not charge for access to its certificate status information services.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

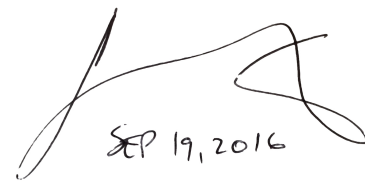
9.2 Financial responsibility

9.2.1 Insurance coverage

TrustCor CA shall have Errors and Omissions insurance for its business activities.

9.2.2 Other assets

No stipulation.



SEP 19, 2016

9.2.3 Insurance or warranty coverage for end-entities

The CPS shall denote such warranties as offered by TrustCor CA to its subscribers.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

TrustCor CA shall specify in its CPS and Security Policy documents what it considers confidential information, as well as the criteria used to reach those assessments.

9.3.2 Information not within the scope of confidential information

Any information not designated as confidential is deemed to be public information.

9.3.3 Responsibility to protect confidential information

All employees of, and contractors for, TrustCor CA are required by their contracts of engagement to preserve confidentiality of information so labelled. All employees are trained (and such training recorded) in handling of confidential information.

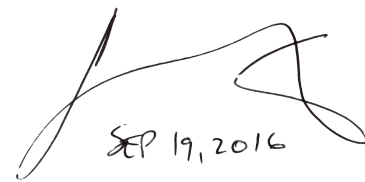
9.4 Privacy of personal information

9.4.1 Privacy plan

TrustCor shall publish and periodically review its privacy policy regarding the classification and handling of personal identifying information. That policy must be available online under the same terms as its CPS and CP documents.

9.4.2 Information treated as private

All PII which is not to appear in a certificate or CRL published by TrustCor CA is deemed to be private, and must not be disclosed except under the terms of the privacy policy.



SEP 19, 2016

9.4.3 Information not deemed private

The contents of CRLs and certificates are not private information, even if such content can identify an individual.

9.4.4 Responsibility to protect private information

TrustCor CA has a duty under its privacy policy to protect private PII from unauthorized disclosure and to ensure timely destruction of such PII when it services no business need.

9.4.5 Notice and consent to use private information

As part of a subscriber agreement, applicants must agree to TrustCor CA handling and transferring to its places of business any PII required for the issuance and maintenance of certificates.

9.4.6 Disclosure pursuant to judicial or administrative process

TrustCor CA will not disclose to any party, any PII regarding its subscribers except where compelled to do so by a competent legal authority and on production of a properly formed legal instrument which compels such release.

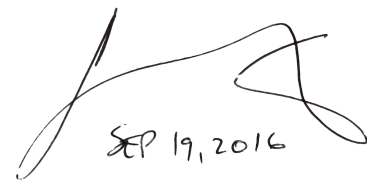
TrustCor CA reserves the right to publish the fact that it has not been compelled to disclose any subscriber information to any party, and to withdraw such notice at its sole discretion.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

TrustCor CA shall respect the intellectual property rights of any third party, and not knowingly violate the same.



SEP 19, 2016

9.6 Representations and warranties

9.6.1 CA representations and warranties

TrustCor CA is required to comply with all of the requirements imposed by this document, the attendant CPS, its security policy and privacy policy. This declaration must be made to the TCPA, any subscribers, those charged with operating a browser root certificate programme and any parties who would rely on the contents of a TrustCor CA issued certificate.

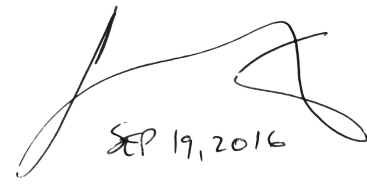
9.6.2 RA representations and warranties

Any RAs operating on behalf of TrustCor CA shall be required to stipulate that they are aware of, and follow the strictures of, this CP and its attendant CPS, together with the rules imposed by the security and privacy policy documents of TrustCor CA.

9.6.3 Subscriber representations and warranties

Any subscriber applying for a TrustCor CA issued certificate must agree (amongst other conditions dependent on the certificate application):

- that it shall generate its private keys in a secure manner
- that it shall endeavor to avoid compromise of its keys
- that any information in the certificate shall be reviewed, and that the subscriber shall not use the certificate unless it deems that information valid and as expected
- that the data provided during verification is accurate and complete
- that it shall notify TrustCor CA at the earliest opportunity should the subscriber be aware that:
 1. It no longer has the right to assert any of the details present in the issued certificate.
 2. There is a reasonable suspicion that the subscriber has lost sole control of the private key material.
- that the subscriber will only use the certificate for such purposes as the subscriber agreement allows,



SEP 19, 2016

and compliant with such law as applies to the subscriber; moreover that TrustCor CA has the right to revoke the certificate should it discover that the terms of the agreement have been violated

- that upon expiration of the certificate, the subscriber will cease using it

9.6.4 Relying party representations and warranties

RPs must use such validation processes as described elsewhere in this document for the complete validation of the certificate. If these processes are not completely followed, any reliance on the data present in a certificate is not warranted.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

TrustCor CA specifically disclaims any warranties and obligations except as stated in this document, or as limited by law.

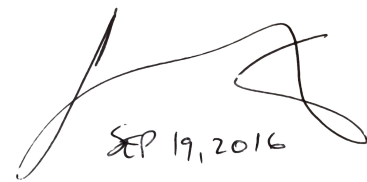
9.8 Limitations of liability

Any limitation of liability by any external subordinate CA of TrustCor CA may choose to limit its liability as it sees fit; except where such limitation violates the requirements of this CP and its attendant CPS.

9.9 Indemnities

External subordinate CAs must indemnify TrustCor CA for any violation of this CP or other requirements which they agree to in signing a subscriber agreement.

Subscriber agreements shall also contain indemnification clauses to ensure that TrustCor CA is not liable for behavior resulting from use of a subscriber's private key.



SEP 19, 2016

9.10 Term and termination

9.10.1 Term

This CP is in effect from the time of its approval and publication on the online repository; and until such time as a replacement document appears.

9.10.2 Termination

This CP holds until a replacement document terminates its effects.

9.10.3 Effect of termination and survival

Any effects resulting from the termination of this CP shall be described in the online repository. The changes to this document shall also form part of the publication such that those clauses surviving termination are apparent.

9.11 Individual notices and communications with participants

TrustCor CA will accept written communications at the address given in section 2.2.

Communications may also be made through email to such addresses are published on the online repository for TrustCor CA.

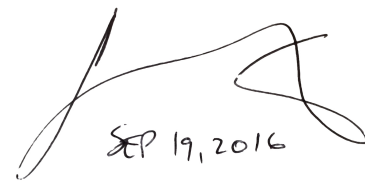
9.12 Amendments

9.12.1 Procedure for amendment

The policies for TrustCor CA (including this document) are determined by the TCPA. Changes are made to an internal document repository where they are reviewed by TCPA members, and eventually approved for release. A new version together with its changes from the old version are published on the online repository.

9.12.2 Notification mechanism and period

The contents of this CP are solely under the control of the TCPA. No notification period is required or given.



SEP 19, 2016

9.12.3 Circumstances under which OID must be changed

See Section 1.5.4

9.13 Dispute resolution provisions

Any dispute regarding the contents of this CP should be made to TrustCor CA prior to seeking third party involvement.

9.14 Governing law

The law of the Republic of Panama shall govern the interpretation of this document.

9.15 Compliance with applicable law

With regard to the PII provisions of Section 9.4.5, the requirements of the data protection regulations of the European Union regarding access, disclosure and destruction shall hold.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

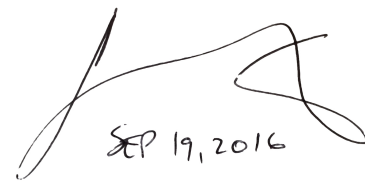
Any external subordinate CAs which have contractual agreements in place with TrustCor CA are bound to all the terms of this CP.

9.16.2 Assignment

No entity operating under this CP may assign their rights or obligations except by written permission of TrustCor CA.

9.16.3 Severability

In the event of a clause of this document being held invalid by a recognized judicial authority, the remainder of the document is still held to be valid and enforceable.

A handwritten signature in black ink is located in the top right corner of the page. Below the signature, the date "SEP 19, 2016" is written in a similar handwritten style.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

TrustCor CA shall enforce its rights and seek damages (including attorneys' fees and losses) from any party which violates the terms of any agreement with TrustCor CA. The terms of this CP are not waived by a failure to enforce all or part of them with regard to any party bound by this document (except where a waiver is granted by explicit written permission by TrustCor CA).

9.16.5 Force Majeure

TrustCor CA accepts no liability for failure to perform any obligation under the terms of this document, where such failure results from events outside TrustCor CA's reasonable control.

9.17 Other provisions

No stipulation.