

*Rachel M. Thorne*  
April 19, 2019

# TrustCor Systems S. de R.L.

## Certification Practice Statement

Version: 1.5.0

This document is PUBLIC

Generated on April 19, 2019 at 16:02 UTC.

## 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

##### 2.2.1 Notification of incorrect issuance

#### 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

###### 3.2.2.4 Validation of Domain Authorization or Control

###### 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



- 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
- 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
  - 4.9.8 Maximum latency for CRLs
  - 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

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

## 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

## 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

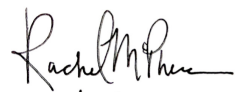
9.1.4 Fees for other services

9.1.5 Refund policy

9.2 Financial responsibility

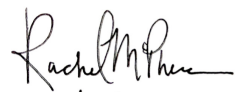
9.2.1 Insurance coverage

9.2.2 Other assets

Rachel M. P.   
April 19, 2019

- 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
  - 9.9.1 Indemnification by CAs
  - 9.9.2 Indemnification by Subscribers
  - 9.9.3 Indemnification by Relying Parties
- 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
- 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



  
April 19, 2019

## 1. INTRODUCTION

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

This document details the practices which TrustCor CA must follow in order to meet the policy specifications laid down in the TrustCor CA Certificate Policy document (CP). Accordingly this document is called the TrustCor CA Certification Practice Statement (CPS). It should also meet the disclosure and control statements required within the document "Trust Service Principles and Criteria for Certification Authorities, Version 2.0" (WebTrust CA), issued by AICPA/CICA in May 2011 (CICA now being CPA Canada since 2012).

### 1.1 Overview

This document is designed to conform with the Certificate Authority/ Browser Forum (CA/B Forum) requirements laid down in the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificate (Baseline Requirements). As of this version of the CPS, the version of the Baseline Requirements against which audit is performed is version 1.6.5 (April 16, 2019).

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

- The TrustCor CA Certificate Policy (CP)
- The TrustCor CA Privacy Policy
- The TrustCor CA Security Policy (+)
- The TrustCor Master Subscriber Agreement
- The TrustCor Terms of Use
- The TrustCor Relying Party Agreement
- Enterprise Subordinate CA Business Agreement(s) (+)

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

Those documents which are publicly available can be reached online at <http://www.trustcor.ca/resources>

### 1.2 Document name and identification

This document is version 1.5.0 of the TrustCor CA Certification Practice Statement, created and published on 2019-04-19. It carries the OID of 1.3.6.1.4.1.44031.1.1.9.

*Rachel M. Thorne*  
April 19, 2019

1.3.6.1.4.1.44031 is the root branch of the enterprise OID space allocated to TrustCor Systems S. de R.L. via <https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers>

The change record for this document relative to its predecessors is below:

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

## **1.3 PKI participants**

### **1.3.1 Certification authorities**

TrustCor CA operates three root certificates in its CA infrastructure:

- The Basic Root Certificate (CA-1) - used to ultimately be the root of trust for all certificates issued under the Basic Assurance program.  
This certificate currently signs the subordinate CAs:
  - Basic Secure Email CA (Subordinate CA1-Email)
  - Basic Secure Site CA (Subordinate CA1-Site)
  - Basic Secure Site CA [Restricted Key Size] (Subordinate CA1-Site-2048)

*Rachel M. Thorne*  
April 19, 2019

- The Enhanced Root Certificate (CA-2) - used as the root of trust for certificates issued under the Enhanced Assurance program. Currently two subordinate CA are issued under this root:
  - Enhanced Secure Email CA (Subordinate CA2-Email)
  - Enhanced Secure Site CA (Subordinate CA2-Site)
- The Enterprise Root Certificate (ECA-1) - used as the ultimate root for enterprise PKIs issuing credentials to their principals in restricted namespaces. There is one subordinate CA under this root:
  - Enterprise External PKI CA (Subordinate ECA1-External)

TrustCor CA undertakes to ensure that all operations conducted using these certificates, including registration of entities, validation of same, issuance and revocation of certificates are performed in accordance with the strictures of this document, the governing CP. Note that Enterprise Subordinate CA certificates are still TrustCor CA certificates, and TrustCor CA is responsible for their issuance, insofar as the enterprise subscriber agreements is obeyed. TrustCor CA is responsible for revoking an enterprise subordinate CA should it discover substantive violations of its enterprise agreements.

### **1.3.2 Registration authorities**

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

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

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

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

### 1.3.3 Subscribers

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

### 1.3.4 Relying parties

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

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

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

### 1.3.5 Other participants

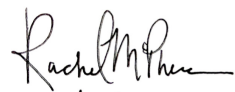
No stipulation.

## 1.4 Certificate usage

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

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

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

  
April 19, 2019

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

#### **1.4.1 Appropriate certificate uses**

The uses permitted for each certificate vary by the business offering. Because TrustCor CA has different pricing for its offerings dependent on certificate type, prospective subscribers must evaluate which type of certificate is most likely to fit their needs dependent on the type of information they wish certified and the evidence of identity which they are willing to submit to TrustCor CA.

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

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

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

The business categories are:

- Basic Secure Mail - IV, maximum 825 day validity (S/MIME)
- Basic Secure Site - DV, maximum 825 day validity (SSL)
- Enhanced Secure Mail - OV, maximum 825 day validity (S/MIME)
- Enhanced Secure Site - OV, maximum 825 day validity (SSL)
- Enterprise PKI Subordinate CA - OV, issued end-entity certificates may have a maximum lifetime of 825 days.

Note that, dependent on individual product offerings, TrustCor CA may issue certificates with shorter lifespans than the maxima described above.

## 1.4.2 Prohibited certificate uses

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

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

## 1.5 Policy administration

### 1.5.1 Organization administering the document

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

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

The TCPA can be emailed at: [legal@trustcor.ca](mailto:legal@trustcor.ca)

### 1.5.2 Contact person

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

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

### 1.5.3 Person determining CPS suitability for the policy

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

### **1.5.4 CPS approval procedures**

The TCPA will review such changes as are required to this CPS and updated CPS versioning accordingly. The version of any document has three components: Major, Minor and Micro.

As per Section 1.5.4 of the CP, versioning follows the same strategy.

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.

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.

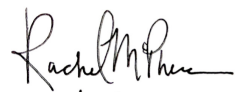
#### **Applicant**

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**

  
April 19, 2019

A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

#### 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

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



Rachel M. Thorne  
April 19, 2019

“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(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**

Rachel M. Thorne  
April 19, 2019

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.

#### 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**

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**

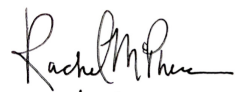
A natural person or Legal Entity that meets the requirements of Section 8.2 (Identity/Qualifications of Assessor).

**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

  
April 19, 2019

application process or revocation process or both. When “RA” is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

#### Reliable Data Source

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

#### Reliable Method of Communication

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

#### Relying Party

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

#### Repository

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

#### Requirements

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

#### Reserved IP Address

An IPv4 or IPv6 address that 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

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

*Rachel M. Thorne*  
April 19, 2019

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 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**

*Rachel M. Thorne*  
April 19, 2019

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
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	

Rachel M. Thorne  
April 19, 2019

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

### **1.6.3 References**

No stipulation

### **1.6.4 Conventions**

No stipulation

## **2. PUBLICATION AND REPOSITORY RESPONSIBILITIES**

### **2.1 Repositories**

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

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

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

Rachel M. Thorne  
April 19, 2019

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

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

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

## 2.2 Publication of certification information

In addition to the above web locations into which TrustCor CA publishes its certification information, email to [legal@trustcor.ca](mailto:legal@trustcor.ca) with requests for information will yield the same documentation.

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

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

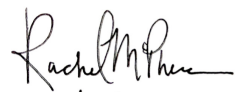
Root CA	State	URI
RootCert CA-1	valid	<a href="https://catest1.trustcor.ca/">https://catest1.trustcor.ca/</a>
RootCert CA-1	revoked	<a href="https://catest1-revoke.trustcor.ca/">https://catest1-revoke.trustcor.ca/</a>
RootCert CA-1	expired	<a href="https://catest1-expire.trustcor.ca/">https://catest1-expire.trustcor.ca/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

### 2.2.1 Notification of incorrect issuance

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

- a description of the incident, listing the certificate identifiers involved, a root cause analysis of the incorrect issuance, and the



  
April 19, 2019

remediation steps taken to address the requirements breach, shall be published under the URI <http://www.trustcor.ca/resources/issuance-incidents/> with a name which is the ISO-8601-Z (with colons replaced by hyphens) timestamp with a .txt suffix (e.g. 2016-05-01T18-12-07Z.txt). To the end of this report, the PEM formatted X.509 certificates shall be appended by way of an appendix.

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

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

### **2.3 Time or frequency of publication**

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

CPS and CP documents are published no more than seven days after the TCPA approves their contents. New CPS and CP documents are produced as and when the Baseline Requirements (BR) change such that new text is required, or when changes in TrustCor CA's business practices require such modification. The CP and CPS documents are reviewed every six months (even if merely to confirm that no changes are warranted).

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

### **2.4 Access controls on repositories**

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

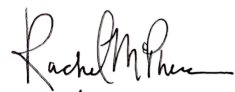
Updates to the documents are stored in a version control system to which TrustCor CA personnel alone have access; all changes are recorded with both the nature of the alteration as well as the author of the change.

Document change logs are reviewed periodically as per the section on log review.

## **3. IDENTIFICATION AND AUTHENTICATION**

### **3.1 Naming**

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

  
April 19, 2019

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

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

### **3.1.1 Types of names**

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

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

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

TrustCor CA does not currently issue EU Qualified Certificates.

### **3.1.2 Need for names to be meaningful**

Any fully qualified domain name (FQDN) which is embedded into a certificate either as a DN component, or as a dnsName subjectAltName must conform to the standard semantics for DNS names described in RFC 1034. All DNS names must be validly formed and have a recognized public ICANN recognized suffix as found via <https://publicsuffix.org>

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

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

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

Rachel M. Thorne  
April 19, 2019

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

### 3.1.3 Anonymity or pseudonymity of subscribers

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

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

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

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

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

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

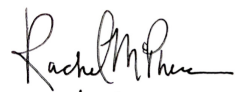
### 3.1.4 Rules for interpreting various name forms

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

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

### 3.1.5 Uniqueness of names

Subject DNs, where present, are unique under the aegis of a single issuer DN. Issuer DNs are unique to particular business categories. Subject to a caveat below, no two **current** (ie, having a non-revoked status) certificates may have the same (subject DN, issuer DN) pair. This is enforced by the CA software end entity issuer profiles.

  
April 19, 2019

The caveat to the uniqueness constraint is that where a certificate is approaching the end of its life, a replacement certificate may be published and the older certificate not revoked. This is to allow customers to roll over new certificates without risking business disruption, where parties relying on the certificate might suffer TLS failures owing to the old certificate revocation. The grace period for such rollovers is specified in the Terms of Use.

Domain uniqueness is enforced by ICANN and fqdn uniqueness is enforced by the DNS records of the domain owner, but the same certificate uniqueness constraint above obtains.

### **3.1.6 Recognition, authentication, and role of trademarks**

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

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

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

### **3.2 Initial identity validation**

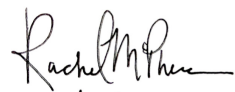
TrustCor CA may use any legal and well known paths to contact applicants, for the purposes of validation, including:

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

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

The following information is collected at registration time:

- for all Secure Mail certificates, the email address of the operator of the private/key certificate pair

  
April 19, 2019

- for all Secure Site certificates, the fqdn of the endpoint which will appear as the primary identity in the subject DN
- for all Basic certificates, whether the requestor wishes for all of the certificates in the chain to the root CA to be limited to 2048 bit moduli only (sometimes needed for devices with limited processing power). This choice is not available for Enhanced grade certificates.

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

### **3.2.1 Method to prove possession of private key**

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

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

### **3.2.2 Authentication of organization identity**

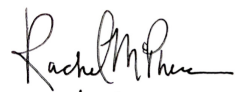
For any OV certificate, the following information is collected upon registration (nb: other information may be collected which does not form part of the validation process):

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

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

For Enhanced Secure Site certificates:

- any other FQDNs which will form subjectAltNames in the certificate

  
April 19, 2019

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

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

### **3.2.2.1 Identity**

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

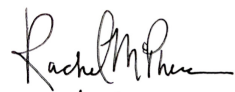
1. Within the jurisdiction of the applicant's organization, a check on a recognized government agency must yield that the organization is registered and currently active. Such agencies can be charity registries, company registries or lists of academic institutions. In all cases the identity of the organization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

### **3.2.2.2 DBA/Tradename**

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

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

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

  
April 19, 2019

In all cases, the validation must include reasonable evidence that the organization is currently operational, or has updated its registration with a relevant registry within the last 398 days at time of request. Dormant or dissolved organizations may not be issued certificates.

### **3.2.2.3 Verification of Country**

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

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

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

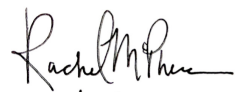
### **3.2.2.4 Validation of Domain Authorization or Control**

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

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

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

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

  
April 19, 2019

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

For all domain validations, the domain must end in a domain published via [https://www.publicsuffix.org/list/public\\_suffix\\_list.dat](https://www.publicsuffix.org/list/public_suffix_list.dat) and appearing within the ICANN DOMAINS section. Specifically, .int is recognized as meaning an international organization and **NOT** designating some internal domain.

#### **3.2.2.4.1 Validating the Applicant as a Domain Contact**

TrustCor CA does not use WHOIS domain contacts as a method for validating identity of the Applicant.

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

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

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

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

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

#### **3.2.2.4.3 Phone Contact with Domain Contact**

If the WHOIS/RDAP reply contains a telephone number, TrustCor CA may use that number to conduct a validation process. If multiple FQDNs are requested, the same number must be present for each WHOIS record.



#### 3.2.2.4.4 Constructed Email to Domain Contact

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

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

#### 3.2.2.4.5 Domain Authorization Documents

As of this CPS, TrustCor CA does not rely upon domain authorization documents to validate applications.

#### 3.2.2.4.6 Agreed-Upon Change to Website

For each FQDN requested, TrustCor CA may require of the applicant to place a resource reachable via

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

This document must contain a base64 representation of a request token (generated uniquely per application) - see Section 3.2.2.4.7 for token format. That token must appear on a line in the text document on its own (with leading or trailing spaces allowed).

The document may also be presented via the TLS URI

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

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

It is permissible for the document to contain multiple lines with different response values - since a website may be reachable by several URIs, each of which have a different certificate.

Requested random values have a lifespan of 7 days. If TrustCor CA's automated web crawler does not pick up the response within that time, the application is rejected, and must be started again.

*Rachel M. Thorne*  
April 19, 2019

Note that this method of validation only establishes control over the particular FQDN. It does not demonstrate control over the Base Domain.

### 3.2.2.4.7 DNS Change

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

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

trustcor-ca={base64 representation of a random value}
---

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

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

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

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

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


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

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

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

### 3.2.2.4.8 IP Address

TrustCor CA does not use the IP Address validation lookup.

  
April 19, 2019

#### **3.2.2.4.9 Test Certificates**

TrustCor CA does not use the test certificate validation method.

#### **3.2.2.4.10 TLS Using a Random Number**

TrustCor CA does not use verification of a random value contained within a certificate as proof of domain control.

#### **3.2.2.4.11 Any Other Method**

TrustCor CA does not use any validation method described under this obsoleted section.

#### **3.2.2.4.12 Validating Applicant as a Domain Contact**

TrustCor CA does not use the domain contact validation method.

#### **3.2.2.4.13 Email to DNS CAA Contact**

TrustCor CA does not currently use this validation method.

#### **3.2.2.4.14 Email to DNS TXT Contact**

TrustCor CA does not currently use this validation method.

#### **3.2.2.4.15 Phone Contact with Domain Contact**

TrustCor CA does not currently use this validation method.

#### **3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact**

TrustCor CA does not currently use this validation method.

#### **3.2.2.5 Authentication for an IP Address**

TrustCor CA does not issue certificates containing IP address identities.  
Section not applicable.

### 3.2.2.6 Wildcard Domain Validation

TrustCor CA does not currently issue wildcard certificates. Section not applicable.

### 3.2.2.7 Data Source Accuracy

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

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

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

### 3.2.2.8 CAA Records

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

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

- `issue` tag: must contain the text `trustcor.ca`
- `issuewild` tag: not applicable. TrustCor CA does not currently issue wildcard certificates

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

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

Rachel M. Thorne  
April 19, 2019

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

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

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

### 3.2.3 Authentication of individual identity

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

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

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

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

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

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

### 3.2.4 Non-verified subscriber information

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

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

### 3.2.5 Validation of authority

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

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

### 3.2.6 Criteria for interoperation

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

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

## 3.3 Identification and authentication for re-key requests

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

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

### **3.3.1 Identification and authentication for routine re-key**

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

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

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

For Enhanced Secure Site certificates, further authentication via a recognized one time password scheme (OTP) or U2F is required.

For Enhanced Secure Site certificates, a signed email request signed by the certificate needing re-key will suffice (assuming that the certificate has not been revoked hitherto). Alternatively, authentication using password and OTP/U2F to the company certificate management site will be acceptable.

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

Under all circumstances, if identity validation was substantiated by documentation, that documentation must not be older than 825 days from time of re-keying. If the documentation is older, then a new certificate request must be made, after revoking the old certificate.

### **3.3.2 Identification and authentication for re-key after revocation**

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

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

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

### **3.4 Identification and authentication for revocation request**

Revocation authentication is dependent on who makes the request:

- Subscriber revocation: simple authentication via username and password (via website authentication) is sufficient to begin revocation. If the certificate is an S/MIME one, verifying a signed email requesting revocation of the signing certificate is sufficient identification and authentication.

*Rachel M. The*  
April 19, 2019

- TrustCor CA revocation: CA/RA administrators are required to authenticate to the CA software via client certificates issued by an internal management CA, in order to revoke a subscriber's certificate.

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

## **4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS**

### **4.1 Certificate Application**

Certificate application can be done via one of two means:

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

#### **4.1.1 Who can submit a certificate application**

Any member of the general public can apply for a TrustCor CA certificate, assuming that they can either view HTTPS web servers or send and receive email.

Application will be turned down if the Applicant is on a blacklist operated by TrustCor CA, which lists those identities thought to present an unacceptable risk of fraud or damage to TrustCor CA's business. That blacklist shall encompass those individuals on the US Treasury Department's OFAC list of proscribed persons.

Any applicant who has had a TrustCor CA issued certificate revoked by reason of fraudulent representation will be added to the blacklist, and service refused for further requests.

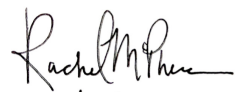
Application for Enterprise Subordinate CA certificates may be initiated via email, but the process of registration and validation then requires postal/courier communications, as well as possible site visit scrutiny from TrustCor CA.

#### **4.1.2 Enrollment process and responsibilities**

The enrollment process involves:

- generating an account for the certificate applicant



  
April 19, 2019

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

The responsibilities on the subscriber include:

- providing complete and accurate information regarding identity
- keeping the private key corresponding to the public key in the CSR confidential.
- generating a public key which satisfies the requirements of the TrustCor CA program.

The responsibilities on TrustCor CA include:

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

## **4.2 Certificate application processing**

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

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

### **4.2.1 Performing identification and authentication functions**

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

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

Rachel M. Thorne  
April 19, 2019

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

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

TrustCor CA also maintains a list of high value trademarks and domains. If a request is visually similar to an entity on that list (via the confusables mapping) the request may be designated high risk and require human intervention to progress the application. If a request is felt (by TrustCor CA personnel) to possess a high likelihood of being fraudulent then the requestor's account may be blacklisted from future requests.

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

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

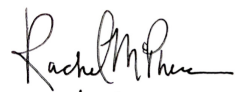
TrustCor CA does not issue certificates to FQDNs under those domains reserved as IANA managed domains (available via <https://www.iana.org/assignments/special-use-domain-names/special-use-domain.csv>), nor to any of the test domains listed in <https://www.iana.org/domains/reserved>

#### **4.2.2 Approval or rejection of certificate applications**

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

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

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

  
April 19, 2019

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

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

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

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

As mentioned elsewhere, all FQDNs and email addresses to be embedded in TrustCor CA certificates must be within the ICANN section of the publicsuffix database. Private domains will not be certified, even if they are under consideration for inclusion by ICANN.

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

#### **4.2.3 Time to process certificate applications**

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

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

### **4.3 Certificate issuance**

#### **4.3.1 CA actions during certificate issuance**

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

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

#### **4.3.2 Notification to subscriber by the CA of issuance of certificate**

For all Basic and Enhanced grade certificates, an email containing the certificate is sent to the technical contact named during application. The subscriber may also download the certificate from the certificate management website.

Enterprise Subordinate CAs may elect to deliver their end-entity certificates through email or web-site download as they see fit.

### **4.4 Certificate acceptance**

#### **4.4.1 Conduct constituting certificate acceptance**

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

If the subscriber is not satisfied with the details contained within the certificate, he or she must email [support@trustcor.ca](mailto:support@trustcor.ca) explaining why the certificate is not being accepted. This communication must take place within 30 days of issuance, otherwise the certificate is deemed to have been accepted.

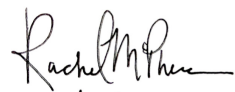
The mechanisms for acceptance are established in the subscriber agreement.

#### **4.4.2 Publication of the certificate by the CA**

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

[Certificate Transparency Known Logs \(https://www.gstatic.com/ct/log\\_list/log\\_list.json\)](https://www.gstatic.com/ct/log_list/log_list.json)

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

  
April 19, 2019

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

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

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

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

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

S/MIME certificates are not published to CT logs. These are only communicated to the end users.

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

#### **4.4.3 Notification of certificate issuance by the CA to other entities**

Other than CT publication per 4.4.2, no stipulation.

#### **4.5 Key pair and certificate usage**

##### **4.5.1 Subscriber private key and certificate usage**

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

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

#### 4.5.2 Relying party public key and certificate usage

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

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

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

#### 4.6 Certificate renewal

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

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

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

##### 4.6.1 Circumstance for certificate renewal

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

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

##### 4.6.2 Who may request renewal

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

Enterprise Subordinate CA subscribers may accept renewal requests from agents within their enterprise if the relevant subscriber agreement allows this arrangement.

### **4.6.3 Processing certificate renewal requests**

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

- use of a website function for renewal after authentication via username and shared secret. Enhanced grade certificates also require two-factor validation (either a TrustCor CA approved OTP method or U2F).
- use of secure email to send a renewal request, where the body of the email contains a signature capable of validating the request.

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

TrustCor CA will then verify that:

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

### **4.6.4 Notification of new certificate issuance to subscriber**

See section 4.3.2 for notification protocols.

### **4.6.5 Conduct constituting acceptance of a renewal certificate**

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

### **4.6.6 Publication of the renewal certificate by the CA**

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

### **4.6.7 Notification of certificate issuance by the CA to other entities**

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

## 4.7 Certificate re-key

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

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

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

### 4.7.1 Circumstance for certificate re-key

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

### 4.7.2 Who may request certification of a new public key

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

### 4.7.3 Processing certificate re-keying requests

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

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

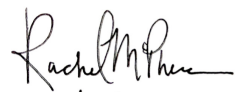
- website authentication using a user name and shared secret
- secure email where the re-key request body contains a valid signature from the subscriber

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

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

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



  
April 19, 2019

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

#### **4.7.4 Notification of new certificate issuance to subscriber**

See Section 4.3.2 of this document for notification protocols.

#### **4.7.5 Conduct constituting acceptance of a re-keyed certificate**

See Section 4.4.1 of this document for acceptance criteria.

#### **4.7.6 Publication of the re-keyed certificate by the CA**

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

#### **4.7.7 Notification of certificate issuance by the CA to other entities**

No stipulation.

### **4.8 Certificate modification**

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

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

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

#### **4.8.1 Circumstance for certificate modification**

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

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

#### **4.8.2 Who may request certificate modification**

Subscribers holding Enhanced Secure Site certificates may request modification.

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

#### **4.8.3 Processing certificate modification requests**

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

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

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

#### **4.8.4 Notification of new certificate issuance to subscriber**

See section 4.3.2 for notification protocols.

#### **4.8.5 Conduct constituting acceptance of modified certificate**

See section 4.4.1 for acceptance criteria.

#### **4.8.6 Publication of the modified certificate by the CA**

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

#### **4.8.7 Notification of certificate issuance by the CA to other entities**

No stipulation.

## 4.9 Certificate revocation and suspension

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

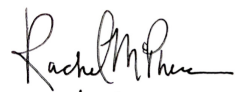
TrustCor CA does not suspend certificates (that is, revoke and then unrevoke them).

### 4.9.1 Circumstances for revocation

#### 4.9.1.1 Reasons for Revoking a Subscriber Certificate

TrustCor CA may revoke subscriber certificates for the following reasons:

- TrustCor CA has reason to believe that the private key is no longer under the sole control of the subscriber who owns the corresponding certificate. This can be through theft, loss, accidental disclosure, or any other such compromise.
- TrustCor CA is informed by the subscriber that the certificate is no longer required and that the subscriber does not wish to be bound any longer by the Subscriber Agreement. This request must be validated so that TrustCor CA has reasonable belief that the subscriber is truly making this request.
- TrustCor CA becomes aware that the subscriber has violated the terms of the binding subscriber agreement.
- The identity assertions present in the certificate no longer hold.
- A trademark dispute has settled that the subscriber does not hold the right to assert the trade names present in the certificate.
- The account authentication information (e.g. shared secret) has become compromised (e.g. loss, theft, accidental disclosure)
- The subscriber engages in fraudulent or other such illegal conduct involving use of the certificate
- The subscription, or any validation evidence for the certificate, was obtained or produced improperly, through misrepresentation, fraud or lack of authority to produce such evidence.
- The subscriber appears (after proper issue) upon a proscribed list of entities or embargoed nations on the OFAC list produced by the government of the United States of America, and this appearance is brought to the attention of TrustCor CA.
- The subscriber does not wish to accept the certificate as it has been issued.
- The subscriber has an Enhanced Secure Site certificate and wishes to delete some of the FQDNs from the certified set.
- Through self-audit, TrustCor CA discovers that a certificate was mistakenly or improperly issued.
- A ballot of the CA/B Forum determines that the content of any certificate constitutes an unacceptable risk to parties relying on the

  
April 19, 2019

certificate information. (For example, if TrustCor CA had issued SHA-1 signed certificates, they would be revoked as those have been deemed insecure).

#### **4.9.1.2 Reasons for Revoking a Subordinate CA Certificate**

TrustCor CA may revoke CA certificates for the following reasons:

- TrustCor CA has reason to believe that the private key is no longer under the sole control of the party who is thought to own it (normally TrustCor CA itself, but in the case of an external subordinate CA, it could be a subscriber in a contractual relationship with TrustCor CA). This can be through theft, loss, accidental disclosure or any other such compromise.
- TrustCor CA ceases operations and is unable to pass its CA duties on to a successor entity.
- Widespread misuse of the CA certificate indicates that TrustCor CA does not control the certificate within the terms of its business controls, or where its technical controls have proven insufficient to safeguard asset integrity. Note that this would not be the case if an insufficiently aware staff member issued an improper certificate - only if such behavior had gone unmonitored and unchecked for a significant time.
- An Enterprise Subordinate CA issues certificates in violation of the terms of its agreement with TrustCor CA.
- An Enterprise Subordinate CA cannot maintain its operations consistent with behavior required in the Baseline Requirements.

#### **4.9.2 Who can request revocation**

The subscriber owning a certificate may request revocation.

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

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

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

- representatives of the browser root certificate programs such as Microsoft, Mozilla, Apple, where TrustCor CA has been accepted into such programs.
- representatives of the CA/B Forum.

### 4.9.3 Procedure for revocation request

Revocation requests may come in one of the following forms:

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

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

This mail must contain contact details (including physical address, email addresses or phone numbers) which enable TrustCor CA to contact the requestor in order to validate the revocation request.

- via a web form, <https://revoke.trustcor.ca/> reached via a username and shared secret (and possible two factor response code), again listing issuer, serial and reason.
- via TrustCor CA's internal ticketing system, which is authenticated via username and password. (This is restricted to requests originating from TrustCor CA itself)

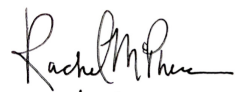
For signed emails, the signature will be validated to ensure that it sufficiently identifies the requestor as belonging to the authorized groups listed in Section 4.9.2.

For unsigned emails, TrustCor CA will attempt to:

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

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

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

  
April 19, 2019

Any revocation request must be ticketed within 24 hours of the request being initiated.

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

#### **4.9.4 Revocation request grace period**

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

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

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

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

#### **4.9.5 Time within which CA must process the revocation request**

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

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

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

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

*Rachel M. Thorne*  
April 19, 2019

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

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

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

#### **4.9.6 Revocation checking requirement for relying parties**

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

#### **4.9.7 CRL issuance frequency**

The CRLs containing the serial numbers for end-entity certificate are published at least every 24 hours, with issuance taking place at shorter intervals at TrustCor CA's discretion.

The CRLs issued by the root CAs are published at least every 6 months, with TrustCor CA having the right to re-issue at shorter intervals as it sees fit. If a subordinate CA under a root certificate is revoked, the new CRL is published no later than 24 hours after revocation.

#### **4.9.8 Maximum latency for CRLs**

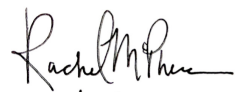
From signing a new CRL to publishing it on the online repository, TrustCor CA will normally take no more than 1 hour to do so. In no case will latency exceed 24 hours.

Every new CRL must be published at least 10 minutes prior to the expiry of the previous CRL in the repository. That is, the most recent CRL on the repository will never be expired.

#### **4.9.9 On-line revocation/status checking availability**

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

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

  
April 19, 2019

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

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

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

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

#### **4.9.10 On-line revocation checking requirements**

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

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

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

#### **4.9.11 Other forms of revocation advertisements available**

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

#### **4.9.12 Special requirements re key compromise**

Other than the disclosure requirements of the CP in this section, there are no special requirements regarding key compromise.

#### **4.9.13 Circumstances for suspension**

TrustCor CA does not suspend certificates. Revocation is permanent.

#### **4.9.14 Who can request suspension**

Not applicable.



#### **4.9.15 Procedure for suspension request**

Not applicable.

#### **4.9.16 Limits on suspension period**

Not applicable.

### **4.10 Certificate status services**

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

#### **4.10.1 Operational characteristics**

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

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

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

#### **4.10.2 Service availability**

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

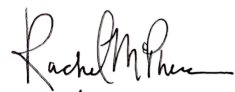
Both OCSP and CRL download services are made available via plaintext HTTP, not HTTPS.

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

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

#### **4.10.3 Optional features**

No stipulation.

  
April 19, 2019

#### **4.11 End of subscription**

A subscriber agreement ends:

- when a certificate is revoked
- when a certificate expires and is not renewed under the same agreement
- when TrustCor is contacted by the subscriber, in writing, who has expressed a desire to terminate the subscription.

#### **4.12 Key escrow and recovery**

TrustCor CA does not escrow keys for any party.

Enterprise Subordinate CAs are not permitted to escrow their keys.

##### **4.12.1 Key escrow and recovery policy and practices**

Not applicable.

##### **4.12.2 Session key encapsulation and recovery policy and practices**

No stipulation.

### **5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS**

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

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

TrustCor CA maintains a security policy details its hiring practices, operational characteristics, monitoring methods, backup and disaster recovery practices. The contents of that policy are forwarded to its auditors, who validate that the policy is being followed.

#### **5.1 Physical controls**

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

##### **5.1.1 Site location and construction**

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

*Rachel M. Thorne*  
April 19, 2019

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

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

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

### **5.1.2 Physical access**

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

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

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

External entrances and exits are patrolled by trained security personnel.

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

### **5.1.3 Power and air conditioning**

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

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

All cabinets are supplied via filtered UPS power.

### **5.1.4 Water exposures**

No data center is in a known flood risk area.

HVAC systems are in place to prevent humidity buildup.

All cabinets have sealed roofs to prevent water exposure.

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

*Rachel M. Thorne*  
April 19, 2019

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

### **5.1.5 Fire prevention and protection**

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

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

### **5.1.6 Media storage**

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

Media is stored away from known fire/flood hazards, in a safe rated to at least UL 72 Class 100-2 Hour.

### **5.1.7 Waste disposal**

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

### **5.1.8 Off-site backup**

TrustCor CA backs up its host's data to locations in the West Coast of the USA and to Western Europe.

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

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

## **5.2 Procedural controls**

### **5.2.1 Trusted roles**

TrustCor CA defines the follow roles for operations:

*Rachel M. Thorne*  
 April 19, 2019

<b>Role Name</b>	<b>Function</b>	<b>Trust Level</b>
Systems Administrator	Deploying or controlling computers hosting TrustCor CA data	Normal
CA Administrator	Changing the configuration of profiles or operation of the CA software	Normal
CA Operator	Issuing and revoking end-entity certificates	Normal
Auditor	Reviewing log data to ensure compliance with stated policies	Normal
HR	Admitting new personnel into TrustCor CA's employ	Normal
Root Operator	Causing the Root CA to sign a certificate request or CRL	High
Remote Hands	Physically installing, altering or removing TrustCor CA equipment in a data center	High

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

Role assignments are granted, reviewed and revoked by the TCPA on at least a quarterly basis.

### **5.2.2 Number of persons required per task**

Generating, or using private keys stored on an offline HSM partition requires two people: one to activate the partition and another to perform the signing or generation.

Transferring CA equipment into data centers requires one person to record the equipment being shipped and one to perform the supervision that the packaged equipment is as recorded.

Tasks which require highly trusted roles are manually performed: not automated.

### **5.2.3 Identification and authentication for each role**

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

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

#### **5.2.4 Roles requiring separation of duties**

Only the Systems Administrator may act under another role designation, but even so, cannot use system level credentialing to assume that other role (ie, must be authenticated via management PKI controls).

#### **5.3 Personnel controls**

Physical access to TrustCor CA equipment is only granted to Remote Hands with the controls for access listed above.

##### **5.3.1 Qualifications, experience, and clearance requirements**

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

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

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

##### **5.3.2 Background check procedures**

All TrustCor CA personnel undergo background checks prior to employment. These checks include:

- criminal records checks
- employment and education history
- residences covering the previous five years
- identity checks using government issued photo ID
- court ordered disqualifications from office holding
- tax and social security references

##### **5.3.3 Training requirements**

Suitable training in job performance is given to all TrustCor CA personnel taking on a trusted role. Each person working for TrustCor CA is made aware of the requirements imposed upon them by:

- The TrustCor CA Security Policy
- The TrustCor CA Privacy Policy

Every employee is trained in TrustCor CA's business offerings as well as the basic operations of any CA/RA, and the operations of the CA software, if their duties require such operation.

*Rachel M. Thorne*  
April 19, 2019

All training is recorded in TrustCor CA's knowledge base, which is part of its workflow software.

#### **5.3.4 Retraining frequency and requirements**

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

This retraining is recorded as per Section 5.3.3

#### **5.3.5 Job rotation frequency and sequence**

No stipulation.

#### **5.3.6 Sanctions for unauthorized actions**

All employees of TrustCor CA are made aware that performing actions outside the rules established by operational regulation, security policy or privacy policy carries the possibility of disciplinary action up to and including termination of employment.

Should that violation of company policy encompass potential criminal wrongdoing, TrustCor CA will report the matter to the appropriate law enforcement agencies for further investigation and action.

Personnel who perform unauthorized actions have their role credentials revoked, to be re-issued if and when the TCPA deems that any retraining has been completed, such that it makes the risk or role recommencement an acceptable one for TrustCor CA.

#### **5.3.7 Independent contractor requirements**

TrustCor CA contractors must undergo the same background checking and conduct training as permanent employees. The sanctions for contractors extends to termination of contract and possible legal action to recover damages.

#### **5.3.8 Documentation supplied to personnel**

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

## 5.4 Audit logging procedures

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

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

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

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

### 5.4.1 Types of events recorded

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

1. CA Key Life Cycle Management events, such as \* Key generation \* Key backup from a key store to any another device \* Key restoration from a device to an approved key store \* Key storage on an approved key store \* Withdrawal of key from service \* Retiring and archival of keys \* Key destruction
2. Cryptographic Device Life Cycle Management events: \* Commissioning/decommissioning of new hardware \* Erasure of data on a hardware device \* Changes in configuration of new devices \* Updates to firmware on devices \* Transportation of hardware devices \* Access control changes to hardware devices \* Activation and deactivation of a cryptographic hardware device \* Compromise of private key
3. CA/Subscriber Certificate Life Cycle events \* Certificate request events
  - All requests for a new certificate
  - All requests for renewal of a certificate
  - All requests for the re-keying of a certificate
  - All requests for the revocation of a certificate \* Certificate data verification events
  - The date and times, phone number used, persons spoken to and the results of any verification telephone calls or data associated with the issuance of a certificate.



Rachel M. Thorne  
April 19, 2019

- The dates, times and results of all verification activities stipulated in TrustCor CA's Certification Practice Statement.
    - \* Results of certificate requests
  - The successful validation of a certificate request
  - The reason for the rejection of a certificate request \*  
Certificate issuance
  - The issuance of both CT pre-certificates and final certificates
  - The results of submission to CT logs of any pre-certificates and final certificates
  - Signing of data using a key stored on a hardware device \*  
Certificate status generation
  - The generation of CRLs for each of the CAs being managed
  - The generation of OCSP responses for each possible response
  - The publication results for the above CRLs and OCSP responses (where applicable)
4. Generalized Security Events \* PKI system access attempts
- All authentication and authorization results (successful or not) for access to any system involved in the processing or handling of PKI data
  - All lockout/clearances caused by system access protection logic \* PKI/Security system events
  - Deployment of new systems to handle PKI data
  - Decommissioning of systems which used to handle PKI data
  - Backup of PKI systems
  - Restoration of PKI systems
  - Alteration of configuration of any software involved in the processing of PKI data
  - Detection of alteration of known sensitive files, including system binaries or configuration files
  - All software packages/patches (with version numbers and identified source) installed or removed from the systems
  - System clock correction events
  - Alteration of the control profiles for the system configuration management subsystems \* Security profile changes
  - Addition of new authorized users/principals to a host
  - Removal of authorized users/principals from a host
  - Alteration of privileges associated with a user or principal
  - Alteration of privilege groups within any host or application involved in the processing of PKI data \* System availability events
  - System crashes (both operating system level and application)
  - Systems becoming non-responsive
  - Systems being restarted
  - Anomalous results emanating from possible hardware faults \*  
Firewall and router activities \* CA facility access
  - Entries to the facility where CA hardware is maintained
  - Exits to the facility where CA hardware is contained

- Access to CA components

#### **5.4.2 Frequency of processing log**

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

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

#### **5.4.3 Retention period for audit log**

Audit logs are maintained onsite until review is complete. Logs are retained for at least 7 years. In the event of audit log information pertaining to certificates, that log retention period starts from the date that the certificate ceases to be valid.

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

#### **5.4.4 Protection of audit log**

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

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

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

#### **5.4.5 Audit log backup procedures**

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

#### **5.4.6 Audit collection system (internal vs. external)**

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

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

*Rachel M. Thorne*  
April 19, 2019

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

#### **5.4.7 Notification to event-causing subject**

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

#### **5.4.8 Vulnerability assessments**

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

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

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

### **5.5 Records archival**

#### **5.5.1 Types of records archived**

The following data forms part of the CA archive:

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

### **5.5.2 Retention period for archive**

Archived records relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, are retained for at least seven years after the Certificate ceases to be valid.

### **5.5.3 Protection of archive**

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

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

### **5.5.4 Archive backup procedures**

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

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

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

### **5.5.5 Requirements for time-stamping of records**

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

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

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

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

### **5.5.6 Archive collection system (internal or external)**

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

### **5.5.7 Procedures to obtain and verify archive information**

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

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

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

### **5.6 Key changeover**

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

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

### **5.7 Compromise and disaster recovery**

#### **5.7.1 Incident and compromise handling procedures**

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

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

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

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

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

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

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

### **5.7.3 Entity private key compromise procedures**

Any CA keys held by TrustCor CA are deemed to be of critical importance. In the event of compromise, the TCPA shall determine what actions must be taken, given the nature and extent of that compromise.

This action could be as much as revoking all current certificates issued under that CA program, and deploying a new CA program to replace the compromised one. TrustCor CA subscribers affected by this revocation would be credited so that they could obtain new credentials from the replacement program.

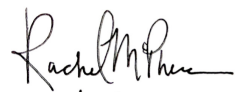
### **5.7.4 Business continuity capabilities after a disaster**

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

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

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

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

  
April 19, 2019

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

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

## **5.8 CA or RA termination**

Should TrustCor CA be about to cease operations, it shall make the best efforts to communicate this state of affairs to:

- The operators of the browser root certificate programs
- The CA/B Forum
- all subscribers to current certificates

This communication should take place 3 months from cessation of operations and must explain that current certificates will not remain valid after cessation of operations. The last act of the CA shall be the revocation of its existing certificate base and the publication of those CRLs.

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

## **6. TECHNICAL SECURITY CONTROLS**

### **6.1 Key pair generation and installation**

#### **6.1.1 Key pair generation**

##### **6.1.1.1 CA Key Pair Generation**

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

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

### **6.1.1.2 Subscriber Key Pair Generation**

TrustCor CA does not perform key generation on behalf of subscribers - such key generation and storage is entirely the responsibility of the subscriber.

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

### **6.1.2 Private key delivery to subscriber**

Not applicable.

### **6.1.3 Public key delivery to certificate issuer**

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

### **6.1.4 CA public key delivery to relying parties**

TrustCor CA publishes all CA certificates on its online repository.

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

### **6.1.5 Key sizes**

The minimum key size allowed for RSA keys in any business offering is 2048 bits, except for Enterprise Subordinate CA keys, which must be 4096 bits long.

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

The minimum key size for any ECC key is 384 bits. ECC keys are not accepted for Enterprise Subordinate CAs. ECC keys must use either the P-384 or P-521 curves.

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

### **6.1.6 Public key parameters generation and quality checking**

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

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



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

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

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

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

## **6.2 Private Key Protection and Cryptographic Module Engineering Controls**

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

### **6.2.1 Cryptographic module standards and controls**

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

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

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

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

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

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

### **6.2.3 Private key escrow**

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

#### **6.2.4 Private key backup**

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

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

#### **6.2.5 Private key archival**

TrustCor CA does not archive its private keys.

#### **6.2.6 Private key transfer into or from a cryptographic module**

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

#### **6.2.7 Private key storage on cryptographic module**

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

#### **6.2.8 Method of activating private key**

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

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

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

#### **6.2.9 Method of deactivating private key**

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

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

#### **6.2.10 Method of destroying private key**

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

### **6.2.11 Cryptographic Module Rating**

See Section 6.2.1 of this document.

## **6.3 Other aspects of key pair management**

### **6.3.1 Public key archival**

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

### **6.3.2 Certificate operational periods and key pair usage periods**

The CA certificates operated directly by TrustCor CA are valid for a period of 15 years.

End entity certificates are valid for periods described in Section 1.4.1 depending on the type of certificate.

## **6.4 Activation data**

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

### **6.4.1 Activation data generation and installation**

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

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

### **6.4.2 Activation data protection**

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

### **6.4.3 Other aspects of activation data**

No stipulation.

## 6.5 Computer security controls

### 6.5.1 Specific computer security technical requirements

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

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

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

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

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

Medium sensitivity hosts must exhibit at least the following controls:

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

Normal sensitivity hosts are controlled using:

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

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

### 6.5.2 Computer security rating

No stipulation.

## 6.6 Life cycle technical controls

### 6.6.1 System development controls

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

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

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

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

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

### 6.6.2 Security management controls

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

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

### 6.6.3 Life cycle security controls

No stipulation.

## 6.7 Network security controls

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

Rachel M. Thorne  
April 19, 2019

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

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

## 6.8 Time-stamping

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

Clock adjustment is an auditable event.

## 7. CERTIFICATE, CRL, AND OCSP PROFILES

### 7.1 Certificate profile

TrustCor CA issues certificates compliant with the ITU X.509 standard, as well as RFC 5280. They are also designed to comply with the Baseline Requirements.

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

#### 7.1.1 Version number(s)

TrustCor CA certificates are X.509v3 certificates.

#### 7.1.2 Certificate extensions

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

##### 7.1.2.1 Root CA Certificate

The Root CA certificates from TrustCor CA contain the following extensions:

- basicConstraints: CA = True [critical]
- subjectKeyIdentifier: hash of public key info, as per RFC 5280, 4.2.1.2
- authorityKeyIdentifier: keyid: (identical to subjectKeyIdentifier value)
- keyUsage: keyCertSign, cRLSign, digitalSignature [critical]

No other extensions are present.

### 7.1.2.2 Subordinate CA Certificate

The Subordinate CA certificates contain the following extensions:

- basicConstraints: CA = True [critical]
- keyUsage: keyCertSign, cRLSign, digitalSignature [critical]
- subjectKeyIdentifier: hash of public key info, as per RFC 5280, 4.2.1.2
- authorityKeyIdentifier: key identifier of signer, per RFC 5280, 4.2.1.1
- authorityInformationAccess:
  - OCSP (URI):
    - Subordinate CA1-Email: <http://ocsp.trustcor.ca/root/ca1> (<http://ocsp.trustcor.ca/root/ca1>)
    - Subordinate CA1-Site: <http://ocsp.trustcor.ca/root/ca1> (<http://ocsp.trustcor.ca/root/ca1>)
    - Subordinate CA1-Site-2048: <http://ocsp.trustcor.ca/root/ca1> (<http://ocsp.trustcor.ca/root/ca1>)
    - Subordinate CA2-Email: <http://ocsp.trustcor.ca/root/ca2> (<http://ocsp.trustcor.ca/root/ca2>)
    - Subordinate CA2-Site: <http://ocsp.trustcor.ca/root/ca2> (<http://ocsp.trustcor.ca/root/ca2>)
    - Subordinate ECA1-External: <http://ocsp.trustcor.ca/root/eca1> (<http://ocsp.trustcor.ca/root/eca1>)
  - CA Issuers (URI):
    - Subordinate CA1-Email: <http://www.trustcor.ca/certs/root/ca1.pem> (<http://www.trustcor.ca/certs/root/ca1.pem>)
    - Subordinate CA1-Site: <http://www.trustcor.ca/certs/root/ca1.pem> (<http://www.trustcor.ca/certs/root/ca1.pem>)
    - Subordinate CA1-Site-2048: <http://www.trustcor.ca/certs/root/ca1.pem> (<http://www.trustcor.ca/certs/root/ca1.pem>)
    - Subordinate CA2-Email: <http://www.trustcor.ca/certs/root/ca2.pem> (<http://www.trustcor.ca/certs/root/ca2.pem>)
    - Subordinate CA2-Site: <http://www.trustcor.ca/certs/root/ca2.pem> (<http://www.trustcor.ca/certs/root/ca2.pem>)
    - Subordinate ECA1-External: <http://www.trustcor.ca/certs/root/eca1.pem> (<http://www.trustcor.ca/certs/root/eca1.pem>)
- cRLDistributionPoints:
  - Subordinate CA1-Email: URI: <http://crl.trustcor.ca/root/ca1.crl> (<http://crl.trustcor.ca/root/ca1.crl>)

Rachel M. The  
April 19, 2019

- Subordinate CA1-Site: URI: <http://crl.trustcor.ca/root/ca1.crl> (<http://crl.trustcor.ca/root/ca1.crl>)
- Subordinate CA1-Site-2048: URI: <http://crl.trustcor.ca/root/ca1.crl> (<http://crl.trustcor.ca/root/ca1.crl>)
- Subordinate CA2-Email: URI: <http://crl.trustcor.ca/root/ca2.crl> (<http://crl.trustcor.ca/root/ca2.crl>)
- Subordinate CA2-Site: URI: <http://crl.trustcor.ca/root/ca2.crl> (<http://crl.trustcor.ca/root/ca2.crl>)
- Subordinate ECA1-External: URI: <http://crl.trustcor.ca/root/eca1.crl> (<http://crl.trustcor.ca/root/eca1.crl>)
- certificatePolicies:
  - policyIdentifier: 1.3.6.1.4.1.44031.1.1.1
  - policyQualifiers:policyQualifierId: id-qt-cps
  - policyQualifiers:qualifier:cpsURI: <http://www.trustcorsystems.com/resources/cps.pdf>

Note that AIA and CRLDP sections have only one URI per type, which changes per the type of CA certificate.

Enterprise Subordinate CAs have different authorityInformationAccess and cRLDistributionPoints extensions:

- authorityInformationAccess:
  - OCSP (URI): <http://ocsp.trustcor.ca/sub/eca1-external> (<http://ocsp.trustcor.ca/sub/eca1-external>)
  - CA Issuers (URI): <http://www.trustcor.ca/certs/sub-eca1-external.pem> (<http://www.trustcor.ca/certs/sub-eca1-external.pem>)
- cRLDistributionPoints: URI: <http://crl.trustcor.ca/sub/eca1-external.crl> (<http://crl.trustcor.ca/sub/eca1-external.crl>)

as well as:

- certificatePolicies:
  - policyIdentifier: <OID from TrustCor CA's 1.3.6.1.4.1.44031.1 arc>
  - policyQualifiers:policyQualifierId: id-qt-cps
  - policyQualifiers:qualifier:cpsURI: <URI of enterprise's CPS document>

Enterprise subscribers are assigned a CPS OID from TrustCor CA's CPS space.

For Enterprise Subordinate CAs, there will also be a NameConstraints extension, which represents the following information:

- permittedSubtree:
  - dNSName: (repeated for each domain owned by the subscriber's enterprise)



- dirName: C=, ST=, L=, O=
- excludedSubTree:
  - 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

### 7.1.2.3 Subscriber Certificate

The extensions vary as per the type of end-entity certificate issued.

#### Basic Secure Mail

- subjectKeyIdentifier: hash of public key info, as per RFC 5280, 4.2.1.2
- authorityKeyIdentifier: key identifier of signer, per RFC 5280, 4.2.1.1
- certificatePolicies:
  - policyIdentifier: 1.3.6.1.4.1.44031.1.1.7 (the OID of this document)
  - policyQualifiers:policyQualifierId: id-qt-cps
  - policyQualifiers:qualifier:cpsURI: <http://www.trustcor.ca/resources/cps.pdf> (<http://www.trustcor.ca/resources/cps.pdf>)
- basicConstraints: CA = False
- keyUsage: digitalSignature, keyEncipherment
- extendedKeyUsage: id-kp-emailProtection
- authorityInformationAccess:
  - OCSP (URI): <http://ocsp.trustcor.ca/sub/ca1-email> (<http://ocsp.trustcor.ca/sub/ca1-email>)
  - CA Issuers (URI): <http://www.trustcor.ca/certs/sub-ca1-email.pem> (<http://www.trustcor.ca/certs/sub-ca1-email.pem>)
- crlDistributionPoints: URI: <http://crl.trustcor.ca/sub/ca1-email.crl> (<http://crl.trustcor.ca/sub/ca1-email.crl>)
- subjectAlternativeName:
  - rfc822Name: *email address of subscriber*

#### Basic Secure Site

- subjectKeyIdentifier: hash of public key info, as per RFC 5280, 4.2.1.2
- authorityKeyIdentifier: key identifier of signer, per RFC 5280, 4.2.1.1
- certificatePolicies:
  - policyIdentifier: 1.3.6.1.4.1.44031.1.1.7 (the OID of this document)
  - policyQualifiers:policyQualifierId: id-qt-cps
  - policyQualifiers:qualifier:cpsURI: <http://www.trustcor.ca/resources/cps.pdf> (<http://www.trustcor.ca/resources/cps.pdf>)
- basicConstraints: CA = False
- keyUsage: digitalSignature, keyEncipherment

Rachel M. Thorne  
April 19, 2019

- extendedKeyUsage: id-kp-clientAuth, id-kp-ServerAuth
- authorityInformationAccess:
  - OCSP (URI): <http://ocsp.trustcor.ca/sub/ca1-site> (<http://ocsp.trustcor.ca/sub/ca1-site>)
  - CA Issuers (URI): <http://www.trustcor.ca/certs/sub-ca1-site.pem> (<http://www.trustcor.ca/certs/sub-ca1-site.pem>)
- crlDistributionPoints: URI: <http://crl.trustcor.ca/sub/ca1-site.crl> (<http://crl.trustcor.ca/sub/ca1-site.crl>)
- subjectAlternativeName:
  - dnsName: *FQDN identical to CN component of subjectDN*

### Enhanced Secure Mail

- subjectKeyIdentifier: hash of public key info, as per RFC 5280, 4.2.1.2
- authorityKeyIdentifier: key identifier of signer, per RFC 5280, 4.2.1.1
- certificatePolicies:
  - policyIdentifier: 1.3.6.1.4.1.44031.1.1.7 (the OID of this document)
  - policyQualifiers:policyQualifierId: id-qt-cps
  - policyQualifiers:qualifier:cpsURI: <http://www.trustcor.ca/resources/cps.pdf> (<http://www.trustcor.ca/resources/cps.pdf>)
- basicConstraints: CA = False
- keyUsage: digitalSignature, keyEncipherment
- extendedKeyUsage: id-kp-emailProtection
- authorityInformationAccess:
  - OCSP (URI): <http://ocsp.trustcor.ca/sub/ca2-email> (<http://ocsp.trustcor.ca/sub/ca2-email>)
  - CA Issuers (URI): <http://www.trustcor.ca/certs/sub-ca2-email.pem> (<http://www.trustcor.ca/certs/sub-ca2-email.pem>)
- crlDistributionPoints: URI: <http://crl.trustcor.ca/sub/ca2-email.crl> (<http://crl.trustcor.ca/sub/ca2-email.crl>)
- subjectAlternativeName:
  - rfc822Name: *email address of subscriber*

### Enhanced Secure Site

- subjectKeyIdentifier: hash of public key info, as per RFC 5280, 4.2.1.2
- authorityKeyIdentifier: key identifier of signer, per RFC 5280, 4.2.1.1
- certificatePolicies:
  - policyIdentifier: 1.3.6.1.4.1.44031.1.1.7 (the OID of this document)
  - policyQualifiers:policyQualifierId: id-qt-cps
  - policyQualifiers:qualifier:cpsURI: <http://www.trustcor.ca/resources/cps.pdf> (<http://www.trustcor.ca/resources/cps.pdf>)

- basicConstraints: CA = False
- keyUsage: digitalSignature, keyEncipherment
- extendedKeyUsage: id-kp-clientAuth, id-kp-ServerAuth
- authorityInformationAccess:
  - OCSP (URI): <http://ocsp.trustcor.ca/sub/ca2-site> (<http://ocsp.trustcor.ca/sub/ca2-site>)
  - CA Issuers (URI): <http://www.trustcor.ca/certs/sub-ca2-site.pem> (<http://www.trustcor.ca/certs/sub-ca2-site.pem>)
- crlDistributionPoints: URI: <http://crl.trustcor.ca/sub/ca2-site.crl> (<http://crl.trustcor.ca/sub/ca2-site.crl>)
- subjectAlternativeName:
  - dnsName: *FQDN identical to CN component of subjectDN*
  - dnsName: *FQDN of additional names registered*

#### 7.1.2.4 All Certificates

No stipulation other than those given in sections 7.1.2.2 and 7.1.2.3.

#### 7.1.2.5 Application of RFC 5280

TrustCor CA issues pre-certificates as described in section 4.4.2. Such certificates are not considered to be certificates (compliant with RFC 5280) as per BR section 7.1.2.5

#### 7.1.3 Algorithm object identifiers

All signing algorithms are either sha256WithRSAEncryption or sha512WithRSAEncryption.

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

#### 7.1.4 Name forms

##### 7.1.4.1 Issuing CA Certificate Subject

The Root CA certificates have the following CN component subjectNames:

- CA-1 : TrustCor CA RootCert CA-1
- CA-2 : TrustCor CA RootCert CA-2
- ECA-1 : TrustCor CA ECA-1

followed by the common components:

- OU [Organizational Unit] : TrustCor Certificate Authority
- O [Organization] : TrustCor Systems S. de R.L.
- L [Locality] : Panama City

*Rachel M. The*  
April 19, 2019

- ST [State/Province] : Panama
- C [Country] : PA

The Issuer DN matches the above (being a self signed certificate).

The subordinate CA certificates have the follow CN components:

- Subordinate CA1-Email : TrustCor Basic Secure Email (CA1)
- Subordinate CA1-Site : TrustCor Basic Secure Site (CA1)
- Subordinate CA1-Site-2048 : TrustCor Basic Secure Site 2048 (CA1)
- Subordinate CA2-Email : TrustCor Enhanced Secure Email (CA2)
- Subordinate CA2-Site : TrustCor Enhanced Secure Site (CA2)
- Subordinate ECA1-External : TrustCor External PKI (ECA1)

followed by the common components:

- OU [Organizational Unit] : TrustCor Network
- O [Organization] : TrustCor Systems S. de R.L.
- ST [State/Province] : Panama
- C [Country] : PA

The Issuer DN will be one of the forms given for the Root CAs in this section.

The SHA-256 fingerprints for each CA certificate are as follows:

**Certificate Name    SHA-256 Fingerprint**

RootCert CA-1	D4:0E:9C:86:CD:8F:E4:68:C1:77:69:59:F4:9E:A7:74: FA:54:86:84:B6:C4:06:F3:90:92:61:F4:DC:E2:57:5C
Subordinate CA-1 Email	02:BE:F9:22:B3:2D:46:DF:E7:52:0B:0E:E7:E3:EA:F5: 88:EE:2B:9C:AB:81:B8:48:37:E6:B9:55:E0:75:9A:90
Subordinate CA-1- Site	FE: 1E:CA:DB:DE:E0:E5:58:06:8D:DB:C7:B3:3A:B7:8D: D5:7D:0D:C2:2F:CC:1C:36:01:19:01:03:75:B0:A6:1B
Subordinate CA-1- Site-2048	4E:FA:AA:10:40:AC:2F:44:D3:DE:E2:06:D9:52:2A: 28: 8D:84:EC:38:DD:F5:92:98:C9:26:E0:2F:4C:9D: 9A:EF
RootCert CA-2	07:53:E9:40:37:8C:1B:D5:E3:83:6E:39:5D:AE:A5:CB: 83:9E:50:46:F1:BD:0E:AE:19:51:CF:10:FE:C7:C9:65
Subordinate CA2- Email	A6:D3:65:16:1B:58:53:9C:B4:4B:29:D7:7C:64:81:26: F3:3D:B3:C4:93:11:6C:30:40:E1:8D:E3:E0:1A:42:42
Subordinate CA2- Site	38:30:DB:8E:A1:52:0B:6C:DF:57:E1:E0:0A:5F:12:97: BE:11:D9:E6:43:0C:83:60:71:76:21:2F:F8:5D:2D:B8

#### Certificate Name SHA-256 Fingerprint

External ECA-1	5A:88:5D:B1:9C:01:D9:12:C5:75:93:88:93:8C:AF:BB:DF:03:1A:B2:D4:8E:91:EE:15:58:9B:42:97:1D:03:9C
Subordinate ECA1-External	78:82:D9:FA:A4:9A:8B:B3:51:F0:FC:6E:D6:85:EF:1F:C5:15:41:D0:CE:0A:42:22:07:4D:1D:9E:16:FD:C3:0B

#### 7.1.4.2 Subject Information for Standard Server Authentication certificates

If a Subject DN is present for Basic Secure Site certificates, it will always be:

- CN = *certified FQDN*

The subject of Enhanced Secure Site certificates is always:

- CN = *certified FQDN*
- O = *certified organization name*
- ST = *state/province of certified organization*
- L = *locality of certified organization*
- C = *country of certified organization*

While not required in this section, the subject of Basic Secure Mail certificates (if one is present) is always:

- emailAddress = *address of subscriber*

and that of Enhanced Secure Mail certificates is:

- emailAddress = *certified FQDN*
- CN = *common name of organization associated entity*
- O = *certified organization name*
- ST = *state/province of certified organization*
- L = *locality of certified organization*
- C = *country of certified organization*

In all cases, the Issuer DN will be identical to the subject DN of the issuing CA certificate, as described in Section 7.1.4.1.

#### 7.1.4.3 Subject Alternative Names for Standard Server Authentication certificates

#### 7.1.5 Name constraints

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

## 7.1.6 Certificate policy object identifier

### 7.1.6.1. Reserved Certificate Policy Identifiers

The DV and OV policy identifiers are included in certificates as described in Section 7.1.6.4.

### 7.1.6.2. Root CA Certificates

Root CAs have no certificatePolicies extension.

### 7.1.6.3 Subordinate CA Certificates

All subordinate CAs contain policy identifiers noting the governing CPS policy at the time of issuance. In addition, Enterprise Subordinate CAs contain the extendedKeyUsage identifiers restricting the CAs to issue particular categories of end entity certificates.

### 7.1.6.4 Subscriber Certificates

In addition to general CPS policy identifiers, additional identifiers may be present in end entity certificates, described below:

#### **Basic Secure Mail**

These certificates carry no policy identifier.

#### **Basic Secure Site**

These certificates carry the policy identifier of 2.23.140.1.2.1 (DV)

#### **Enhanced Secure Mail**

These certificates carry the policy identifier of 2.23.140.1.2.3 (IV)

#### **Enhanced Secure Site**

These certificates carry the policy identifier of 2.23.140.1.2.2 (OV)

## 7.1.7 Usage of Policy Constraints extension

Not applicable.

## 7.1.8 Policy qualifiers syntax and semantics

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

### **7.1.9 Processing semantics for the critical Certificate Policies extension**

No stipulation.

### **7.2 CRL profile**

Root CA CRLs have a validity period of 6 months.

Subordinate CA CRLs are issued with a validity period covering 96 hours.

#### **7.2.1 Version number(s)**

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

#### **7.2.2 CRL and CRL entry extensions**

The CRL number is a monotonically increasing integer.

The Authority Key Identifier matches that in the signing certificate.

The Invalidation date is given as a UTC date.

### **7.3 OCSP profile**

OCSP responses have a maximum of 96 hours validity, except in the cases of OCSP responses for subordinate CAs, which may have a 6 month validity period, consistent with the CRL durations given above.

#### **7.3.1 Version number(s)**

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

#### **7.3.2 OCSP extensions**

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

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

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

## **8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS**

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

### **8.1 Frequency or circumstances of assessment**

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

### **8.2 Identity/qualifications of assessor**

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

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

### **8.3 Assessor's relationship to assessed entity**

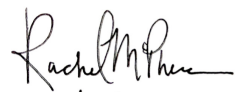
TrustCor CA has selected an auditor/assessor who is completely independent from TrustCor Systems S. de R.L. or any of its affiliated companies. The auditor selected will not have any interest which would cause a bias in any direction regarding audit findings.

### **8.4 Topics covered by assessment**

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

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



  
April 19, 2019

## **8.5 Actions taken as a result of deficiency**

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

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

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

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

## **8.6 Communication of results**

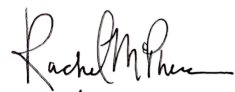
The results of all compliance audits will be communicated to the TCPA and to any third party entities which are entitled by law or regulation to receive a copy of the audit results.

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

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

## **8.7 Self-Audits**

TrustCor CA monitors adherences to the Certificate Policy, This Certificate Practice Statement, and the Baseline Requirements and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one Certificate or at least three percent of the Certificates issued, from each business offering, during the period commencing immediately after the previous self-audit sample was taken.

  
April 19, 2019

## **9. OTHER BUSINESS AND LEGAL MATTERS**

### **9.1 Fees**

#### **9.1.1 Certificate issuance or renewal fees**

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

#### **9.1.2 Certificate access fees**

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

#### **9.1.3 Revocation or status information access fees**

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

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

#### **9.1.4 Fees for other services**

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

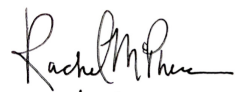
#### **9.1.5 Refund policy**

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

### **9.2 Financial responsibility**

#### **9.2.1 Insurance coverage**

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

  
April 19, 2019

### **9.2.2 Other assets**

No stipulation.

### **9.2.3 Insurance or warranty coverage for end-entities**

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

## **9.3 Confidentiality of business information**

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

### **9.3.1 Scope of confidential information**

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

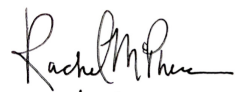
- Subscriber Agreements and Relying Party Agreements
- Contingency, Disaster Recovery, And Business Continuity Plans
- Any certificate application records and documentation submitted in support of certificate applications, which is not in relation to an issued certificate, whether successful or rejected.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

### **9.3.2 Information not within the scope of confidential information**

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

### **9.3.3 Responsibility to protect confidential information**

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

  
April 19, 2019

## **9.4 Privacy of personal information**

### **9.4.1 Privacy plan**

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

### **9.4.2 Information treated as private**

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

### **9.4.3 Information not deemed private**

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

### **9.4.4 Responsibility to protect private information**

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

### **9.4.5 Notice and consent to use private information**

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

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

### **9.4.6 Disclosure pursuant to judicial or administrative process**

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

### **9.4.7 Other information disclosure circumstances**

No stipulation.

## 9.5 Intellectual property rights

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

## 9.6 Representations and warranties

### 9.6.1 CA representations and warranties

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

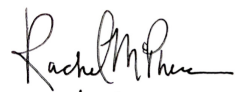
- TrustCor CA complies with its company policies, the CP and this CPS
- Certificates issued will comply and be verified in accordance with this CPS
- To the best of TrustCor CA's knowledge, there are no misrepresentations of fact in the Certificates
- TrustCor CA's revocation services, including its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

### 9.6.2 RA representations and warranties

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

The RA warranties include, but are not limited to:

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

  
April 19, 2019

### **9.6.3 Subscriber representations and warranties**

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

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

### **9.6.4 Relying party representations and warranties**

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

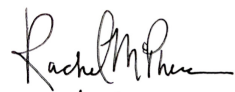
- Understand and obtain sufficient information on the use of Certificates and PKI
- Not rely on or use a TrustCor CA Certificate which has expired, been revoked or is being used for any purpose other than contained in the Certificate itself
- Verify both the TrustCor CA Certificate and the Certificates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

### **9.6.5 Representations and warranties of other participants**

No stipulation.

### **9.7 Disclaimers of warranties**

All Certificates and any related services and software are provided on an “as is” and “as available” basis. To the maximum extent permitted by law, TrustCor CA disclaims all express and implied warranties, including warranties of merchantability, fitness for a particular purpose, satisfactory quality and non-infringement. TrustCor CA does not warrant that any service or product will meet any expectations, be uninterrupted or that

  
April 19, 2019

access to Certificates will be timely or error-free. TrustCor CA does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time.

## **9.8 Limitations of liability**

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

## **9.9 Indemnities**

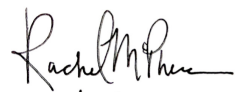
### **9.9.1 Indemnification by CAs**

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

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

### **9.9.2 Indemnification by Subscribers**

Subscriber shall release, indemnify and hold harmless TrustCor CA, its partners, all RAs operating under TrustCor CA and any Resellers, and all respective directors, shareholders, officers, agents, employees, contractors and successors of the foregoing, against any and all liabilities, third party claims, proceedings, judgments, damages, losses, expenses and costs (including reasonable attorney's fees and court costs) that, directly or indirectly, arise from: \* Subscriber's breach of warranties, representations and obligations under the Subscriber Agreement, this CPS or applicable law; \* Any error, misrepresentation or omission made by Subscriber in using or applying for the Certificate; \* Any infringement of an Intellectual Property Right of any person or entity in information or content provided

  
April 19, 2019

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

### **9.9.3 Indemnification by Relying Parties**

No stipulation.

## **9.10 Term and termination**

### **9.10.1 Term**

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

### **9.10.2 Termination**

The terms of this CPS and any amendments remain in effect until replaced by the issuance of a properly approved newer version. Changes become effective immediately upon publication.

### **9.10.3 Effect of termination and survival**

Changes to this version, and all versions of the CPS, are published to TrustCor CA's online repository. Regardless of such changes, the following rights, responsibilities and obligations will survive termination:

- All Subscriber Agreements and any Relying Party Agreements;
- All payment obligations;
- All responsibilities and obligations related to confidential information, including those stated in section 9.3 of this CPS;
- All responsibilities and obligations to protect private information, including those stated in section 9.4.4 of this CPS;
- All representations and warranties, including those stated in section 9.6 of this CPS;
- All warranties disclaimed in section 9.7 of this CPS;
- All limitations of liabilities as described in section 9.8 of this CPS;
- and
- All indemnities described in section 9.9 of this CPS.

## **9.11 Individual notices and communications with participants**

TrustCor CA accepts notices related to this CPS, by means of digitally signed emails or in paper form sent to the TCPA, at the locations specified in section 1.5.1 (electronic and physical are given). All such notices are deemed effective upon receipt of a valid and digitally signed



Rachel M. Thorne  
April 19, 2019

acknowledgement from TrustCor CA. The sender must receive such acknowledgment within ten (10) business days, or else written notice must then be sent in paper form through a courier service that confirms delivery.

## 9.12 Amendments

Amendments to this document are classified by severity:

- minimal - no changes to conditions to any party is involved. Typically used when correcting grammar, clarifying meaning or reformatting the appearance of text.
- small - additional business offerings or minor changes to existing business offerings are made which have minimal impact on any party's obligations
- large - major changes to rights or responsibilities are entailed. Major new business offerings, withdrawal of existing lines of business (where premature revocation of certificates might be needed) would be classified as major.

### 9.12.1 Procedure for amendment

Any proposed change to this CPS is made in a source code controlled repository operated by TrustCor CA. Controls are in place to reasonably ensure that this CPS is not amended and published without the prior review and authorization of the TCPA. If accepted for inclusion, the TCPA will issue incremented numbering to the CPS version based on the severity of the change.

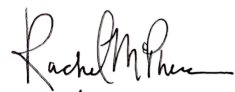
The version of the document will change as follows:

- minimal: the micro version of this document is incremented. No new OID is generated. (e.g. 1.0.1 -> 1.0.2)
- small: the minor version of this document is incremented, a new OID is generated, and included in all future certificates issued pursuant to the new CPS. (e.g. 1.2.4 -> 1.3.0)
- large: the major version of this document is incremented, and a new OID is generated. (e.g. 1.3.5 -> 2.0.0)

Updated versions of the CPS are posted to the online repository of the TrustCor CA website.

### 9.12.2 Notification mechanism and period

TrustCor CA provides notice of CPS revisions by publication of the CPS to the online repository. Amendments become effective on the date provided in the document. TrustCor CA reserves the right to make changes to this CPS without prior notice and at any time.

  
April 19, 2019

### **9.12.3 Circumstances under which OID must be changed**

The TCPA has the sole authority to determine whether an amendment to the CPS requires an OID change. Circumstances for new OID changes are listed in section 9.12.1 of this CPS.

### **9.13 Dispute resolution provisions**

Before filing suit, initiating an administrative claim, or resorting to any other dispute resolution mechanism, all parties agree to notify TrustCor CA for the purpose of seeking a dispute resolution.

If the dispute is not resolved within sixty (60) days after the initial confirmed notice, then the disputing party may proceed as permitted under applicable law as specified under the relevant Subscriber Agreement or Relying Party Agreement.

### **9.14 Governing law**

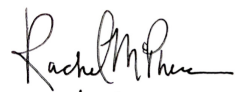
The substantive laws of the Republic of Panama govern the interpretation, construction and enforcement of this CPS and all matters related to it, including tort claims, without regards to any conflict-of-law provisions. The law of Panama applies to all TrustCor CA commercial or contractual relationships in which this CPS may apply, quoted implicitly or explicitly, in relation to TrustCor CA products and services where TrustCor CA acts as a provider, supplier, beneficiary receiver or otherwise.

Each party, including Subscribers, Relying Parties and all other related parties, hereby agree to the exclusive jurisdiction of the courts of the Republic of Panama.

### **9.15 Compliance with applicable law**

Each party acknowledges and agrees to comply with all applicable national, state, local and foreign laws, regulations and export requirements. TrustCor CA shall have the right to refuse issuance or revoke a Certificate, without any prior notice, if Applicant or Subscriber fails to comply with this provision.

With regard to the PII provisions of Section 9.4.5, TrustCor CA meets the requirements of the data protection regulations of the European Union regarding access, disclosure and destruction of personal data.

  
April 19, 2019

## **9.16 Miscellaneous provisions**

### **9.16.1 Entire agreement**

This CPS, the CP, the applicable Subscriber Agreement and Relying Party Agreement represent the entire agreement between the parties, superseding any and all agreements and representations that may exist pertaining to its subject matter.

In the event of any inconsistency between the provisions of this CPS and the provisions of any Subscriber Agreement or any Relying Party Agreement, the terms and conditions of this CPS shall govern.

### **9.16.2 Assignment**

Entities operating under this CPS may not assign their rights or obligations to any other party without the prior written consent of TrustCor Systems S. de R.L.

### **9.16.3 Severability**

If any provision of this CPS is found to be invalid, illegal or unenforceable by a court of competent jurisdiction, the provision affected will be construed so as to be enforceable to the maximum extent permissible by law; and the validity, legality and enforceability of the remaining provisions contained in this CPS shall not, in any way, be affected or impaired thereby.

### **9.16.4 Enforcement (attorneys' fees and waiver of rights)**

If a party violates the terms of any agreement with TrustCor CA, including but not limited to this CPS, TrustCor CA may seek indemnification and any fees (including reasonable attorney's fees and court costs) from such party for damages, losses and expenses related to that party's conduct.

TrustCor CA's failure to enforce a provision of this CPS does not waive TrustCor CA's right to enforce the same provision later, or right to enforce any other provision of this CPS (except where a waiver is granted of explicit written permission by TrustCor CA).

### **9.16.5 Force Majeure**

TrustCor CA shall not be liable for any interruption in performance or failure to perform an obligation under the this CPS, where such interruption or failure is caused by an event outside TrustCor CA's reasonable control.

## **9.17 Other provisions**

Rachel M. Thorne  
April 19, 2019

No stipulation.