Rachel McPherson
2022-02-08

TrustCor CA Certificate Policy

Version 1.8.1

TrustCor Policy Authority

2022-02-08

Rachel McPherson
2022-02-08

Contents

1 Introduction **10**
1.1 Overview . . . 10
1.2 Document Name and Identification . . . 11
1.2.1 Revisions . . . 12
1.3 PKI Participants . . . 13
1.3.1 Certification Authorities . . . 13
1.3.2 Registration Authorities . . . 13
1.3.3 Subscribers . . . 14
1.3.4 Relying Parties . . . 14
1.3.5 Other Participants . . . 14
1.4 Certificate Usage . . . 14
1.4.1 Appropriate Certificate Uses . . . 15
1.4.2 Prohibited Certificate Uses . . . 15
1.5 Policy Administration . . . 15
1.5.1 Organization Administering the Document . . . 15
1.5.2 Contact Person . . . 16
1.5.3 Person Determining CPS Suitability For the Policy . . . 16
1.5.4 CPS approval procedures . . . 16
1.6 Definitions and Acronyms . . . 17
1.6.1 Definitions . . . 17
1.6.2 Acronyms . . . 23
1.6.3 References . . . 24

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES **24**
2.1 Repositories . . . 24
2.2 Publication of Certification Information . . . 24
2.3 Time or Frequency of Publication . . . 25
2.4 Access Controls on Repositories . . . 25

3 IDENTIFICATION AND AUTHENTICATION **25**
3.1 Naming . . . 25
3.1.1 Types of Names . . . 25
3.1.2 Need for Names to Be Meaningful . . . 26
3.1.3 Anonymity or Pseudonymity of Subscribers . . . 26
3.1.4 Rules for Interpreting Various Name Forms . . . 27
3.1.5 Uniqueness of Names . . . 27

Rachel McPherson
2022-02-08

3.1.6 Recognition, Authentication, and Role of Trademarks 27
3.2 Initial Identity Validation 27
3.2.1 Method to Prove Possession of Private Key 28
3.2.2 Authentication of Organization and Domain Identity 28
3.2.2.1 Identity 28
3.2.2.2 DBA/Tradename 29
3.2.2.3 Verification of Country 29
3.2.2.4 Validation of Domain Authorization or Control 29
3.2.2.4.1 Validating the Applicant as a Domain Contact 30
3.2.2.4.2 Email, Fax, SMS or Postal Mail to Domain Contact . . 30
3.2.2.4.3 Phone Contact with Domain Contact 30
3.2.2.4.4 Constructed Email to Domain Contact 30
3.2.2.4.5 Domain Authorization Document 30
3.2.2.4.6 Agreed-Upon Change to Website 30
3.2.2.4.7 DNS Change 30
3.2.2.4.8 IP Address 30
3.2.2.4.9 Test Certificates 30
3.2.2.4.10 TLS Using a Random Number 30
3.2.2.4.11 Any Other Method 30
3.2.2.4.12 Validating Applicant as a Domain Contact 31
3.2.2.4.13 Email to DNS CAA Contact 31
3.2.2.4.14 Email to DNS TXT Contact 31
3.2.2.4.15 Phone Contact with Domain Contact 31
3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact . 31
3.2.2.4.17 Phone Context with DNS CAA Phone Contact 31
3.2.2.4.18 Agreed-Upon Change to Website v2 31
3.2.2.4.19 Agreed-Upon Change to Website - ACME 31
3.2.2.4.20 TLS Using ALPN 31
3.2.2.5 Authentication for an IP Address 32
3.2.2.6 Wildcard Domain Validation 32
3.2.2.7 Data Source Accuracy 32
3.2.2.8 CAA Records 32
3.2.3 Authentication of Individual Identity 32
3.2.4 Non-verified Subscriber Information 33
3.2.5 Validation of Authority 34
3.2.6 Criteria for Interoperation 34
3.3 Identification and Authentication for Re-key Requests 34
3.3.1 Identification and Authentication for Routine Re-key 34

3.3.2 Identification and Authentication for Re-key after Revocation 35
3.4 Identification and Authentication for Revocation Request 35

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 36
4.1 Certificate Application 36
4.1.1 Who Can Submit a Certificate Application 36
4.1.2 Enrollment Process and Responsibilities 36
4.2 Certificate Application Processing 37
4.2.1 Performing Identification and Authentication Functions 37
4.2.2 Approval or Rejection of Certificate Applications 37
4.2.3 Time to Process Certificate Applications 37
4.3 Certificate Issuance 38
4.3.1 CA Actions during Certificate Issuance 38
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 38
4.4 Certificate Acceptance 38
4.4.1 Conduct Constituting Certificate Acceptance 38
4.4.2 Publication of the Certificate by the CA 39
4.4.3 Notification of certificate issuance by the CA to other entities 39
4.5 Key Pair and Certificate Usage 39
4.5.1 Subscriber Private Key and Certificate Usage 39
4.5.2 Relying Party Public Key and Certificate Usage 39
4.6 Certificate Renewal 40
4.6.1 Circumstance for Certificate Renewal 40
4.6.2 Who May Request Renewal 40
4.6.3 Processing Certificate Renewal Requests 40
4.6.4 Notification of New Certificate Issuance to Subscriber 40
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 40
4.6.6 Publication of the Renewal Certificate by the CA 41
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 41
4.7 Certificate Re-key 41
4.7.1 Circumstance for Certificate Re-key 41
4.7.2 Who May Request Certification of a New Public Key 41
4.7.3 Processing Certificate Re-keying Requests 41
4.7.4 Notification of New Certificate Issuance to Subscriber 41
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 42
4.7.6 Publication of the Re-keyed Certificate by the CA 42
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 42

Rachel McPherson
2022-02-08

4.8 Certificate Modification 42
4.8.1 Circumstance for Certificate Modification 42
4.8.2 Who May Request Certificate Modification 43
4.8.3 Processing Certificate Modification Requests 43
4.8.4 Notification of New Certificate Issuance to Subscriber 43
4.8.5 Conduct Constituting Acceptance of Modified Certificate 43
4.8.6 Publication of the Modified Certificate by the CA 43
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 43
4.9 Certificate Revocation and Suspension 44
4.9.1 Circumstances for Revocation 44
4.9.1.1 Reasons for Revoking a Subscriber Certificate 45
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate 46
4.9.2 Who Can Request Revocation 46
4.9.3 Procedure for Revocation Request 47
4.9.4 Revocation Request Grace Period 47
4.9.5 Time within Which Ca Must Process the Revocation Request 47
4.9.6 Revocation Checking Requirement for Relying Parties 48
4.9.7 CRL Issuance Frequency (if Applicable) 48
4.9.8 Maximum Latency for CRLs (if Applicable) 48
4.9.9 On-line Revocation/Status Checking Availability 48
4.9.10 On-line Revocation Checking Requirements 49
4.9.11 Other Forms of Revocation Advertisements Available 49
4.9.12 Special Requirements Related to Key Compromise 49
4.9.13 Circumstances for Suspension 49
4.9.14 Who Can Request Suspension 49
4.9.15 Procedure for Suspension Request 49
4.9.16 Limits on Suspension Period 50
4.10 Certificate Status Services 50
4.10.1 Operational Characteristics 50
4.10.2 Service Availability 50
4.11 End of Subscription 50
4.12 Key Escrow and Recovery 50
4.12.1 Key Escrow and Recovery Policy and Practices 51
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 51

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 51

5.1 Physical Controls 51
5.1.1 Site Location and Construction 51

5.1.2 Physical Access . . . 51
5.1.3 Power and Air Conditioning . . . 52
5.1.4 Water Exposures . . . 52
5.1.5 Fire Prevention and Protection . . . 53
5.1.6 Media Storage . . . 53
5.1.7 Waste Disposal . . . 53
5.1.8 Off-site Backup . . . 53
5.2 Procedural Controls . . . 54
5.2.1 Trusted Roles . . . 54
5.2.2 Number of Persons Required per Task . . . 54
5.2.3 Identification and Authentication for Each Role . . . 54
5.2.4 Roles Requiring Separation of Duties . . . 55
5.3 Personnel Controls . . . 55
5.3.1 Qualifications, Experience, and Clearance Requirements . . . 55
5.3.2 Background Check Procedures . . . 55
5.3.3 Training Requirements . . . 55
5.3.4 Retraining Frequency and Requirements . . . 55
5.3.5 Job Rotation Frequency and Sequence . . . 56
5.3.6 Sanctions for Unauthorized Actions . . . 56
5.3.7 Independent Contractor Requirements . . . 56
5.3.8 Documentation Supplied to Personnel . . . 56
5.4 Audit Logging Procedures . . . 56
5.4.1 Types of Events Recorded . . . 56
5.4.2 Frequency for Processing and Archiving Audit Logs . . . 59
5.4.3 Retention Period for Audit Logs . . . 59
5.4.4 Protection of Audit Log . . . 59
5.4.5 Audit Log Backup Procedures . . . 60
5.4.6 Audit Log Accumulation System (internal vs. external) . . . 60
5.4.7 Notification to Event-Causing Subject . . . 60
5.4.8 Vulnerability Assessments . . . 60
5.5 Records Archival . . . 60
5.5.1 Types of Records Archived . . . 60
5.5.2 Retention Period for Archive . . . 61
5.5.3 Protection of Archive . . . 61
5.5.4 Archive Backup Procedures . . . 61
5.5.5 Requirements for Time-stamping of Records . . . 61
5.5.6 Archive Collection System (internal or external) . . . 61
5.5.7 Procedures to Obtain and Verify Archive Information . . . 61

Rachel McPherson
2022-02-08

5.6 Key Changeover . . . 62
5.7 Compromise and Disaster Recovery . . . 62
5.7.1 Incident and Compromise Handling Procedures . . . 62
5.7.2 Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted . . . 62
5.7.3 Recovery Procedures After Key Compromise . . . 62
5.7.4 Business Continuity Capabilities after a Disaster . . . 63
5.8 CA or RA Termination . . . 63

6 TECHNICAL SECURITY CONTROLS 64
6.1 Key Pair Generation and Installation . . . 64
6.1.1 Key Pair Generation . . . 64
6.1.1.1 CA Key Pair Generation . . . 64
6.1.1.2 Subscriber Key Pair Generation . . . 64
6.1.2 Private Key Delivery to Subscriber . . . 64
6.1.3 Public Key Delivery to Certificate Issuer . . . 64
6.1.4 CA Public Key Delivery to Relying Parties . . . 64
6.1.5 Key Sizes . . . 64
6.1.6 Public Key Parameters Generation and Quality Checking . . . 65
6.1.7 Key Usage Purposes . . . 65
6.2 Private Key Protection and Cryptographic Module Engineering Controls . . . 66
6.2.1 Cryptographic Module Standards and Controls . . . 66
6.2.2 Private Key (n out of m) Multi-person Control . . . 66
6.2.3 Private Key Escrow . . . 66
6.2.4 Private Key Backup . . . 66
6.2.5 Private Key Archival . . . 67
6.2.6 Private Key Transfer into or from a Cryptographic Module . . . 67
6.2.7 Private Key Storage on Cryptographic Module . . . 67
6.2.8 Method of Activating Private Key . . . 67
6.2.9 Method of Deactivating Private Key . . . 67
6.2.10 Method of Destroying Private Key . . . 68
6.2.11 Cryptographic Module Rating . . . 68
6.3 Other Aspects of Key Pair Management . . . 68
6.3.1 Public Key Archival . . . 68
6.3.2 Certificate Operational Periods and Key Pair Usage Periods . . . 68
6.4 Activation Data . . . 69
6.4.1 Activation Data Generation and Installation . . . 69
6.4.2 Activation Data Protection . . . 69

6.4.3 Other Aspects of Activation Data . . . 70
6.5 Computer Security Controls . . . 70
6.5.1 Specific Computer Security Technical Requirements . . . 70
6.5.2 Computer Security Rating . . . 70
6.6 Life Cycle Technical Controls . . . 71
6.6.1 System Development Controls . . . 71
6.6.2 Security Management Controls . . . 71
6.6.3 Life Cycle Security Controls . . . 71
6.7 Network Security Controls . . . 71
6.8 Time-stamping . . . 72

7 CERTIFICATE, CRL, AND OCSP PROFILES 72
7.1 Certificate Profile . . . 72
7.1.1 Version Number(s) . . . 72
7.1.2 Certificate Content and Extensions . . . 72
7.1.3 Algorithm Object Identifiers . . . 72
7.1.4 Name Forms . . . 73
7.1.4.1 Issuer Information . . . 73
7.1.4.2 Subject Information - Subscriber Certificates . . . 73
7.1.4.2.1 Subject Alternative Name Extension . . . 73
7.1.4.2.2 Subject Distinguished Name Fields . . . 73
7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates . . . 74
7.1.4.3.1 Subject Distinguished Name Fields . . . 74
7.1.5 Name Constraints . . . 74
7.1.6 Certificate Policy Object Identifier . . . 75
7.1.6.1 Reserved Certificate Policy Identifiers . . . 75
7.1.6.2 Root CA Certificates . . . 75
7.1.6.3 Subordinate CA Certificates . . . 75
7.1.6.4 Subscriber Certificates . . . 75
7.1.7 Usage of Policy Constraints Extension . . . 75
7.1.8 Policy Qualifiers Syntax and Semantics . . . 76
7.1.9 Processing Semantics for the Critical Certificate Policies Extension . . . 76
7.2 CRL Profile . . . 76
7.2.1 Version Number(s) . . . 76
7.2.2 CRL and CRL Entry Extensions . . . 76
7.3 OCSP Profile . . . 76
7.3.1 Version Number(s) . . . 76

7.3.2 OCSP Extensions 76

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 76

8.1 Frequency or Circumstances of Assessment 77
8.2 Identity/qualifications of Assessor 77
8.3 Assessor's Relationship to Assessed Entity 77
8.4 Topics Covered by Assessment 77
8.5 Actions Taken as a Result of Deficiency 77
8.6 Communication of Results 78
8.7 Self-Audits 78

9 OTHER BUSINESS AND LEGAL MATTERS 78

9.1 Fees 78
9.1.1 Certificate Issuance or Renewal Fees 78
9.1.2 Certificate Access Fees 78
9.1.3 Revocation or Status Information Access Fees 79
9.1.4 Fees for Other Services 79
9.1.5 Refund Policy 79
9.2 Financial Responsibility 79
9.2.1 Insurance Coverage 79
9.2.2 Other Assets 79
9.2.3 Insurance or Warranty Coverage for End-entities 79
9.3 Confidentiality of Business Information 80
9.3.1 Scope of Confidential Information 80
9.3.2 Information Not within the Scope of Confidential Information 80
9.3.3 Responsibility to Protect Confidential Information 80
9.4 Privacy of Personal Information 80
9.4.1 Privacy Plan 80
9.4.2 Information Treated as Private 80
9.4.3 Information Not Deemed Private 80
9.4.4 Responsibility to Protect Private Information 81
9.4.5 Notice and Consent to Use Private Information 81
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 81
9.4.7 Other Information Disclosure Circumstances 81
9.5 Intellectual Property Rights 81
9.6 Representations and Warranties 81
9.6.1 CA Representations and Warranties 81
9.6.2 RA representations and warranties 82

Rachel McPherson
2022-02-08

9.6.3 Subscriber Representations and Warranties . . . 82
9.6.4 Relying Party Representations and Warranties . . . 82
9.6.5 Representations and Warranties of Other Participants . . . 82
9.7 Disclaimers of Warranties . . . 82
9.8 Limitations of Liability . . . 82
9.9 Indemnities . . . 82
9.10 Term and Termination . . . 83
9.10.1 Term . . . 83
9.10.2 Termination . . . 83
9.10.3 Effect of Termination and Survival . . . 83
9.11 Individual Notices and Communications with Participants . . . 83
9.12 Amendments . . . 83
9.12.1 Procedure for Amendment . . . 83
9.12.2 Notification Mechanism and Period . . . 83
9.12.3 Circumstances under Which OID must be Changed . . . 84
9.13 Dispute Resolution Provisions . . . 84
9.14 Governing Law . . . 84
9.15 Compliance with Applicable Law . . . 84
9.16 Miscellaneous Provisions . . . 84
9.16.1 Entire Agreement . . . 84
9.16.2 Assignment . . . 84
9.16.3 Severability . . . 85
9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights) . . . 85
9.16.5 Force Majeure . . . 85
9.17 Other Provisions . . . 85

1 Introduction

1.1 Overview

This Certificate Policy (CP) contains the policy adopted by the CA managed by TrustCor Systems S. de R.L. ("TrustCor CA") for the issuance and management of publicly trusted SSL certificates, as adopted by the CA/Browser forum and is designed to be compliant with the criteria stated in Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") version 1.8.1 (available at https://cabforum.org).

TrustCor CA's certificate policies are controlled by the TrustCor Policy Authority (TCPA). The TCPA determines how this CP applies to the entities which make up TrustCor CA's business:

Rachel McPherson
2022-02-08

the Certificate and Registration Authorities (CAs and RAs respectively), the Subscribers and Relying Parties.

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

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

- TrustCor CA Certificate Practice Statements (CPS)
- TrustCor CA Privacy Policy
- TrustCor CA Subscriber Agreements
- TrustCor CA Relying Party Agreements
- TrustCor CA Information Security Policy (see below)

The TrustCor Information Security Policy is comprised of several internal documents. They include, but are not limited to:

Document
Business Continuity and Disaster Recovery Policies
Incident Response Plan
Information Security Policy
Risk Assessment Policy
Staff Workplace Policies

This document is formatted according to the IETF RFC 3647 CP/CPS framework. Sections which do not apply to TrustCor CA, or where TrustCor CA makes no authoritative statement, will have either the text "No stipulation" or "Not Applicable".

1.2 Document Name and Identification

This document is the "TrustCor Systems S. de R.L. Certificate Policy", version 1.8.1, and was approved by the TCPA on 2022-02-08.

Rachel McPherson
2022-02-08

1.2.1 Revisions

Date	Changes	Version
2022-02-08	Updates to Overview to reflect current policy list, and sections 4.9.7, 5 and 8.7 for clarity.	1.8.1
2021-09-22	Update to section 1.6, 3.2.2.4 and 6.3.2 to align with CPS. Updated section 7.1.4.2.2 and 1.6.1 as per SC 48.	1.8.0
2021-07-07	Fixes for typos and explicit statement about validation methods	1.7.2
2021-05-28	Updates to revocation reasoning in 4.9.12	1.7.1
2020-10-20	Updates to verification methods and wildcard policy	1.7.0
2020-03-27	TSA/CodeSign additions	1.6.0
2019-10-21	Clarification and reorganisation of some text	1.5.1
2019-04-19	Major review of all sections	1.5.0
2018-10-23	Revocation guidelines updated	1.4.2
2018-08-15	OCSP response lifetime changes and review	1.4.1
2018-02-16	Update to 3.2.2.4 and CT publication policy	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	More details in policies and compliance with BR 1.4.4	1.3.1

Rachel McPherson
2022-02-08

Date	Changes	Version
2016-09-15	Changes to policies to meet with BRs 1.4.0	1.3.0
2016-07-04	Review of document - no changes made	1.2.1
2016-01-23	This version 1.2.1 corrects the incorrect policyID root 1.3.6.1.4.4 to 1.3.6.1.4.1	1.2.1
2015-11-16	This version 1.2.0 replaces the TrustCor CA Certificate Policy, dated 2015-08-15, being reformatted into RFC 3647 form.	1.2.0

TrustCor CA designates its OIDs with the prefix `1.3.6.1.4.1.44031`

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

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

This Certificate Policy has the OID `1.3.6.1.4.1.44031.1.1.16`

1.3 PKI Participants

1.3.1 Certification Authorities

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

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

1.3.2 Registration Authorities

Registration Authorities (RAs) collect and validate Subscriber details which can then be submitted to TrustCor CA for signing into a certificate. TrustCor CA shall require any external RA (that is, one not run directly by TrustCor CA) to submit policy and practice documentation which is

then reviewed by the TCPA to ensure that it meets the same policy and practice requirements which govern TrustCor CA's own registration processes.

1.3.3 Subscribers

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

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

1.3.4 Relying Parties

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

TrustCor CA shall express the agreement between Relying Parties and TrustCor CA in the form of a Relying Party Agreement, to be published in TrustCor CA's document repository.

1.3.5 Other Participants

The CPS shall describe the nature of any other participants in the PKI services operated by TrustCor Systems S. de R.L., and their role in the service provision.

1.4 Certificate Usage

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

A time-stamp token (TST) is a binding between a representation of data (normally a hashed digest of that data) to a particular timestamp, providing evidence that the data existed in that exact form at that particular time. The binding is signed cryptographically.

Rachel McPherson
2022-02-08

TrustCor CA shall ensure that all certificate holders are bound by a Subscriber Agreement which sets out the permitted uses of the certificate.

1.4.1 Appropriate Certificate Uses

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

1.4.2 Prohibited Certificate Uses

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

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

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

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

Signatures verified by code signing certificates may not be taken to establish that the code so signed is fit for purpose, free of any malware, introduces no vulnerability to the running system or does not contain any bugs.

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

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

1.5.2 Contact Person

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

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

1.5.3 Person Determining CPS Suitability For the Policy

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

1.5.4 CPS approval procedures

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

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

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 issue is required for such major changes.

Rachel McPherson
2022-02-08

1.6 Definitions and Acronyms

1.6.1 Definitions

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

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

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

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

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 (https://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 Certifi-

cates, 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.

Code Signature A Signature logically associated with a signed Object.

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

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

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

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

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

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

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

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

Domain Name Registrant Sometimes referred to as the "owner" of a Domain Name, but more

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

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

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

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

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

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

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

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

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

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

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

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

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

Key Compromise A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there

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

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

Key Pair The Private Key and its associated Public Key.

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

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

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

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

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

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

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

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

Parent Company A company that Controls a Subsidiary Company.

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

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

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

Public Key The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Rachel McPherson
2022-02-08

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

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

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

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

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

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

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

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

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

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

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

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

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

Signing Service An organization that signs an Object on behalf of a Subscriber using a Private

Key associated with a Code Signing Certificate.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Rachel McPherson
2022-02-08

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

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

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

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

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

1.6.2 Acronyms

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

1.6.3 References

The following documents serve as references points to the data presented in this Certificate Policy:

- Mozilla Root Store Policy v2.7.1
- The CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (“Baseline Requirements”, or “BRs”), v1.8.0
- Baseline Requirements for Code-Signing Certificates, v.2.5
- Adobe Approved Trust List, v2.0

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

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

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

2.2 Publication of Certification Information

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

- All trusted root certificates

- All currently used Subordinate CAs directly signed by the root certificates above
- All CRLs issued by any of the CAs mentioned above
- OCSP Responses for current certificates issued by the CAs above
- All current Certificate Policy documents
- All current Certificate Practice Statements
- All privacy policies issued by TrustCor CA

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

2.3 Time or Frequency of Publication

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

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

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

CP and CPS documents must be made publicly available no more than seven (7) days after approval by the TCPA. Other documents mentioned in the overview shall be made available to their respective audiences within, at most, thirty (30) days after approval by the TCPA.

2.4 Access Controls on Repositories

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

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

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

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

3.1.2 Need for Names to Be Meaningful

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

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

Any component of a name must not consist purely of punctuation, or carry the impression that the name component has a `not applicable` or `empty` value.

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

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

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

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

3.1.3 Anonymity or Pseudonymity of Subscribers

TrustCor CA may issue certificate to end-entities who choose to remain anonymous or pseudonymous subject to the restriction that the validation evidence supports the use of the

pseudonym, that the grade of certificate chosen does not prohibit such use, and that the name chosen is canonically unique (eg, whitespace is insignificant, case is insignificant, etc.)

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

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

TrustCor CA may not have two concurrently valid (that is, unexpired and unrevoked) certificates issued by the same CA which have an identical subject DN, excepting a brief overlap as one certificate approaches the end of its life and a new one is issued. The duration of such overlaps shall be defined within the CPS, if they are allowed.

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

Timestamps must have a unique hash and time, or a unique serial number assigned to the timestamp.

3.1.6 Recognition, Authentication, and Role of Trademarks

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

3.2 Initial Identity Validation

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

- Telephone Calls
- SMS messages
- E-mail

- Postal Service

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

3.2.1 Method to Prove Possession of Private Key

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

3.2.2 Authentication of Organization and Domain Identity

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

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

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

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

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

TrustCor CA shall establish processes as per the BR section 3.2.2.1 which it uses to ascertain the identity of an applicant.

Third party databases can be used to establish identity assuming that they meet the criteria established in section 3.2.2.7 of integrity, liveness and authority.

3.2.2.2 DBA/Tradename If a requester wishes to assert the use of a tradename within a certificate, TrustCor CA operational processes shall describe a method to obtain a list of trading bodies within a given national jurisdiction.

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

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

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

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

Where individual identity information is considered, and where national government issued ID is used as proof, the country code will be set to that of the issuing nation, on the understanding that a valid ISO-3166-1 code exists for that nation.

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

Challenges which are sent to applicants must contain sufficient entropy to make a brute force guessing attack infeasible, and shall have a lifespan set to a reasonable timeframe to allow response. Challenges shall follow the construction and use of random values as defined via industry standards.

In the following sections, where policy permits the BR described validation of domains, the CPS shall describe the method (in the identically numbered section) by which this validation is performed. Note that, even if this CP permits issuance, the CPS may still state that no method has yet been defined to put the policy into practice. If this is the case, TrustCor CA shall not issue certificates using the method until the CPS does describe such a process. TrustCor CA may not issue a certificate containing an FQDN which has not been validated by a method explicitly listed in the CPS as being in use and acceptable for its expression within the certificate.

If a validation method is noted as being accepted, it may be used for subdomain and wildcard validation unless noted in the CPS as not being acceptable.

Rachel McPherson
2022-02-08

3.2.2.4.1 Validating the Applicant as a Domain Contact TrustCor CA shall not use domain contact information as a validation method.

3.2.2.4.2 Email, Fax, SMS or Postal Mail to Domain Contact TrustCor CA may use any of the headlined methods to contact applicants for email or domain certificates.

3.2.2.4.3 Phone Contact with Domain Contact TrustCor CA must ensure that only the phone number as presented in the authoritative databases for contacts is used to telephone for validation reasons.

3.2.2.4.4 Constructed Email to Domain Contact TrustCor CA's CPS shall describe a list of approved mailboxes for constructing emails. It must be a subset of those allowed in the BR's for this corresponding section.

3.2.2.4.5 Domain Authorization Document TrustCor CA shall not use DADs to validate requests

3.2.2.4.6 Agreed-Upon Change to Website TrustCor CA shall not use this method to validate requests

3.2.2.4.7 DNS Change TrustCor CA may check for DNS record changes within the domain requested to complete domain control validation. The CPS shall demonstrate that CA formed request tokens are constructed such that it is infeasible for an unauthorized party to guess the content of the desired DNS record.

This method may be used to issue Wildcard Domain Names.

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

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

3.2.2.4.10 TLS Using a Random Number The TLS Random Number method is not to be used by TrustCor CA as a validation method.

3.2.2.4.11 Any Other Method TrustCor CA shall not, under any circumstances, describe a validation method under this section.

Rachel McPherson
2022-02-08

3.2.2.4.12 Validating Applicant as a Domain Contact This method is not to be used by TrustCor CA as a validation method.

3.2.2.4.13 Email to DNS CAA Contact TrustCor CA may use this validation method to validate domain control.

This method may be used to issue Wildcard Domain Names.

3.2.2.4.14 Email to DNS TXT Contact TrustCor CA may use this validation method to validate domain control.

This method may be used to issue Wildcard Domain Names.

3.2.2.4.15 Phone Contact with Domain Contact TrustCor CA may use this validation method to validate domain control.

This method may be used to issue Wildcard Domain Names.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact TrustCor CA may use this validation method to validate domain control.

This method may be used to issue Wildcard Domain Names.

3.2.2.4.17 Phone Context with DNS CAA Phone Contact TrustCor CA may use this validation method to validate domain control.

This method may be used to issue Wildcard Domain Names.

3.2.2.4.18 Agreed-Upon Change to Website v2 TrustCor CA may use this validation method to validate domain control. The CPS shall describe those redirection constraints which must be followed in order to treat the HTTP request as being valid.

This method may NOT be used to issue Wildcard Domain Names.

3.2.2.4.19 Agreed-Upon Change to Website - ACME TrustCor CA may use this validation method to validate domain control.

This method may NOT be used to issue Wildcard Domain Names.

3.2.2.4.20 TLS Using ALPN This method is not be used by TrustCor CA as a validation method.

3.2.2.5 Authentication for an IP Address TrustCor CA shall not issue identities based on either IPv4 or IPv6 addresses.

3.2.2.6 Wildcard Domain Validation TrustCor CA is allowed to issue wildcard certificates, in strict compliance with the Baseline Requirements.

Issuance to a public suffix for wildcard purposes is not allowed, regardless of the ability of an applicant to demonstrate control over that public suffix.

The CPS shall describe how registry controlled domains are identified and rejected if requested.

3.2.2.7 Data Source Accuracy Before allowing a data source to be used as part of any validation process, TrustCor CA must make a judgement that the source is:

- properly constituted to perform such a function
- refreshed regularly (e.g. by receiving company filings regularly)
- likely to produce information of sufficiently high integrity for the purposes of TrustCor CAs information validation requirements.

3.2.2.8 CAA Records Before issuing a certificate designed to be used for terminating a TLS certificate, TrustCor CA shall use DNS checks to validate whether TrustCor CA is entitled to issue certificates for the named domain, by checking the CAA records via DNS, if present.

The CPS shall describe which identifying strings will be used by TrustCor CA to signify that issuance is permissible.

The algorithm to be used for such checking must follow RFC 6844, amended by such errata as exist and have been accepted as canonical by the CA/B Forum.

Where a conflict between a certificate request and CAA authority to publish is found, TrustCor CA shall use its best effort to use iodef fields in the CAA record to report the conflict to the designated end points.

In the event of technical (eg, unsupported critical extensions or DNS) failures making a CAA determination impossible, TrustCor CA shall not issue the certificate.

3.2.3 Authentication of Individual Identity

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

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

  1. his/her date of birth;
  2. his/her current physical address
  3. A valid telephone number.

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

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

  If the requester has an existing relationship at this level, the demonstration of knowledge of appropriate credentials (e.g. passphrase and OTP) shall suffice to prove identity.

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

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

3.2.4 Non-verified Subscriber Information

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

Note that this does not preclude inclusion of subject name components which are derived from TrustCor CA's own set of names (for example, to embed advertising information or strings identifying the business offering under which the certificate was acquired).

3.2.5 Validation of Authority

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

- DV SSL Certificates - the domain name registrar must list the applicant as part of the WHOIS record; or effective control of the domain shall be demonstrated by the applicant or communication satisfying BR 3.2.2.4 shall be obtained.
- OV SSL Certificates - In addition to the communications as per DV SSL Certificates, the CA/RA must also be satisfied that such assurances as per BR 3.2.2.2 and BR 3.2.2.3 have been completed. Specifically, reliable data sources such as government registries of incorporation shall be consulted to verify that the organizational identity can be reasonably asserted in the certificate subject.
- S/MIME Certificates - the requester must demonstrate control over receiving and sending messages from the specified electronic mailbox.
- Level 2 Individual-Organizational Certificates (all types) - the CA must possess communication delivered using a reliable method that the individual has an ongoing association with the organization; and that this communication must be sourced from someone in the organization with the ability to speak authoritatively for its associations (e.g. an HR representative, the signatory to a contract of employment, etc.

3.2.6 Criteria for Interoperation

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

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Upon the premise that validation documentation (ie, that which allowed a certificate to be issued in the first place) is no older than 398 days, TrustCor CA may permit a certificate to be re-issued

using the same names and identity assurance level as the original certificate. A certificate so issued may not be valid for longer than the 398 days **from initial validation**.

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

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

3.3.2 Identification and Authentication for Re-key after Revocation

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

3.4 Identification and Authentication for Revocation Request

Revocation requests must be authenticated to ensure they emanate from authorized personnel. Demonstration of knowledge of a certificate's corresponding private key is sufficient evidence as to validate a revocation request. Other methods (e.g. out of band communications from trusted parties) may also be used to establish the identity of a revocation requester.

Rachel McPherson
2022-02-08

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

TrustCor CA shall accept certificate applications from the general public, with the following caveats:

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

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

If any entity conducts itself in such a way as TrustCor CA feels would damage the reputation of TrustCor Systems or its subsidiary organizations, it may refuse to process an application from such an entity.

TrustCor CA may, but is not required to, inform a rejected applicant as to the reasons why its application will not be processed.

4.1.2 Enrollment Process and Responsibilities

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

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

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

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

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

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

For the issuance of SSL certificates, TrustCor CA will check any domain names against published DNS CAA records to ensure it is not prohibited (or indeed, is expressly allowed) to issue certificates for the domain name which forms part of any SSL Server certificate. This check must be performed for **all** names which will be included in the certificate. The CPS must include the list of strings which the CAA records must include in order to be seen as permitting TrustCor CA to issue certificates to the applicant.

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

TrustCor CA shall not issue certificates to FQDNs under those domains reserved as IANA managed or specified as IANA test domains.

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

4.2.2 Approval or Rejection of Certificate Applications

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

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

4.2.3 Time to Process Certificate Applications

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

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

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

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

Serial numbers on certificates must not be predictable - that is they must contain sufficient entropy as to make guessing serial numbers computationally infeasible. The minimum entropic input shall be guided by the industry standards, such as the BRs.

Root CA certificate issuance (ie, subordinate CAs) may only be performed by specifically authorized individuals (natural persons, not automated processes) possessing the role of `CA Administrator`, issuing specific commands, per the documented Key Generation Script. TrustCor CA shall maintain an internal practice document (Trusted Role Assignment) listing all of the roles and privileges operative within the CA function.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

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

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

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

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The relevant Subscriber agreement shall require a requester to validate that the details present in the certificate match his or her requirements, and to notify TrustCor CA if such requirements have not been met. Subscriber agreements shall also make clear that use of a certificate constitutes acceptance.

4.4.2 Publication of the Certificate by the CA

End entity SSL certificates may be published upon issuance into Certificate Transparency logs. The CPS shall describe such publication mechanisms, if any are in operation. TrustCor CA shall publish certificates into such CT logs as are necessary to satisfy the various certificate transparency policies as published by the browser programs.

CA certificates shall be published by TrustCor CA onto a well known, and TrustCor CA managed, repository.

4.4.3 Notification of certificate issuance by the CA to other entities

Other than CT publication noted in section 4.4.2, TrustCor CA need make no further stipulation for notification.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The Subscriber shall be required by the relevant Subscriber agreement not to release to unauthorized parties any private key corresponding to an issued certificate.

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

The Subscriber agreements shall make clear that certificate may only be used for the purposes designated by the keyUsage and extendedKeyUsage flags, along with any other such policy conditions expressed within this document governing certificate use.

4.5.2 Relying Party Public Key and Certificate Usage

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

The Relying Party Agreement shall further make clear that TrustCor CA gives no guarantee to a relying party other than that the requester of a certificate has provided sufficient evidence to warrant issue of a certificate bearing the identifiers presented.

4.6 Certificate Renewal

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

4.6.1 Circumstance for Certificate Renewal

TrustCor CA may renew certificates when:

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

4.6.2 Who May Request Renewal

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

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

4.6.3 Processing Certificate Renewal Requests

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

4.6.4 Notification of New Certificate Issuance to Subscriber

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

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

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

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

4.6.6 Publication of the Renewal Certificate by the CA

The publication requirements are as per Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The CPS shall describe the notification methods used by the CA to log any renewed certificate issuance. Particular mention shall be made of the Certificate Transparency policy which the CA shall use (if applicable to the type of certificate issued).

4.7 Certificate Re-key

Re-key is defined as the re-release of a certificate bearing the same identity information as an older certificate, but with a different public key embedded within it.

4.7.1 Circumstance for Certificate Re-key

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

Otherwise a new issuance process must be undertaken.

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

4.7.2 Who May Request Certification of a New Public Key

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

4.7.3 Processing Certificate Re-keying Requests

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

4.7.4 Notification of New Certificate Issuance to Subscriber

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

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

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

As before, demonstrated use of the certificate constitutes acceptance.

4.7.6 Publication of the Re-keyed Certificate by the CA

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

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The CPS shall describe the methods used to notify any other entities of a rekeyed certificated being issued, including any Certificate Transparency logging function (if applicable to the type of certificate).

4.8 Certificate Modification

Certificate modification is defined as being the re-release of a certificate using the same public key as an older one, but with the identity information within altered.

4.8.1 Circumstance for Certificate Modification

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

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

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

If the new set of dNSNames is not a strict superset, then the old certificate must be revoked and a new certificate issued. In this case, TrustCor CA may, should it choose, allow the same

public key to be used in the new certificate, and the reason for revocation shall be given as `superseded`.

In the case of multiple dNSName certificates: this is the only case in which an application which lists a previously used public key may be deemed acceptable for certificate issuance - on the assumption that the certificate containing the previously used public key has not been revoked.

4.8.2 Who May Request Certificate Modification

TrustCor CA may institute certificate modification.

The Subscriber may request certificate modification.

4.8.3 Processing Certificate Modification Requests

The constraints of Section 3.3.1 obtain while processing modification requests.

4.8.4 Notification of New Certificate Issuance to Subscriber

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

4.8.5 Conduct Constituting Acceptance of Modified Certificate

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

As before, demonstrated use of the certificate constitutes acceptance.

4.8.6 Publication of the Modified Certificate by the CA

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

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

The CPS shall describe any notification to other entities for any certificate issued after modification, including any Certificate Transparency logging (if applicable to the type of certificate)

4.9 Certificate Revocation and Suspension

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

TrustCor CA will describe in its CPS how Subscribers or other third parties shall request revocation for certificates issued by TrustCor CA.

TrustCor CA shall not permit certificate suspension for any of its Issuing CAs.

4.9.1 Circumstances for Revocation

TrustCor CA will revoke certificates if:

- The Subscriber makes an authenticated request that his/her certificate be revoked
- The Subscriber chooses not to accept a certificate as not being satisfactory
- A certificate has been not been issued according to the policies described in this CP, or in the CPS which satisfies it.
- For code signing certificates, if the Application Software Supplier requests revocation
- For code signing certificates, if the certificate is being used for Suspect Code
- It is brought to TrustCor CA's attention that the private key for the certificate is no longer in the sole control of the Subscriber
- The Subscriber no longer has the right to assert any of the details described in the certificate, such as trade names, trademarks, association with an organization noted in the certificate, etc.
- TrustCor CA has received a properly issued, legally binding order to revoke a certificate from a competent legal authority
- TrustCor CA ceases operations and no successor organization has taken over its obligations
- The details present in the certificate is deemed to mislead or confuse relying parties
- The Subscriber engages in behavior which is in material breach of the relevant Subscriber agreement
- The Subscriber appears, subsequent to issue, on a blacklist of entities or embargoed nations issued by the government of the United States of America, and that this information becomes known to TrustCor CA.
- The Subscriber does not take delivery of the certificate within a reasonable time frame (where the certificate is delivered by request to TrustCor CA).

Since it is part of the Subscriber agreement that a Subscriber must notify TrustCor CA of any changes in circumstance which would prevent the details of the certificate being accurate, failure

to so inform constitutes a material breach of the Subscriber agreement, and thus revocation is warranted.

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

1. The Subscriber requests in writing that TrustCor CA should revoke the Certificate;
2. The Subscriber notifies TrustCor CA that the original certificate request was not authorized, and that authorization is not being granted retroactively;
3. TrustCor CA obtains evidence (whether from the Subscriber or elsewhere) that the Subscriber's Private Key corresponding to the Public Key in the Certificate has been compromised; or
4. TrustCor CA becomes aware that the validation process for domain authorization or control for any FQDN in the Certificate should not be relied upon.

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

1. The Certificate no longer satisfies the requirements of Sections 6.1.5 and 6.1.6;
2. TrustCor CA becomes aware that the Certificate was misused;
3. TrustCor CA becomes aware that a Subscriber has violated one or more of its obligations under this CP, any CPS gov, Subscriber Agreement and/or Terms of Use;
4. TrustCor CA becomes aware that any FQDN or email address in a Certificate is no longer legally permitted (this can include such conditions as a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
5. TrustCor CA becomes aware of a material change in the information contained in the Certificate;
6. TrustCor CA becomes aware that the Certificate issuance was not performed in accordance with this CP, or any CPS governed by this CP;
7. TrustCor CA determines that any of the information appearing in the Certificate is not accurate;
8. TrustCor CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless TrustCor CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by TrustCor CA's this CP or any CPS governed by this CP;
10. TrustCor CA becomes aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calcu-

late it based on the Public Key, or if there is clear evidence that the specific method used to generate the Private Key was flawed; or

11. TrustCor CA determines that the ongoing existence of the Certificate represents an unacceptable risk to its business operations.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

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

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

4.9.2 Who Can Request Revocation

The Subscriber owning a certificate can request revocation.

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

Application Software Suppliers and Anti-Malware organisations can request revocation of code signing certificates.

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

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

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

4.9.3 Procedure for Revocation Request

Any request for revocation must:

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

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

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

4.9.4 Revocation Request Grace Period

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

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

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

Any holder of a Subordinate CA private key must make compromise known to TrustCor CA within 1 hour. This, obviously, includes TrustCor CA itself.

4.9.5 Time within Which Ca Must Process the Revocation Request

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

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

Code signing certificates must be revoked within the timeframe set out in the MRCS, section 13.1.5.

4.9.6 Revocation Checking Requirement for Relying Parties

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

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

4.9.7 CRL Issuance Frequency (if Applicable)

For the status of Subscriber Certificates, the CRL shall be updated and reissued at least once every twenty-four (24) hours, and the value of the nextUpdate field must not be more than four (4) days beyond the value of the thisUpdate field.

For the status of Subordinate CA Certificates, CRLs shall be updated and reissued at least once every six (6) months and within twenty-four (24) hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field must not be more than six (6) months beyond the value of the thisUpdate field.

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

4.9.8 Maximum Latency for CRLs (if Applicable)

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

4.9.9 On-line Revocation/Status Checking Availability

TrustCor CA shall provide OCSP servers configured in a high availability mode such that the uptime guarantees of Section 2.1 can be met. Every certificate (excluding infrastructure certificates like dedicated OCSP responders and root CA certificates) shall be able to be validated in an OCSP via a URI published within the certificate.

4.9.10 On-line Revocation Checking Requirements

RPs must have OCSP client software which adheres to RFC 6960 specifications in order to use the OCSP services. TrustCor CA is allowed to constrain its responses to adhere to the profiles set out in RFC 5019.

4.9.11 Other Forms of Revocation Advertisements Available

For each issuing CA, the CPS shall describe any other methods of revocation advertisement used (as well as CRLs and OCSP). Each method must adhere to the following policies:

- the latency and frequency requirements must be in line with those required for CRLs in sections 4.9.5, 4.9.7, and 4.9.8
- the method must preserve integrity and availability properties to at least the equivalent of the CRL and OCSP services described in the CPS.

4.9.12 Special Requirements Related to Key Compromise

In the event that TrustCor CA discovers that private keys under its ownership have become compromised, TrustCor CA shall make all reasonable efforts to communicate this information to any Relying Parties as well as those contacts within browser root certificate programs in which TrustCor CA is a member.

The CPS shall make clear what methods may be used, either by subscribers or the public at large, how to indicate that a private key corresponding to a TrustCor CA issued certificate should be considered to be compromised.

4.9.13 Circumstances for Suspension

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

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

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

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

For Code Signing certificates, revocations will remain in the CRL and OCSP responses for at least 10 years after the expiration of the revoked certificates.

OCSP services must not return a 'good' response to queries for certificates which have not been issued.

4.10.2 Service Availability

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

4.11 End of Subscription

Subscriber Agreements terminate upon revocation of all certificates issued under that Agreement, unless the Subscriber elects to request new certificates under the same Subscription Agreement, or such business offerings as TrustCor CA deems similar in nature to the previous agreement.

4.12 Key Escrow and Recovery

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

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

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

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 abides by the language in the CPS.

5.1.1 Site Location and Construction

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

- Not located in areas likely to exhibit hazard of environmental damage, chemical, biological or radiological pollution
- Possessed of redundant stable electricity supplies from at least two separate providers
- Physically separated areas for visitor reception, clearance and computer equipment hosting
- Capable of safely storing, separate to any computer equipment, fuel to power facilities in the event of loss of mains power

5.1.2 Physical Access

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

- A log in durable form is kept of every visitor to the facility listing their affiliation, name, purpose of visit and area of visit

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

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

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

5.1.3 Power and Air Conditioning

Any data center housing TrustCor CA services must have:

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

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

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

5.1.4 Water Exposures

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

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

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

5.1.5 Fire Prevention and Protection

The data center must provide regularly tested, reliable fire suppression systems.

5.1.6 Media Storage

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

5.1.7 Waste Disposal

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

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

5.1.8 Off-site Backup

TrustCor CA makes regular backups of system data to ensure copies are retained for disaster recovery purposes. These backups are stored off-site, deemed company sensitive information and must be encrypted during transit. Backup data access is restricted to TrustCor CA personnel. The off-site facility must retain adequate physical security and procedural controls in place to protect against unauthorized access and fire or flood damage.

5.2 Procedural Controls

5.2.1 Trusted Roles

The following abilities are deemed to be trusted roles:

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

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

The following abilities are deemed to be highly trusted roles:

- The ability to cause the root certificate key store to sign a certificate request
- The ability to cause the root certificate key store to sign a CRL
- The ability to transfer an HSM stored private key to another HSM
- The ability to physically access the equipment of TrustCor CA
- The ability to alter production profiles governing the issuance of certificates from TrustCor CA (e.g. the duration of a certificate, the appropriate key types and lengths of public keys, etc.)

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

5.2.2 Number of Persons Required per Task

TrustCor CA requires that highly trusted operations require at least two people performing their specific roles to conduct the operation.

5.2.3 Identification and Authentication for Each Role

Any CA operations require individual authentication using management issued credentials to perform the operation. Generic administrative users accounts **must not** be used for such pur-

poses. The logs must show which actual principal performed the operation.

5.2.4 Roles Requiring Separation of Duties

Every person in TrustCor CA's employ who is authorized to perform duties within a trusted role shall be given such authority as allows them to act in exactly one of the roles listed in Section 5.2.1 at a time.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

TrustCor CA shall ensure that, prior to engagement in any trusted role, a person has been vetted to confirm both identity and trustworthiness. In addition, said person will be evaluated for potential conflict of interest and cannot appear on a prohibited list of persons, or affiliated to any proscribed organization, issued by the government of the United States of America.

5.3.2 Background Check Procedures

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

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

5.3.3 Training Requirements

TrustCor CA must maintain records of training and ensure that employees and contractors maintain skill levels consistent with internal training policies and programs for their role. In addition, any employee or contractor in the Validation Specialist role must demonstrate skill level ability prior to performing validation tasks and are required to pass an exam.

5.3.4 Retraining Frequency and Requirements

All persons in a Trusted Role must demonstrate skill level consistent with TrustCor CA's expectations in regards to the specific role requirements. If the TCPA deems that new training is required for any personnel as a result of actual or likely changes in CA/RA behavior, TrustCor CA shall provide that training and document in the internal knowledge base accordingly.

5.3.5 Job Rotation Frequency and Sequence

TrustCor CA is not required to rotate staff between different roles, although it may do so at management's discretion.

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, regardless of intent, carries the possibility of disciplinary action up to and including termination of employment and criminal sanctions.

5.3.7 Independent Contractor Requirements

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

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

All logs of auditable events must maintain a timestamp, a human readable description of the entry and the identity of the persons or principals causing, or being involved in, the event to be noted.

Logs may be maintained as manual documents or via electronic means.

Logs must be generated in accordance with any privacy policies established by TrustCor, and personal identifying information treated so as to be in compliance with that policy.

5.4.1 Types of Events Recorded

The types of events which are to be recorded shall include, at a minimum (but not restricted to):

Rachel McPherson
2022-02-08

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.
  - 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 for Processing and Archiving Audit Logs

Internal log review shall be performed at frequent intervals (at least quarterly). Anomalies, suspicions of loss of confidentiality or integrity are documented and treated as actionable events for TrustCor CA personnel.

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

5.4.3 Retention Period for Audit Logs

Audit logs must be retained for a minimum of 7 years. If any audit information pertains to a certificate issued by TrustCor CA, that log information must be maintained for 7 years past the date where the certificate ceases to be valid.

Audit logs shall be retained on site until they have been reviewed.

Audit logs must be made available to the Qualified Auditor as part of the regular external audit process.

5.4.4 Protection of Audit Log

TrustCor CA shall ensure that (i) only authorized personnel have read-only access to logs, (ii) only authorized personnel may archive audit logs, and (iii) audit logs are not modified.

Intruder detection systems shall be configured to report log file shrinkage or unexpected alteration.

Audit logs are deemed to be company confidential, and shall be treated as such per the company's information security policy. Specifically, logs must be generated and stored in such a way as to make tampering of the log record easily detectable. The confidentiality must be maintained if the logs are transferred outside of company hardware.

5.4.5 Audit Log Backup Procedures

Audit logs shall be saved and stored offsite daily; the logs so stored shall retain their sensitivity as described in 5.4.4.

5.4.6 Audit Log Accumulation System (internal vs. external)

Automated audit logs must run from system startup to shutdown. If a node is no longer logging, it becomes suspect, and the TCPA shall determine to suspend CA operations depending on severity of the event.

5.4.7 Notification to Event-Causing Subject

TrustCor CA is not required to notify a subject that it has been the cause of an auditable event.

5.4.8 Vulnerability Assessments

TrustCor CA shall maintain a regular (performed at least once per year) review of internal and external threats which could harm the integrity, confidentiality or availability of TrustCor CA PKI systems or data. Each threat shall be categorized with respect to its scope of harm (which must include the sensitivity of the data which the relevant systems handle), likelihood/prevalence of exploit, and possible mitigations to counter the threat.

Each threat so identified shall be entered into a risk assessment policy document, and TrustCor CA shall then judge whether the existing policies, procedures or security postures are sufficient to accept the risk, or whether changes to the same are needed to protect the integrity and confidentiality of TrustCor CA systems, personnel and customers.

5.5 Records Archival

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

5.5.1 Types of Records Archived

TrustCor CA archives all records of certificate requests, verification and revocation. TrustCor CA may also archive other items related to CA operations in accordance with the CPS Sections 5.5.1 and 5.4.1.

5.5.2 Retention Period for Archive

All documentation relating to certificate requests, including the verification and revocation thereof, must be retained for at least seven years after any Certificate based on that documentation ceases to be valid.

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

Archive data is backed up securely and on a regular basis in accordance with the CPS. This data must be readily accessible in the event of disaster to the primary archive.

5.5.5 Requirements for Time-stamping of Records

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

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

5.5.6 Archive Collection System (internal or external)

Archive data shall be collected internally by TrustCor CA.

5.5.7 Procedures to Obtain and Verify Archive Information

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

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

Where archive data is electronically generated, archive generating systems shall use integrity codes to establish that the archive data has not been altered. Document control systems shall also use integrity coding to ensure that changes to documents can be checked as being valid.

5.6 Key Changeover

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

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

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

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

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

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

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

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

5.7.3 Recovery Procedures After Key Compromise

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

If any CA key is discovered to have been compromised, or is suspected of compromise, the TCPA shall investigate and determine what actions must be taken, given the nature and extent of that compromise.

If indeed a compromise has occurred, TrustCor CA must revoke the certificate as described in Section 4.9.5 and proceed with notification described in Section 4.9.12.

5.7.4 Business Continuity Capabilities after a Disaster

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

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

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

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

Further notification must be made to:

- The operators of any browser root certificate programs
- The CA/B Forum

5.8 CA or RA Termination

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

Rachel McPherson
2022-02-08

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation CA private keys must be only be generated on HSMs rated to FIPS 140-L3 or EAL 4 or higher.

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

6.1.1.2 Subscriber Key Pair Generation TrustCor CA does not generate private key materials for Subscribers.

6.1.2 Private Key Delivery to Subscriber

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

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

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

6.1.5 Key Sizes

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

The minimum ECDSA key size used for TrustCor CA keys is 256 bits.

The minimum hash used for any certificate embedded signature is SHA-256, although SHA-512 is also rated as acceptable.

OCSP responder signatures use a minimum hash of SHA-256. Requests to use lower strength digests in signatures must be denied.

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

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

6.1.6 Public Key Parameters Generation and Quality Checking

Any software deployed by TrustCor CA shall enforce the mandates of the CA/B Forum Basic Requirements (BRs), Section 6.1.6 regarding public key parameters generation. The version of the BRs used for this enforcement will be given in this document in Section 1.1 (Overview). TrustCor CA must not sign any certificate request which contains known weak keys.

6.1.7 Key Usage Purposes

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

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

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

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

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

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

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

- Level 1 - No restrictions placed on Subscriber
- Level 2 - FIPS 140 Level 1 (Hardware or Software)

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

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

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

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

6.2.3 Private Key Escrow

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

6.2.4 Private Key Backup

All CA private keys are backed up to a device which has at least the same system protections as the originating device (See Section 6.2.1). These backup devices, if not stored in a data center, must be removed to secure offsite locations under TrustCor CA's control. An audit record must

exist to show authenticated access when either removing or storing a backup device in offsite locations.

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

6.2.5 Private Key Archival

TrustCor CA does not archive its private keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

All CA keys must be generated by, and stored in a cryptographic module as per Section 6.2.1. Export (for key backup procedures) may only be done using an encrypted transfer to another cryptographic module providing the same guarantees of security. The exported data for transfer must be encrypted in such a way as to protect the private key from exposure.

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

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

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

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

6.2.9 Method of Deactivating Private Key

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

6.2.10 Method of Destroying Private Key

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

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

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

TrustCor CA certificates have a maximum validity period of:

Certificate Type	Maximum Validity Period
Root CA	15 years
Subordinate CA	15 years
External Subordinate CA	1128 days

The Subordinate CA certificate may not live longer than the Root CA certificate. No end entity certificate issued under an external Subordinate CA may have a lifetime greater than 398 days.

End entity certificates have the following certificate validity periods:

Certificate Type	Maximum Validity Period
DV SSL	398 days
OV SSL	398 days

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

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

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

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

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

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

6.4.2 Activation Data Protection

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

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

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

6.4.3 Other Aspects of Activation Data

Activation data may not be stored in any fashion other than described as permissible within the TrustCor CA security policies.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

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

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

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

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

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

6.5.2 Computer Security Rating

TrustCor CA is entitled to use any computer systems which its security policy personnel has approved for processing of highly sensitive data.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

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

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

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

6.6.2 Security Management Controls

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

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

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

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

6.6.3 Life Cycle Security Controls

Expiry and rotation of credentials are described in TrustCor CA's security policy. All trusted personnel are required to be familiar with those documents and to adhere to their restrictions with regard to the life cycle of equipment, software and credentials.

6.7 Network Security Controls

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

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

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

6.8 Time-stamping

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

All timestamping services shall be synchronised to at least one GPS receiver as well as more than one NTP service of at least Stratum 3. Time stamping policies are performed in accordance with RFC 3161

All clock adjustments of more than 1 second are auditable events.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version Number(s)

TrustCor CA issues X.509 version 3 certificates.

7.1.2 Certificate Content and Extensions

The CPS shall describe the extension used in TrustCor CA and end-entity certificates, and any rules regarding the permissible combinations of those extensions.

7.1.3 Algorithm Object Identifiers

All CAs whose certificates embed RSA public keys must sign certificates using one of the following algorithms:

- sha256withRSAEncryption (1.2.840.113549.1.1.11)
- sha384withRSAEncryption (1.2.840.113549.1.1.12)
- sha512withRSAEncryption (1.2.840.113549.1.1.13)

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

7.1.4 Name Forms

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

- subject:emailAddress (OID 1.2.840.113549.1.9.1)
- subject:commonName (CN) (OID: 2.5.4.3)
- subject:organizationalName (O) (OID: 2.5.4.10)
- subject:stateOrProvinceName (ST) (OID: 2.5.4.8)
- subject:localityName (L) (OID: 2.5.4.7)
- subject:countryName (C) (OID: 2.5.4.6)

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

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

7.1.4.2 Subject Information - Subscriber Certificates Subscriber Certificates need not contain a Subject DN. However, if a certificate does not contain one, then any `subjectAltName` extension must be marked as **critical**.

7.1.4.2.1 Subject Alternative Name Extension TrustCor CA will only append subjectAltNames with a dNSNames tag followed by an FQDN or wildcard followed by a FQDN for a domain which was validated during application. IP addresses are not to be used.

7.1.4.2.2 Subject Distinguished Name Fields For Level 1 certificates, the subject shall be entirely:

- CN={fqdn or Wildcard Domain Name of subject}

For Level 2 certificates, the subject shall be entirely:

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

Note that while L, or ST must be present, a certificate need not include *both* attributes and values.

7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates

7.1.4.3.1 Subject Distinguished Name Fields For Root Certificates the format of all Subject DNs shall be:

1. subject:commonName (OID 2.5.4.3): *Name of Root CA*
2. subject:organizationalUnitName (OID: 2.5.4.11): TrustCor Certificate Authority
3. subject:organizationName (OID: 2.5.4.10): TrustCor Systems S. de R.L.
4. subject:localityName (OID: 2.5.4.7): Panama City
5. subject:stateOrProvinceName (OID: 2.5.4.8): Panama
6. subject:countryName (OID: 2.5.4.6): PA

For Subordinate Certificates the format of all Subject DNs shall be:

- subject:commonName (OID: 2.5.4.3): *Name of Subordinate CA*
- subject:organizationalUnitName (OID: 2.5.4.11): TrustCor Network
- subject:organizationName (OID: 2.5.4.10): TrustCor Systems S. de R.L.
- subject:localityName (OID: 2.5.4.7): Panama City
- subject:stateOrProvinceName (OID: 2.5.4.8): Panama
- subject:countryName (OID: 2.5.4.6): PA

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

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

7.1.5 Name Constraints

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

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

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

In addition to this, the name constraints contains an excludedSubtrees value of:

- IP: 0.0.0.0/0.0.0.0
- IP: 0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0

to prevent issuance of ipAddress certificates.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Reserved Certificate Policy Identifiers Level 1 SSL client and server certificates shall contain a CPI of 2.23.140.1.2.1 (DV identifier)

Level 2 certificates for SSL, Timestamping and Code Signing must contain a CPI 2.23.140.1.2.2 (OV identifier)

Level 2 S/MIME certificates must contain a CPI of 2.23.140.1.2.3 (IV identifier) or 2.23.140.1.2.2 (OV identifier) depending on whether the certificate is intended to identify a natural person or an email address from a validated organization.

All code signing certificates intended for use in Microsoft Authenticode environments shall have a CPI with OID 2.23.140.1.4.1 (adherence to Minimum Requirements for Code Signing).

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

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

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

7.1.7 Usage of Policy Constraints Extension

TrustCor CA certificates shall not contain a Policy Constraints extension.

7.1.8 Policy Qualifiers Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

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

7.2 CRL Profile

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

The CRLs may use any extensions described in RFC 5280, and such usage must be described in the CPS.

The CRL Number extension (RFC 5280 Section 5.2.3) must be present in all CRLs issued.

7.3 OCSP Profile

7.3.1 Version Number(s)

OCSP requests and responses are at version 1, defined in RFC 6960.

7.3.2 OCSP Extensions

TrustCor CA OCSP responses may support any extension described in RFC 6960. If used, the CPS must detail what those extensions are.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The policies described in this document are designed to satisfy the requirements of the AICPA/CPA Canada WebTrust Program for Certification Authorities and the latest version of

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

8.1 Frequency or Circumstances of Assessment

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

- any company operating a root certificate program for browsers which TrustCor CA has joined
- the CA/B Forum

8.2 Identity/qualifications of Assessor

TrustCor CA shall use a qualified auditor that meets Section 8.2 of the Baseline Requirements.

Unless stated otherwise, an auditor must be selected from the list of WebTrust's licensed practitioners.

8.3 Assessor's Relationship to Assessed Entity

TrustCor CA shall utilize independent auditors that do not have any financial interest or business relationship that could foreseeably create a significant bias for or against TrustCor CA.

8.4 Topics Covered by Assessment

Any audit must conform to industry standards, cover TrustCor CA's compliance with its business practices, as disclosed within this CP, the accompanying CPS and any other related documents TrustCor CA uses to describe its business operations and policies.

8.5 Actions Taken as a Result of Deficiency

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

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

8.6 Communication of Results

The results of all compliance audits will be sent to the TCPA and to any third party entities which are entitled by law or regulation to receive a copy of the audit results. Such parties will include WebTrust and the Common CA Database.

TrustCor CA shall make its audit report publicly available no later than three months after the end of the audit period.

8.7 Self-Audits

TrustCor CA is required to perform regular internal audits of its operations, personnel, and compliance with this CP.

TrustCor CA must also perform a self-audit on a quarterly basis against a random sample of at least three percent of each, SSL and Code Signing, end-entity certificates issued since the last self-audit to ensure compliance with the certificate policies and practices in force at the time of certificate issuance. The result of this log shall be noted in the company's audit log and form part of the company archives.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

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

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

TrustCor CA may charge such fees for access to its revocation or certificate status information as its business offerings dictate.

9.1.4 Fees for Other Services

TrustCor CA may charge such fees for any of its other services as it sees fit, and those charges shall be described in the relevant Subscriber Agreement, Relying Party Agreement or Reseller Agreement, or any other commercial service agreement which TrustCor CA uses.

9.1.5 Refund Policy

Any refund policy shall be described in the relevant Subscriber Agreement, Relying Party Agreement or Reseller Agreement, or any other commercial service agreement which TrustCor CA uses.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

TrustCor CA's CPS and warranty documentation shall describe the insurance coverage for its business activities.

9.2.2 Other Assets

Any other assets which bear upon TrustCor CA's financial responsibilities shall be described in the CPS or relevant warranty documentation.

9.2.3 Insurance or Warranty Coverage for End-entities

TrustCor CA shall maintain Professional Liability/Errors and Omissions insurance with policy limits of at least one million US dollars in coverage.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

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

9.3.2 Information Not within the Scope of Confidential Information

TrustCor CA may treat any information not regarded as confidential in the CPS as public information.

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

All PII not publicly available in the contents of a certificate or CRL is deemed to be private, and must not be disclosed except under the terms of the privacy policy.

TrustCor CA shall protect private information in its possession using a reasonable degree of care and appropriate safeguards.

9.4.3 Information Not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

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

9.4.5 Notice and Consent to Use Private Information

As part of a Subscriber Agreement, all Subscribers consent to the global transfer of any personal data contained in the Certificate and agree to allow TrustCor CA to handle any PII required for the issuance and maintenance of certificates.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

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

9.4.7 Other Information Disclosure Circumstances

If any publication relating to disclosure of non-public information is performed by TrustCor CA, it shall make this known via the mailing lists of the CA/Browser Forum.

9.5 Intellectual Property Rights

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

TrustCor CA shall describe any CA warranties in its CPS, which may in turn refer to other published business documentation. These warranties are considered additional to the warranties described in BR section 9.6.1.

9.6.2 RA representations and warranties

TrustCor CA shall describe any RA warranties in its CPS. All RAs operating on behalf of TrustCor CA shall be bound by these warranties.

9.6.3 Subscriber Representations and Warranties

TrustCor CA shall describe the warranties required of any applicant in its relevant Subscriber Agreements or Terms of Use documents. These terms shall include all conditions described in BRs Section 9.6.3.

9.6.4 Relying Party Representations and Warranties

TrustCor CA shall describe such warranties required of relying parties in its Relying Party Agreement.

9.6.5 Representations and Warranties of Other Participants

Any other warranties and representations shall be described in the Agreements or Terms of Use documents which pertain to those other parties.

9.7 Disclaimers of Warranties

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

9.8 Limitations of Liability

TrustCor CA may limit its liability to any extent not otherwise prohibited by this CP, provided that TrustCor CA remains responsible for complying with this CP and the CPS. Any limitations of liability shall be outlined in the CPS.

9.9 Indemnities

The CPS shall describe any indemnifications which obtain from CAs, Subscribers and Relying Parties.

9.10 Term and Termination

9.10.1 Term

This CP is in effect from the time of its approval and publication to the online repository and remain in effect until replaced with a newer version.

9.10.2 Termination

This CP and any amendments remain in effect until replaced by a newer version.

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

TrustCor CA accepts digitally signed or paper notices related to this CP that are addressed to the locations specified in Section 2.2.

9.12 Amendments

9.12.1 Procedure for Amendment

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

9.12.2 Notification Mechanism and Period

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

9.12.3 Circumstances under Which OID must be Changed

See Section 1.5.4

9.13 Dispute Resolution Provisions

Before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution, a party must notify TrustCor CA of the dispute with a view to seek dispute resolution.

9.14 Governing Law

The substantive laws of the Republic of Panama govern the interpretation, construction and enforcement of this CP and all matters related to it, including tort claims, without regards to any conflict-of-law provisions.

9.15 Compliance with Applicable Law

This CP is subject to all applicable laws and regulations. Subject to the PII provisions of section 9.4.5, TrustCor CA shall meet the requirements of the data protection regulations of the European Union regarding access, disclosure and destruction of personal data and maintain appropriate technical and organization measures.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Any RAs involved in Certificate issuance shall be obligated under contractual agreement with TrustCor CA to comply with this CP and applicable industry guidelines.

9.16.2 Assignment

No entity operating under this CP may 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 CP is held invalid or unenforceable by a court of competent jurisdiction, the remainder of this CP will remain valid and enforceable.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

TrustCor CA may seek indemnification and any fees (including reasonable attorney's fees and court costs) from a party for damages, losses and expenses related to that party's conduct.

TrustCor CA's failure to enforce a provision of this CP does not waive TrustCor CA's right to enforce the same provision later, or right to enforce any other provision of this CP (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 CP, where such interruption or failure is caused by an event outside TrustCor CA's reasonable control.

9.17 Other Provisions

All Certificates issued by TrustCor CA are the property of TrustCor CA. Permission is given to reproduce and distribute on a non-exclusive, royalty-free basis **provided** that the reproduction is performed in full.

Private keys for Subscriber Certificates are **not** owned by TrustCor CA, but remain the property and responsibility of the Subscriber.