

TLS Certificate Policy / Certification Practice Statement

Version 5.1.3

IdenTrust Services LLC.

November 15, 2026

Copyright © 2026 IdenTrust Services, LLC. All rights reserved.

Table of Contents

1 INTRODUCTION 2
1.1 Overview 2
1.2 Document Name and Identification 3
1.2.1 Alphanumeric Identifier 3
CP-CPS Document Versions 3
1.2.2 Object Identifier 4
1.3 PKI Participants 5
1.3.1 Certification Authorities 5
1.3.2 Registration Authorities 5
1.3.3 Subscribers 7
1.3.4 Relying Parties 7
1.3.5 Other Participants 7
1.4 Certificate Usage 8
1.4.1 Appropriate Certificate Uses 8
1.4.2 Prohibited Certificate Uses 8
1.5 Policy Administration 9
1.5.1 Organization Administering the Document 9
1.5.2 Contact Person 9
1.5.3 Certificate Problem Reporting 9
1.5.4 Person Determining CP-CPS Suitability for the Policy 9
1.5.5 CP-CPS Approval Procedures 9
1.6 Definitions and Acronyms 10
1.6.1 Definitions 10
1.6.2 Acronyms 24
1.6.3 References 25
1.6.4 Conventions 25
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 25
2.1 Repositories 25
2.2 Publication of Certification Information 25
2.3 Time or Frequency of Publication 26
2.4 Access Controls on Repositories 26
3 IDENTIFICATION AND AUTHENTICATION 26
3.1 Naming 26
3.1.1 Types of Names 26
3.1.2 Need for Names to Be Meaningful 26
3.1.3 Anonymity or Pseudonymity of Subscribers 27
3.1.4 Rules for Interpreting Various Name Forms 27
3.1.5 Uniqueness of Names 27
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
3.2.3 Authentication of Individual Identity 41
3.2.4 Non-Verified Subscriber information 41
3.2.5 Validation of Authority 42
3.2.6 Criteria for Interoperation 44
3.3 Identification and Authentication for Re-Key Requests 46
3.3.1 Identification and Authentication for Routine Re-Key 46
3.3.2 Identification and Authentication for Re-Key after Revocation 46
3.4 Identification and Authentication for Revocation Requests 46
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 46
4.1 Certificate Application 46
4.1.1 Who Can Submit a Certificate Application 46
4.1.2 Enrollment Process and Responsibilities 48
4.2 Certificate Application Processing 48
4.2.1 Performing Identification and Authentication Functions 48
4.2.2 Approval or Rejection of Certificate Applications 52
4.2.3 Time to Process Certificate Applications 52
4.3 Certificate Issuance 52
4.3.1 CA Actions During Certificate Issuance 53
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 54
4.4 Certificate Acceptance 55
4.4.1 Conduct Constituting Certificate Acceptance 55
4.4.2 Publication of the Certificate by the CA 55
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 55
4.5 Key Pair and Certificate Usage 55
4.5.1 Subscriber Private Key and Certificate Usage 55
4.5.2 Relying Party Public Key and Certificate Usage 55
4.6 Certificate Renewal 56
4.6.1 Circumstance for Certificate Renewal 56
4.6.2 Who May Request Renewal 56
4.6.3 Processing Certificate Renewal Requests 56
4.6.4 Notification of New Certificate Issuance to Subscriber 56
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 56
4.6.6 Publication of the Renewal Certificate by the CA 56
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 56
4.7 Certificate Re-Key 56
4.7.1 Circumstance for Certificate Re-Key 57
4.7.2 Who May Request Certification of a New Public Key 57
4.7.3 Processing Certificate Re-Keying Requests 57
4.7.4 Notification of New Certificate Issuance to Subscriber 57
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 57
4.7.6 Publication of the Re-Keyed Certificate by the CA 57
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 57
4.8 Certificate Modification 57
4.8.1 Circumstance for Certificate Modification 57
4.8.2 Who May Request Certificate Modification 58
4.8.3 Processing Certificate Modification Requests 58

4.8.4 Notification of New Certificate Issuance to Subscriber 58
4.8.5 Conduct Constituting Acceptance of a Modified Certificate 58
4.8.6 Publication of the Modified Certificate by the CA 58
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 58
4.9 Certificate Revocation and Suspension 59
4.9.1 Circumstances for Revocation 59
4.9.2 Who Can Request Revocation 60
4.9.3 Procedure for Revocation Request 61
4.9.4 Revocation Request Grace Period 61
4.9.5 Time Within Which CA Must Process the Revocation Request 61
4.9.6 Revocation Checking Requirements for Relying Parties 62
4.9.7 CRL Issuance Frequency 62
4.9.8 Maximum Latency for CRLs 62
4.9.9 Online Revocation/Status Checking Availability 63
4.9.10 Online Revocation Checking Requirements 63
4.9.11 Other Forms of Revocation Advertisements Available 64
4.9.12 Special Requirements for Re-Key Compromise 64
4.9.13 Circumstances for Suspension 65
4.9.14 Who Can Request Suspension 65
4.9.15 Procedure for Suspension Request 65
4.9.16 Limits on Suspension Period 65
4.10 Certificate Status Services 65
4.10.1 Operational Characteristics 65
4.10.2 Service Availability 65
4.10.3 Optional Features 65
4.11 End of Subscription 65
4.12 Key Escrow and Recovery 66
4.12.1 Key Escrow and Recovery Policy and Practices 66
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 66
5.1 IdenTrust Physical Security Controls 67
5.1.1 Site Location and Construction 67
5.1.2 Physical Access 67
5.1.3 Power and Air Conditioning 67
5.1.4 Water Exposures 67
5.1.5 Fire Prevention and Protection 67
5.1.6 Media Storage 68
5.1.7 Waste Disposal 68
5.1.8 Off-Site Backup 69
5.2 Procedural Controls 69
5.2.1 Trusted Roles 69
5.2.2 Number of Persons Required per Task 73
5.2.3 Identification and Authentication for Each Role 73
5.2.4 Roles Requiring Separation of Duties 74
5.3 Personnel Controls 74
5.3.1 Qualifications, Experience, and Clearance Requirements 74
5.3.2 Background Check Procedures 75
5.3.3 Training Requirements and Procedures 76
5.3.4 Retraining Frequency and Requirements 76

5.3.5 Job Rotation Frequency and Sequence 77
5.3.6 Sanctions for Unauthorized Actions 77
5.3.7 Independent Contractor Requirements 77
5.3.8 Documentation Supplied to Personnel 77
5.4 Audit Logging Procedures 77
5.4.1 Types of Events Recorded 78
5.4.2 Frequency of Processing Log 80
5.4.3 Retention Period for Audit Log 80
5.4.4 Protection of Audit Log 81
5.4.5 Audit Log Backup Procedures 81
5.4.6 Audit Collection System (Internal vs. External) 81
5.4.7 Notification to Event-Causing Subject 82
5.4.8 Vulnerability Assessments 82
5.5 Records Archival 82
5.5.1 Types of Records Archived 82
5.5.2 Retention Period for Archive 83
5.5.3 Protection of Archive 84
5.5.4 Archive Backup Procedures 85
5.5.5 Requirements for Times-Stamping of Records 85
5.5.6 Archive Collection System (Internal or External) 85
5.5.7 Procedures to Obtain and Verify Archive Information 85
5.6 Key Changeover 85
5.7 Compromise and Disaster Recovery 85
5.7.1 Incident and Compromise Handling Procedures 85
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 86
5.7.3 Entity Private Key Compromise Procedures 87
5.7.4 Business Continuity Capabilities After a Disaster 87
5.8 CA or RA Termination 87
6 TECHNICAL SECURITY CONTROLS 87
6.1 Key Pair Generation and Installation 88
6.1.1 Key Pair Generation 88
6.1.2 Private Key Delivery to Subscriber 90
6.1.3 Public Key Delivery to Certificate Issuer 90
6.1.4 CA Public Key Delivery to Relying Parties 91
6.1.5 Key Sizes 91
6.1.6 Public Key Parameters Generation and Quality Checking 92
6.1.7 Key Usage Purposes (as per X509 v3 *keyUsage* Field) 92
6.2 Private Key Protection and Cryptographic Module Engineering Controls 92
6.2.1 Cryptographic Module Standards and Controls 92
6.2.2 Private Key (N out of M) Multi-Person Control 93
6.2.3 Private Key Escrow 93
6.2.4 Private Key Backup 93
6.2.5 Private Key Archival 94
6.2.6 Private Key Transfer Into or From a Cryptographic Module 94
6.2.7 Private Key Storage on Cryptographic Module 94
6.2.8 Method of Activating Private Key 94
6.2.9 Method of Deactivating Private Key 94
6.2.10 Method of Destroying Private Key 95

6.2.11 Cryptographic Module Rating 95
6.3 Other Aspects of Key PAIR Management 95
6.3.1 Public Key Archival 95
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 95
6.4 Activation Data 96
6.4.1 Activation Data Generation and Installation 96
6.4.2 Activation Data Protection 96
6.4.3 Other Aspects of Activation Data 96
6.5 Computer Security Controls 96
6.5.1 Specific Computer Security Technical Requirements 96
6.5.2 Computer Security Rating 97
6.6 Life Cycle Technical Controls 97
6.6.1 System Development Controls 97
6.6.2 Security Management Controls 97
6.6.3 Life Cycle Security Controls 97
6.7 Network Security Controls 97
6.8 Time-stamping 98
7 CERTIFICATE, CRL, AND OCSP PROFILES 99
7.1 Certificate Profile 99
7.1.1 Version Number(s) 99
7.1.2 Certificate Content and Extensions 99
7.1.3 Algorithm Object Identifiers 103
7.1.4 Name Forms 104
7.1.5 Name Constraints 104
7.1.6 Certificate Policy Object Identifier 104
7.1.7 Usage of Policy Constraints Extension 105
7.1.8 Policy Qualifiers Syntax and Semantics 105
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 105
7.2 CRL Profile 105
7.2.1 Version Number(s) 105
7.2.2 CRL and CRL Entry Extensions 105
7.3 OCSP Profile 106
7.3.1 Version Number(s) 106
7.3.2 OCSP Extensions 106
8 **COMPLIANCE AUDIT AND OTHER ASSESSMENTS** 106
8.1 Frequency or Circumstances of Assessment 107
8.2 Identity/Qualifications of Assessor 107
8.3 Assessor's Relationship to Assessed Entity 109
8.4 Topics Covered by Assessment 109
8.4.1 CA Assessment 109
8.5 Actions Taken as a Result of Deficiency 110
8.6 Communication of Results 110
8.7 Self-Audits 110
9 OTHER BUSINESS AND LEGAL MATTERS 110
9.1 Fees 111
9.1.1 Certificate Issuance or Renewal Fees 111
9.1.2 Certificate Access Fees 111
9.1.3 Revocation or Status Information Access Fees 111

9.1.4 Fees for Other Services 111
9.1.5 Refund Policy 111
9.2 Financial Responsibility 111
9.2.1 Insurance Coverage 111
9.2.2 Other Assets 111
9.2.3 Insurance or Warranty Coverage for End-Entities 112
9.3 Confidentiality of Business Information 112
9.3.1 Scope of Confidential Information 112
9.3.2 Information Not Within the Scope of Confidential Information 112
9.3.3 Responsibility to Protect Confidential Information 112
9.4 Privacy of Personal Information 112
9.4.1 Privacy Plan 112
9.4.2 Information Treated As Private 113
9.4.3 Information Not Deemed Private 113
9.4.4 Responsibility to Protect Private Information 113
9.4.5 Notice and Consent to Use Private Information 113
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 114
9.4.7 Other Information Disclosure Circumstances 114
9.5 Intellectual Property Rights 114
9.6 Representations and Warranties 114
9.6.1 CA Representations and Warranties 114
9.6.2 RA Representations and Warranties 116
9.6.3 Subscriber Representations and Warranties 116
9.6.4 Relying Party Representations and Warranties 117
9.6.5 Representations and Warranties of Other Participants 118
9.7 Disclaimer of Warranties 118
9.8 Limitations of Liability 119
9.9 Indemnities 119
9.10 Term and Termination 120
9.10.1 Term 120
9.10.2 Termination 120
9.10.3 Effect of Termination and Survival 120
9.11 Individual Notices and Communications with Participants 121
9.11.1 Notices by Individual Participants to IdenTrust 121
9.11.2 Notices by IdenTrust to Individual Participants 121
9.11.3 Notices Delivery Method 121
9.12 Amendments 121
9.12.1 Procedure for Amendment 122
9.12.2 Notification Mechanism and Period 122
9.12.3 Circumstances under Which OID Must Be Changed 122
9.13 Dispute Resolution Provisions 122
9.13.1 Specific Provisions/ Incorporation of Policy 122
9.14 Governing Law 122
9.15 Compliance with Applicable Law 123
9.16 Miscellaneous Provisions 123
9.16.1 Entire Agreement 123
9.16.2 Assignment 123
9.16.3 Severability 123

9.16.4 Enforcement (Attorney Fees and Waiver of Rights) 124
9.16.5 Force Majeure 124
9.17 Other Provisions 124

1 INTRODUCTION

1.1 Overview

This TrustID TLS Certificate Policy and Certification Practice Statement, referred to throughout this document as "CP-CPS", defines the policies and practices employed by IdenTrust Services, LLC (IdenTrust) as a Certification Authority (CA) and acting as LRA, and by Registration Authorities (RAs), to fulfill the requirements of IdenTrust TLS Publicly-Trusted Certificates. This CP-CPS governs the issuance of IdenTrust TLS Certificates in accordance with the Certificate Profiles outlined in Section 7 and in compliance with the latest guidelines established by:

- The CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates
- The CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates
- The CA/Browser Forum Network and Certificate System Security Requirements
- The Apple Root Certificate Program
- The Chrome Root Program Policy
- The Microsoft Trusted Root Program
- The Mozilla Root Store Policy
- The CCADB Policy

The copy of this CP-CPS attached hereto (the "Policy Copy") is provided to the Mozilla Foundation subject to the terms of that certain license known as "Creative Commons Attribution-NoDerivatives 4.0 International Public License" (which can be viewed at: https://creativecommons.org/licenses/by-nd/4.0/) and the notices below on this page (collectively, the "License"). The Policy Copy forms the "Licensed Materials" under the License provided that this page is not removed from the Policy Copy.

NOTICES:

A. IdenTrust Services, LLC is the creator of the Policy Copy; provided, however, any documents or other works referenced in the Policy Copy (e.g. "IETF PKIX Certificate Management Protocol", "Repository" materials, or documents referenced in the Policy Copy), (collectively, "References") are understood to be so referenced for contractual purposes insofar as the original of which the Policy Copy is a copy serves as part of a System of contracts applicable to Certificates issued within the Public Key Infrastructure described within the Policy Copy. It is understood that References are not works included in the Policy Copy for purposes of the License.

B. With respect to the Policy Copy as provided by IdenTrust Services, LLC under the License, the following notice is provided:

Copyright © 2026 IdenTrust Services, LLC. All rights reserved.

C. PKI Participants (see Section 1.3) must not, as PKI Participants, rely or otherwise use the Policy Copy. The Policy Copy may not be accurate or current. At any point in time, for the then-current authoritative version of the "TrustID TLS CP-CPS", PKI Participants can visit the IdenTrust Repository located at: https://www.identrust.com/support/documents/trustid. Access to and the contents of such Repository are not within the scope of the License.

D. This page must be included with every copy of the Policy.

1.2 Document Name and Identification

1.2.1 Alphanumeric Identifier

The name of this CP-CPS which follows the RFC 3647 framework, is the "TrustID TLS Certificate Policy / Certificate Practice Statement", approved for publication on November 15, 2026 by the IdenTrust PMA.

The following table contains subsequent revisions: (Prior versions of IdenTrust CP, CPS and combined CP-CPS documents can be found in the "Policies – Archived" Section of the IdenTrust TrustID Document Library).

CP-CPS Document Versions

Version	Date	Summary of Changes / Comments
5.0.0	October 30, 2025	This document replaces IdenTrust CP v4.9.2 and IdenTrust CPS v4.9.2 with the following updates: (1) Removed all Non-TLS Certificate references, (2) Added relevant CP language where applicable, (3) Section 1.2.2: Moved OID details to Section 7.1.6, (4) Section 1.6: Added/updated definitions/Acronyms/References, (5) Section 3.2.2.4: Removed Domain validation methods not used, (6) Section 3.2.2.9: Added Multi-Perspective details, (7) Section 4.2.1.1: Added details for CAA checking, (8) Section 4.10.2.1: "Problem Report" moved to Section 1.5.2.1, (9) Section 5.2.1: Updated language for Trusted Roles, (10) Section 5.2.4: Removed detailed separation of duties, (11) Section 5.4.1: Removed detailed audit log entries table, (12) Section 6.3.2: Updated Key Usage period table, (12) Section 7: Removed non-TLS Certificate Profile details, (13) Removed Appendix A
5.0.1	November 12, 2025	(1) Sections 1.5.2, 1.6.1, 1.6.2, 3.2.2, 2.4.1.1, 4.3.2, 4.4.2, 4.9.2, 4.9.3, 4.9.12, 6.1.3: Add ACME language, (2) Section 6.6.1: System development controls, (3) Section 5.7.2: Add mass revocation language, Sections: 1.6, 6.7.1, 6.7.2, 6.7.3: NetSec v2.0.5 (NS-008), (4) Sections 4.9.13, 4.9.14, 4.9.15, and 4.9.16: Certificate suspension

Version	Date	Summary of Changes / Comments
5.0.2	January 13, 2026	(1) Section 6.3.2 : Add cross-signed subordinate CA, (2) Section 7.1.2.2: Add cross-signed Subordinate CA Certificate profile, (3) Section 7.1.2.3: Update foot note [9] to reflect '*clientAuth*' as optional, (4) Update internal links throughout the document
5.0.3	March 9, 2026	(1) Section 1.6.1: Removed table format and added definitions, (2) Section 1.6.2: Removed table format, (3) Section 3.2.2.4: Updated language, (4) Section 3.2.2.4.2: Updated language, (5) Section 3.2.2.5.4: Added DNS TXT Record with Persistent Value, (6) Section 4.2.2: updated language, (7) Section 7: Removed table formats, (8) Section 7.1.6: Update for OIDs effective date, (9) Section 7.1.2.3: Updated language, (10) Section 9.12.2 and 9.16.3: Updated legal language, (11) Removed references to explicit sections in external non-IdenTrust documents, adding relevant text.
5.0.4	June 16, 2026	Section 7.1.2.3 and 7.1.6: Removed IdenTrust OID removal date
5.1	September 10, 2026	(1) Overall clean-up of list formatting, (2) Section 1.1 and 1.6.3: Link updates, (3) Section 1.6.1 and Section 7.1.2.3: SC-87v2 updates, (4) Section 3.2.2: Updated methods used and section alignment, (5) Section 5.1: Updated language, (6) Section 5.4.8: Language reworded and moved, (7) Section 6.6.1: Updated language, (8) Section 6.7: Updated language
5.1.1	October 27, 2026	Section 7.1.2.2.1 correct footnote
5.1.2	October 29, 2026	Section 7.1.2.3 address jurisdictionLocalityName field
5.1.3	November 15, 2026	Section 7.1.2.3 address policyQualifier field

1.2.2 Object Identifier

IdenTrust is the owner of a numeric identifier–Object Identifier (OID)—assigned by the American National Standards Institute (ANSI) under {joint-iso-ccitt (2) country (16) USA (840) US-company (1) IdenTrust (113839) CP (0) TrustID-v2(6)}, which IdenTrust uses as a base arc to identify CPs, CPSs, and other documents, schemas, algorithms, etc. The OID arc for IdenTrust's implementation of the CP-CPS and associated Policy documents is 2.16.840.1.113839.

Section 7.1.6 lists individual TLS Certificate OIDs recognized for use within the PKI established by this CP-CPS.

Root and ICAs governed by this CP-CPS are disclosed in the "IdenTrust TrustID Certificate

Hierarchy" table of the "IdenTrust Downloads and Drivers" webpage.

1.3 PKI Participants

This CP-CPS describes an open-but-bounded Public Key Infrastructure. It describes the rights and obligations of all Participants – i.e., all persons and entities authorized under the CP-CPS to fulfill any of the following roles: PMA, CA, RA, CMA, Repository, Subscriber, and Authorized Relying Party.

1.3.1 Certification Authorities

IdenTrust as the Issuing CA is a trusted third party that attests to the binding between an identity and cryptographic Key Pair. CA functions primarily consist of the following:

- Key management functions, such as Key Generation of CA Key Pairs, the secure management of CA Private Keys and the distribution of CA Public Keys;
- Secure delivery of the CA Private Keys to Subscribers specifically ensuring Private Keys are maintained in Cryptographic Modules that are FIPS evaluated, and software based Private Keys will be created and maintained by the Subscriber;
- Establishing an environment and procedure for Applicants and PKI Sponsors for Certificates to submit their Certificate applications (e.g., creating a web-based enrollment page);
- The Identity Proofing of Individuals or entities applying for a Certificate;
- The approval or rejection of Certificate applications;
- The signing and Issuance of Certificates in response to approved Certificate applications;
- The publication of Certificates in a Repository, where Certificates are made available for potential Relying Parties;
- The initiation of Certificate Revocations, either at the Subscriber's request or upon the entity's initiative;
- The Revocation of Certificates, including by such means as issuing and publishing Certificate Revocation Lists (CRLs) or providing Revocation information via Online Certificate Status Protocol (OCSP) when required, or other online methods; and
- The Identity Proofing of Individuals or entities submitting requests to renew Certificates or seeking a new Certificate following a re-keying process, and processes set forth above for Certificates issued in response to approved renewal or re-keying requests.

IdenTrust as the Issuing CA is bound to act according to the terms of this CP-CPS.

1.3.2 Registration Authorities

IdenTrust as the Issuing CA is ultimately responsible for all TrustID Certificates it issues; however, under this CP-CPS, with the exception of Section 3.2.2.4, Section 3.2.2.5, and Section 3.2.6.3, IdenTrust may subcontract registration and Identity Proofing functions to an Organization that agrees to:

1. Meet the qualification requirements of Section 5.3.1, when applicable to the delegated function;
2. Retain documentation in accordance with Section 5.5.2;
3. Abide by the other provisions of the TLS BR that are applicable to the delegated function; and;
4. Comply with this CP-CPS or the Delegated Third Party's Registration Practice Statement that IdenTrust has verified, and complies with the TLS BR. IdenTrust may require an RA Organization to submit a Registration Practice Statement on an annual basis.

An RA is an entity that is responsible for collecting and confirming a Subscriber's identity and other information for inclusion in the Certificate. RA functions are those CA functions that are generally related to the performance of Identity Proofing. These duties can be performed for the entity by Local Registration Agent (LRAs) that are authorized by RAs to perform the duties including the following:

- Establishing an environment and procedure for Certificate Applicants and PKI Sponsors to submit their Certificate applications (e.g., creating a web-based enrollment page);
- The Identity Proofing of Individuals or Affiliated entities who apply for a Certificate;
- The approval or rejection of Certificate applications;
- The initiation of Certificate Revocations, either at the Subscriber's request or upon the Affiliated entity's initiative;
- The Identity Proofing of Individuals or entities submitting requests to renew Certificates or seeking a new Certificate following a re-keying process and processes set forth above for Certificates issued in response to approved renewal or re-keying requests;
- Authenticating the Subject's identity;
- Verifying the attributes requested by the Subject for their Certificate;
- Assigning distinguished (unique) names to Subjects; and
- Distributing tokens and associated software to Subscribers.

1.3.2.1 Enterprise Registration Authorities

IdenTrust may delegate to an Enterprise RA to verify Certificate Requests from Subjects within the Enterprise RA's own Organization. IdenTrust does not Accept Certificate Requests authorized by an Enterprise RA unless the following requirements are satisfied:

1. IdenTrust may delegate to an Enterprise RA to verify Certificate Requests from Subjects within the Enterprise RA's own Organization. IdenTrust shall not Accept Certificate Requests authorized by an Enterprise RA unless the following requirements are satisfied: IdenTrust shall confirm that the requested FQDNs are within the Enterprise RA's verified Domain Namespace. If the Certificate Request includes a Subject name of a type other than a FQDN, IdenTrust shall confirm that the name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject. For example, the CA shall not issue a Certificate containing the Subject name "XYZ Co." on the authority of Enterprise RA "ABC Co.", unless the two companies are affiliated (see Section 3.2.2) or "ABC Co." is the agent of "XYZ Co". This requirement applies regardless of whether the accompanying requested Subject FQDN falls within the Domain Namespace of ABC Co.'s Registered Domain Name.
2. IdenTrust confirms that the subject:organizationName name is either that of the delegated Enterprise RA, or an Affiliate of the delegated Enterprise RA, or that the delegated Enterprise RA is an agent of the named Subject.
3. For EV Certificates, the final cross-correlation and due diligence requirements may be performed by a single person representing the Enterprise RA as follows:

- After completing all verification steps, IdenTrust uses an independent reviewer (not involved in data collection) to examine all documentation for discrepancies or issues.
- Any discrepancies must be clarified or resolved by obtaining additional information from the applicant or trusted sources.
- IdenTrust does not issue the Certificate until all information is accurate and consistent. If clarification is not provided within a reasonable time, the request must is declined, and the

applicant is notified.
- Before issuing the certificate, IdenTrust reviews and confirms that all requirements have been met.

IdenTrust imposes these limitations as a contractual requirement on the Enterprise RA and monitor compliance by the Enterprise RA.

1.3.3 Subscribers

A Subscriber is an entity to whom or to which a Digital Certificate is issued and who is legally bound by a Subscriber Agreement. Subscribers use TrustID Certificates to encrypt and authenticate communication with web browsers.

TrustID Certificates may be issued in conjunction with an Organization that has a relationship with the Subscriber; this is termed affiliation. The organizational affiliation will be indicated in the Certificate. IdenTrust contacts the Affiliated Organization's associate with a Certificate application to verify the affiliation at the time of Certificate application and requesting Revocation of the Certificate if the affiliation is no longer valid.

1.3.4 Relying Parties

This CP-CPS is intended for the benefit of an Authorized Relying Party who is an Individual or Sponsoring Organization that has entered into the Authorized Relying Party Agreement and uses the Subscriber's Certificate to verify the integrity of a Digitally Signed message, to identify the creator of a message, to authenticate such Subscriber, or to establish confidential communications with the Subscriber. This is different than a Relying Party that does not enter into the Authorized Relying Party Agreement but still relies upon the Certificate for the verification and authentication purposes listed above.

Relying parties may check the relevant CRL or OCSP response when available, before relying on the information presented in the Certificate.

1.3.5 Other Participants

1.3.5.1 Policy Management Authority (PMA)

The IdenTrust Policy Management Authority (PMA) oversees the adoption, administration, and application of the CP-CPS with all the PKI Participants. The IdenTrust PMA also has charge of the future development and amendment of this CP-CPS.

1.3.5.2 Certificate Manufacturing Authority (CMA)

IdenTrust as the Issuing CA will remain ultimately responsible for the manufacture of TrustID Certificates. However, IdenTrust may subcontract manufacturing functions to third party CMAs who agree to be bound by this CP-CPS.

1.3.5.3 Repositories

IdenTrust as the Issuing CA will perform the role and functions of the Repository. IdenTrust may subcontract the performance of the Repository functions to a third party Organization that agrees to fulfill the functions of a Repository, and who agrees to be bound by this CP-CPS, but IdenTrust remains responsible for the performance of those services in accordance with this CP-CPS.

1.3.5.4 PKI Sponsors

A PKI Sponsor is an Individual who applies for a Certificate used by an Electronic Device but is not the Subscriber. This Individual is employed by or is an authorized agent of the Sponsoring Organization and acts on behalf of the Sponsoring Organization in relation to the Certificate, including but not limited to applying for such Certificate, completing the application and registration processes, retrieving such Certificate when it is issued, and other Certificate lifecycle events. When so, the PKI Sponsor is responsible for providing the information necessary (i.e., server or application name, Public Keys, equipment authorization or attributes, contact information, and other information) to complete the application and registration processes. The PKI Sponsor will also:

- Sign and submit, or approve a Certificate Request on behalf of the Sponsoring Organization, and/or
- Sign and submit a Subscriber Agreement on behalf of the Sponsoring Organization, and/or
- Acknowledge and agree to the Certificate Terms of Use on behalf of the Sponsoring Organization.

1.3.5.5 Trusted Agents

No stipulation.

1.3.5.6 Delegated Third Parties

IdenTrust does not delegate CA activities to Delegated Third Parties which are not Enterprise RAs.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Applications for which TrustID Certificates are suitable include, but are not limited to, applications that Provide authentication-based access and secure server communication with online sources of information:

- Domain Validation (DV): Verifies that the Subscriber has control over the domain but does not authenticate the Organization behind the website.
- Organization Validation (OV): Verifies that the Certificate Subscriber has control over the domain and authenticate the Organization behind the website.
- Extended Organization Validation (EV): Verifies that the Subscriber has control over the domain and does a comprehensive authentication of the Organization behind the website to meet strict industry standards set by the CA/Browser Forum Baseline Requirements.

Allowed uses are specified in the Key Usage and Extended Key Usage extensions of a Certificate and are documented in the Certificate Profiles Section 7. This section presents the uses for different Certificate types as identified by the Certificate Policy OID.

1.4.2 Prohibited Certificate Uses

Certificates issued under the provisions of this CP-CPS may not be used for:

- Any use not provided for as an allowed use in Section 1.4.1;
- Any application requiring fail-safe performance such as:
- the operation of nuclear power facilities
- air traffic control systems
- aircraft navigation systems

- weapons control systems or
- any other System whose failure could lead to injury, death, or environmental damage; or
- Any transaction where applicable law prohibits the use of Certificates for such transaction or where otherwise prohibited by law.

IdenTrust will not issue Certificates for use in any software or hardware architectures that provide facilities for interference with encrypted communications, including but not limited to:

- Active eavesdropping (e.g., MitM;) or
- Traffic management of Domain Names or IP Addresses that the Organization does not own or control.

The restriction in the preceding sentence shall apply regardless of whether a Relying Party communicating through the software or hardware architecture has knowledge of it providing facilities for interference with encrypted communications.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP-CPS is administered by the IdenTrust PMA

1.5.2 Contact Person

Questions regarding the implementation and administration of this CP-CPS should be directed to:

IdenTrust PMA
IdenTrust Services, LLC.
5225 Wiley Post Way, Suite 450
Salt Lake City, UT 84116
Email: Policy@IdenTrust.com
Phone: (888) 882-1104

1.5.3 Certificate Problem Reporting

IdenTrust provides the following contact options for Subscribers, Relying Parties, Application Software Suppliers, and other third parties to report suspected Private Key compromise, Certificate misuse, fraud, or any other issue related to TrustID Certificates:

- **Website:** https://www.identrust.com/report-certificate-security-compromise-issues
- **Email Support:** support@identrust.com
- **Phone Support:** Available during regular business hours. Urgent issues—such as Key compromises—reported outside of these hours are routed to an after-hours call service, which will escalate and address the issue based on its severity.

1.5.4 Person Determining CP-CPS Suitability for the Policy

The PMA determines the suitability of this CP-CPS based on a compliance analysis performed by the PMA itself or a party independent from the CA and is not the CP-CPS author.

1.5.5 CP-CPS Approval Procedures

The approval and management of this IdenTrust CA's CP-CPS follow procedures defined by the PMA.

If a Policy change is significant, the PMA may assign a new Object Identifier (OID). Full procedural details are outlined in Section 9.12.

1.6 Definitions and Acronyms

1.6.1 Definitions

ACME Protocol: A protocol used for validation, issuance, and management of certificates. The protocol is an open standard managed by the IETF.

Accept or Acceptance: An End Entity's act that triggers the End Entity's rights and obligations with respect to its TrustID Certificate under the applicable Subscriber Agreement or Authorized Relying Party Agreement. Indications of Acceptance may include without limitation: Using the TrustID Certificate (after Issuance); Failing to notify IdenTrust of any problems with the TrustID Certificate within a reasonable time after receiving it; Other manifestations of assent.

Account Password: Private data, which may consist of Activation Data, used by the Applicant/PKI Sponsor for authentication and delivered to the CA securely via a Client-Authenticated SSL/TLS encrypted session, and subsequently used for purposes of authentication by the Applicant/PKI Sponsor when performing Certificate management tasks (e.g., delivering Applicant/PKI Sponsor's *PKCS#10* to the CA or retrieving the Certificate) via a Client-Authenticated SSL/TLS Encrypted Session.

Activation Code: A code generated by RAs or IdenTrust for a successful Applicant/PKI Sponsor to use to initiate the Certificate retrieval process through a secure session online.

Activation Data: Private data used or required to access or activate Cryptographic Modules (e.g., a personal identification number (PIN), pass phrase, or a manually-held Key share used to unlock a Private Key before creating a Digital Signature).

Air-Gapped: Physically and logically separated, disconnected, and isolated from all other Systems.

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.

Affiliated Individual: An Individual having an affiliation with an Organization who has been authorized by the Organization to obtain a TrustID Certificate that identifies the Organization and the fact of the Individual's affiliation with the Organization (see Sponsoring Organization).

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

Applicant Representative: A Natural Person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: who signs and submits, or approves a Certificate Request on behalf of the Applicant; who signs and submits a Subscriber Agreement on behalf of the Applicant; and/or who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

Application Software Supplier: A supplier of email client software or other relying-party application software such as mail user agents (web-based or application based) and email service

providers that process S/MIME Certificates.

Assumed Name: Also known as “doing business as”, “DBA,” or “d/b/a” name in the US and “trading as” name in the UK.

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

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is different from the period of time when the auditors are on-site at the CA). The coverage rules and maximum length of Audit Periods are defined in Section 8.1.

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 the Section 8.2.

Authorization Domain Name: The Domain Name used to obtain authorization for Certificate Issuance for a given FQDN. IdenTrust may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA must remove all wildcard labels from the leftmost portion of the requested FQDN. IdenTrust may prune zero or more labels from left to right until encountering a Base Domain Name and may use any 1 of the intermediate values for the purpose of domain validation.

Authorized Port: One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).

Authorized Relying Party: An Individual or Organization that has entered into an Authorized Relying Party Agreement.

Authorized Relying Party Agreement: A contract between an Individual or an Organization and IdenTrust that allows the party to rely on TrustID Certificates in accordance with the CP-CPS.

Authorizing Official (or AO): An Individual, who is an official, approved by and listed within IdenTrust’s databases as affiliated with a specific Organization. The AO is able to sign the authorizing form for other Individuals or PKI Sponsors for the approval of a RA Administrative Certificate for use within that Organization. This role is exclusive only to the RA Administrative Certificate process.

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

Business Entity: Any entity that is not a Private Organization, Government Entity, or Non-Commercial Entity as defined herein. Examples include, but are not limited to, general partnerships, unincorporated associations, sole proprietorships, etc.

CA Certificate: A Certificate that is at the beginning of a certification chain within the TrustID PKI hierarchy. A CA Certificate is established as part of the set-up and activation of the Issuing CA. The CA Certificate contains the Public Key that corresponds to the CA Private Signing Key that the Issuing CA uses to create or manage TrustID Certificates. CA Certificates and their corresponding Public Key may be embedded in software or obtained or downloaded by the affirmative act of an Authorized Relying Party to establish a certification chain.

CA Infrastructure: Collectively the infrastructure used by the CA or Delegated Third Party which qualifies as a: Certificate System; Root CA System (Air-Gapped and otherwise); or Security Support System.

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

CA Private Signing Key: The Private Key that corresponds to IdenTrust's Public Key listed in its CA Certificate and used to sign TrustID Certificates.

CAA: From RFC 8659: "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS Domain Name holder to specify one or more Certification Authorities (CAs) authorized to Issue Certificates for that Domain Name. CAA Resource Records allow a public a public CA to implement additional controls to reduce the risk of unintended Certificate mis-issue".

Certificate: A computer-based record or electronic message that:

- Identifies the Certification Authority issuing it;
- Names or identifies a Subscriber, Authorized Relying Party, or Electronic Device;
- Contains the Public Key of the Subscriber, Authorized Relying Party, or Electronic Device;
- Identifies the Certificate's Validity Period;
- Is Digitally Signed by a Certification Authority; and
- Has the meaning ascribed to it in accordance with applicable standards.

A Certificate includes not only its actual content but also all documents expressly referenced or incorporated in it.

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

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

Certificate Approver: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to:

1. act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and
2. to approve EV Certificate requests submitted by other Certificate Requesters.

Certificate Requester: A natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits a Certificate request on behalf of the Applicant.

Certificate Manufacturing Authority (or CMA): An Organization that manufactures or creates TrustID Certificates for IdenTrust.

Certificate Policy (or CP): A named set of rules that indicates the applicability of Certificates to particular communities and classes of applications and specifies the Identification and authentication processes performed before Certificate Issuance, the Certificate Profile, and other allowed uses of Certificates.

Certificate Problem Report: Complaint of suspected Private Key compromise, Certificate misuse,

or other types of fraud, compromise, misuse, or inappropriate conduct related to IdenTrust issued Certificates.

Certificate Profile(s): The protocol used in Section 7 of this CP-CPS, and the TrustID Certificate Profile to establish the allowed format and contents of data fields within TrustID Certificates, which identify IdenTrust as the Issuing CA, the End Entity, the Certificate's Validity Period, and other information that identifies the End Entity.

Certificate Request: A request to issue a Certificate, submitted to the CA by an authorized Individual.

Certificate Revocation List (or CRL): A regularly updated time-stamped list of revoked Certificates that is created and Digitally Signed by the CA that issued the Certificates.

Certificate Subject: See Individual-Validated.

Certificate System: A System used by a CA or Delegated Third Party to access, process, or manage data or provide services related to:

1. identity validation;
2. identity authentication;
3. account registration;
4. Certificate application;
5. Certificate approval;
6. Certificate Issuance;
7. Certificate Revocation;
8. authoritative Certificate status; or
9. Key escrow.

Certificate Transparency (or CT): Open standard (see RFC 6962) and open-source framework for monitoring and auditing digital Certificates. Through a System of Certificate logs, monitors, and auditors, Certificate Transparency allows website users and domain owners to identify mistakenly or maliciously issued Certificates and to identify Certificate authorities (CAs) that have gone rogue.

Certification Authority (or CA): An Organization that is responsible for the creation, Issuance, Revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs. See also Issuing CA.

Certification Authority Authorization (or CAA): From RFC 9495: "The Certification Authority Authorization (CAA) DNS resource record (RR) provides a mechanism for domains to express the allowed set of Certification Authorities that are authorized to Issue Certificates for the Domain".

Certification Practice Statement (or CPS): A statement of the practices that a CA employs in creating, issuing, managing, and revoking Certificates.

Client-Authenticated SSL/TLS-Encrypted Session: A Client-Authenticated SSL/TLS-Encrypted Session is a session securely communicated through the use of the Secure Sockets Layer and Transport Layer cryptographic protocols. For Client-Authenticated SSL/TLS-Encrypted Sessions discussed in this CP-CPS, both the Client and the server authenticate to each other using a Certificate. Upon mutual validation of identity, the resulting session is encrypted using Public Key Cryptography.

Contract Signer: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on

behalf of the Applicant to sign Subscriber Agreements.

Critical Security Event: An event, set of circumstances, or anomalous activity that could lead to:

1. a circumvention of CA Infrastructure security controls; or
2. a compromise of CA Infrastructure integrity or operational continuity.

These include, but are not limited to:

1. excessive login attempts;
2. attempts to access prohibited resources;
3. denial of service DoS/DDoS and distributed denial of service attacks;
4. attacker reconnaissance;
5. excessive traffic at unusual hours;
6. signs of unauthorized access;
7. system intrusion; or
8. physical compromise of component integrity.

Critical Vulnerability: A System vulnerability that has a CVSS v2.0 score of 7.0 or higher according to the NVD or an equivalent to such CVSS rating (see https://nvd.nist.gov/vuln-metrics/cvss), or as otherwise designated as a Critical Vulnerability by the CA or the CA/Browser Forum Baseline Requirements.

Cross-Certified Subordinate CA Certificate: A Certificate used to establish a trust relationship between 2 Root CAs.

Cryptographic Module: The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [NIST FIPS 140-3].

CSPRNG: Cryptographically Secure Pseudo-Random Number Generator: a Pseudo-Random Number generator intended for use in a cryptographic System.

Date of Formation: The date on which a Legal Entity is first recognized by the jurisdiction in which it was created or formed.

Delegated Third Party: A Natural Person or Legal Entity that is not the CA and that operates any part of a Certificate Issuing System.

Digital Signature / Digitally Sign: The transformation of an electronic record by one person using a Private Key and Public Key Cryptography so that another person having the transformed record and the corresponding Public Key can accurately determine: Whether the transformation was created using the Private Key that corresponds to the Public Key; and Whether the record has been altered since the transformation was made.

Distinguished Name (or DN): The unique identifier for a Subscriber so that he, she, or it can be located in a directory (e.g., the DN for a Subscriber might contain the following attributes: common name, Email Address (mail), Organization name (o), Organizational unit (ou), locality (l), state (st) and country (c)).

Domain Contact: The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

Domain Label: From RFC 8499: "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".

Domain Name: The label assigned to a node in the Domain Name system (see Fully Qualified Domain Name).

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:

- The Internet Corporation for Assigned Names and Numbers (ICANN);
- A national Domain Name authority/registry; or
- A Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).

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

Electronic Device: Computer software, hardware or other electronic or automated means (including email) configured and enabled by a person to act as their agent and to initiate or respond to electronic records or performances, in whole or in part, without review or intervention by such person.

Email Address(es): From RFC 5321: "A character string that identifies a user to whom mail will be sent or a location into which mail will be deposited".

End Entity(ies): Subscribers and Authorized Relying Parties.

Enterprise RA: An employee or agent of a Sponsoring Organization unaffiliated with the Issuing CA, who authorizes Issuance of Certificates to that Organization. Enterprise RAs sign an agreement with IdenTrust, which set forth their obligations, which include selective equivalent obligations to an LRA.

Extended Validation Server Certificate (or EV Certificate): The type Server Certificate that provides the highest level of authentication for websites.

Fully Qualified Domain Name (or FQDN): A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name system.

Government Agency: In the context of a Private Organization, the Government Agency in the Jurisdiction of Incorporation under whose authority the legal existence of Private Organizations is established (e.g., the government agency that issued the Certificate of Incorporation). In the context of Business Entities, the Government Agency in the jurisdiction of operation registering business entities. In the case of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

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.).

Incorporating Agency: In the context of a Private Organization, the Government Agency in the

Jurisdiction of Incorporation under whose authority the legal existence of the entity is registered (e.g., the government agency that issues certificates of formation or incorporation). In the context of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Individual(s): A Natural Person and not a juridical person or Legal Entity.

Internal Name(s): A string of characters (not an IP Address) in a common name or *subjectAltName* 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.

International Organization: An organization founded by a constituent document, e.g., a charter, treaty, convention or similar document, signed by, or on behalf of, a minimum of two Sovereign State governments.

Internet: The Internet is a global System of interconnected computer networks that uses multiple protocols to communicate data.

Internet Protocol (or IP): The primary protocol in the Internet Layer defined by the Request for Comment as defined in RFC 1122: Requirements for Internet Hosts -- Communication Layers, Internet Engineering Task Force, R. Braden, October 1989. The IP has the task of delivering datagrams from the source host to the destination host solely based on the addresses.

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

IP Address Registration Authority: The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

Issue Certificates / Issuance: The act performed by a CA in creating a Certificate, listing itself as "Issuer," and notifying the Applicant or PKI Sponsor of its contents and that the Certificate is ready and available for Acceptance.

Issuing Certification Authority (or Issuing CA): An entity authorized by the PMA to issue and sign Certificates in accordance with the CP-CPS. In both documents, the term "CA," and/or "Issuing CA," means Issuance of IdenTrust CA TrustID Certificates.

Jurisdiction of Incorporation: The country and (where applicable) the state, province, or locality where the Organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.

Key: A general term used throughout this Policy to encompass any one of the defined Keys mentioned in these general definitions section.

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

Key Generation: The process of creating a Key Pair.

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

Key Pair: The Private Key and its associated Public Key.

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

Linting: A process in which the content of Digitally Signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-be-signed object such as a tbsCertificate (as described in Section 4.1.1.1 of RFC 5280) is checked for conformance with the profiles and requirements defined in Section 7.

Local Registration Agent (or LRA): An employee of an Issuing CA or Registration Authority (RA) who is responsible for confirming the correctness and accuracy of Applicant identity, either through direct contact or via review and approval of documents submitted by a licensed notary or Trusted Agent, executing the requests from Applicants in the System, and approving the Issuance of a Certificate based on that information.

Multi-Factor Authentication: An authentication mechanism consisting of two or more of the following independent categories of credentials (i.e., factors) to verify the user's identity for a login or other transaction:

1. something the user knows (knowledge factor);
2. something the user has (possession factor); and
3. something the user is (inherence factor).

Each factor is independent of the other(s).

Multi-Party Control: An access control mechanism which requires two or more separate, authorized users to successfully authenticate with their own unique credentials prior to access being granted.

Multi-Perspective Issuance Corroboration: A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate Issuance.

Natural Person: An Individual; a human being as distinguished from a Legal Entity.

Network Boundary Control: Components that manage and control network traffic flow to, from, and within CA Infrastructure.

Network Perspective: Related to Multi-Perspective Issuance Corroboration. A System (e.g., a cloud-hosted server instance) or collection of network components (e.g., a VPN and corresponding infrastructure) for sending outbound Internet traffic associated with a domain control validation method and/or CAA check. The location of a Network Perspective is determined by the point where unencapsulated outbound Internet traffic is typically first handed off to the network infrastructure providing Internet connectivity to that perspective.

Non-Commercial Entity: Means any entity, however organized, which furnishes goods or services to the general public in a not-for-profit manner.

Object Identifier (or OID): The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference 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.

Onion Domain Name: A FQDN ending with RFC 7686 ".onion" Special-Use Domain Name. For example, 2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion is an Onion

Domain Name, whereas torproject.org is not an Onion Domain Name.

Online Certificate Status Protocol (or OCSP): An online Certificate-checking protocol that enables Relying Party application software to determine the status of an identified Certificate (see also Online Status Check).

Online Status Check: An online, real-time status check of the validity of a TrustID Certificate. An Online Status Check involving a CRL consists of checking the most recently issued CRL (e.g., not involving a cached CRL).

Operational Period: A Certificate's actual term of validity, beginning with the start of the Validity Period and ending on the earlier of: The end of the Validity Period disclosed in the Certificate; or The Revocation of the Certificate.

Organization(s): An entity that is legally recognized in its jurisdiction of origin (e.g., a corporation, partnership, sole proprietorship, government department, non-government Organization, university, trust, special interest group, or non-profit corporation).

Organization Validated Server Certificate (or OV Certificate): Refers to a Server Certificate Subject that includes only organizational (Legal Entity) attributes, rather than attributes linked to an Individual.

Participants: All PKI Service Providers and End Entities authorized to participate in the PKI defined by this CP-CPS.

Persistent DCV TXT Record: A DNS TXT record identifying an Applicant in accordance with Section 3.2.2.5.4.

Physically Secure Environment: A controlled and protected physical space consisting minimally of a physical environment which is:

1. protected by security controls which address the topics outlined in Section 4.5.1 of RFC 3647; and
2. operated in accordance with Risk Assessments conducted by the CA.

PKI Service Providers: The PMA, IdenTrust, Ras, CMAs, and Repositories participating in the PKI defined by this CP-CPS.

PKI Sponsor: An Individual who is employed by the Sponsoring Organization or an authorized agent who has express authority to represent the Organization but is not the Subscriber. The Sponsoring Organization verifies the PKI Sponsor is an Individual that:

- Signs and submits, or approves a request for a Certificate issued to an Electronic Device on behalf of the Organization, and/or
- Signs and submits a Subscriber Agreement on behalf of the Organization, and/or
- Acknowledges and agrees to the Certificate Terms of Use on behalf of the Organization when the Organization is an Affiliate of the CA (see Section 1.3.5.4).

Place of Business: The location of any facility (such as a factory, retail store, warehouse, etc.) where the Applicant's business is conducted.

Policy: The governing document that dictates the parties involved and requirements for these practices is listed in this Certification Practicing Statement.

Policy Management Authority (PMA): The Organization responsible for setting, implementing, and administering Policy decisions regarding this CP-CPS.

Precertificate: A Precertificate is a signed data structure that can be submitted to a CT log, as defined by [RFC 6962](https://www.rfc-editor.org/rfc/rfc6962.html) and containing the critical poison extension (OID 1.3.6.1.4.1.11129.2.4.3).

Primary Network Perspective: The Network Perspective used by the CA to make the determination of

1. the CA's authority to issue a Certificate for the requested domain(s) or IP address(es) and
2. the Applicant's authority and/or domain authorization or control of the requested domain(s) or IP address(es).

Private Key: The cryptographic Key of an asymmetric Key Pair that is kept secret by the holder of the Key Pair. It may be used to create Digital Signatures and/or to decrypt data that were encrypted by the corresponding Public Key.

Private Organization: Private Organizations are non-governmental entities that operate independently from the state and are not funded by public funds. They can include a variety of Organizations, such as private voluntary Organizations, private corporations (for-profit or nonprofit), and private research institutes.

Privileged Access: Access to CA Infrastructure or Network Boundary Controls that provides capabilities or permissions enabling administration, configuration, management, or operation of such systems.

Public Key: The cryptographic Key of an asymmetric Key Pair that can be made public without compromising the security of the Key Pair. It may be used to verify Digital Signatures and/or to encrypt data that can be decrypted by the corresponding Private Key.

Public Key Cryptography: A type of cryptography also known as asymmetric cryptography that uses a Key Pair to securely encrypt and decrypt messages.

Public Key Infrastructure (or PKI): The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based Public Key Cryptography System.

Public Suffix: The right-most concatenated portion of a Domain Name which appears in a database of information used by the CA as part of the verification process specified in Section 3.2.2.4.

Publicly-Trusted Certificate: An IdenTrust TrustID Certificate that is trusted by virtue of the fact that its corresponding Root CA 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.

Random Value: A value specified by a CA to the Domain Registrant that exhibits at least 112 bits of entropy.

Reasonable Reliance: For purposes of this CP-CPS, an Authorized Relying Party's decision to rely on a TrustID Certificate will be considered Reasonable Reliance if he, she, or it:

- Has entered into an Authorized Relying Party Agreement and agreed to be bound by the terms and conditions of the CP-CPS;
- Verified that the Digital Signature in question (if any) was created by the Private Key corresponding to the Public Key in the TrustID Certificate during the time that the TrustID

Certificate was valid, and that the communication signed with the Digital Signature had not been altered;
- Verified that the TrustID Certificate in question was valid at the time of the Authorized Relying Party's reliance, by conducting a status check of the Certificate's then-current validity as required by IdenTrust; and
- Used the TrustID Certificate for purposes appropriate under this CP-CPS, and under circumstances where reliance would be reasonable and in good faith in light of all the circumstances that were known or should have been known to the Authorized Relying Party before reliance.

An Authorized Relying Party bears all risk of relying on a TrustID Certificate while knowing or having reason to know of any facts that would cause a person of ordinary business prudence to refrain from relying on the Certificate.

Registration Agency: A Government Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter, or other certification. A Registration Agency may include, but is not limited to:

- a State Department of Corporations or a Secretary of State;
- a licensing agency, such as a State Department of Insurance; or
- a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Office of the Comptroller of the Currency or Office of Thrift Supervision.

Registration Authority (or RA): A Legal Entity that is not a CA, and hence does not sign or Issue Certificates, contractually delegated by IdenTrust to Accept and process Certificate applications, and to verify the identity of potential End Entities, and authenticate the information contained in Certificate applications, in conformity with the provisions of this Policy and related agreements. RA's do not sign or Issue Certificates.

Registered Agent: An individual or entity that is:

1. authorized by the Applicant to receive service of process and business communications on behalf of the Applicant; and
2. listed in the official records of the Applicant's Jurisdiction of Incorporation as acting in the role specified in 1. above.

Registered Office: The official address of a company, as recorded with the Incorporating Agency, to which official documents are sent and at which legal notices are received.

Registration Number: The identifier assigned to a Business Entity, Private Organization, or Government Entity by the Incorporating Agency in such entity's Jurisdiction of Incorporation or Registration.

Registry-Controlled Label: A Public Suffix registered with a Domain Name Registrar.

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, which 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.

Request Token: A value, derived in a method specified by the Issuing CA which binds this demonstration of control to the Certificate Request.

Reserved IP Address: An Ipv4 or Ipv6 address that the IANA has marked as reserved:
https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
https://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Revocation: The act of making a Certificate permanently ineffective from a specified time forward. Revocation is effected by notation or inclusion in a set of revoked Certificates or other directory or database of revoked Certificates (e.g., inclusion in a CRL).

Risk Assessment: A formal process that

1. Identifies and documents foreseeable internal and external threats to the CA Infrastructure that could result in:
    - unauthorized access to the CA Infrastructure;
    - disclosure of data stored in the CA Infrastructure;
    - misuse of the CA Infrastructure; or
    - unapproved alteration or destruction of any part of the CA Infrastructure;
2. Assesses and documents the likelihood and potential damage of each identified threat, taking into consideration minimally the sensitivity and criticality of the CA Infrastructure; and
3. Assesses and documents the sufficiency of the policies, procedures, controls, information systems, technology, and other arrangements that the CA has in place to counter each identified threat.

Root CA Certificate: A self-signed and self-issued Certificate where:

1. the issuer and Subject of the Certificate are the same; and
2. the Digital Signature of the Certificate is: generated using the Private Key of a Key Pair whose corresponding Public Key is bound to the Certificate; and verified using the Public Key contained in the Certificate.

Root CA Private Key: The Private Key associated with a Root CA Certificate.

Root CA System: A System used to:

1. generate a Key Pair whose Private Key is or will be a Root CA Private Key;
2. store a Root CA Private Key; or
3. create Digital Signatures using a Root CA Private Key.

Root Key Generation Script: A documented plan of procedures to be performed for the generation of the Root CA Key Pair.

Secure Room: The room within the data center housing the CA production equipment for IdenTrust. Only specific authorized Trusted Role employees are granted access to the Secure Room based on their roles on a need-to-know or need-to-have-access basis. Such authorization is granted by the Head of Operations, or when so designated, by the Security Office.

Security Support System: The System(s) supporting the security of CA Infrastructure, performing functions such as

1. authentication;
2. audit logging;
3. audit log reduction and analysis;
4. vulnerability scanning;
5. physical intrusion detection;
6. host-based intrusion detection; and
7. network-based intrusion detection.

Shared Secret: Activation Data used to assist parties with Identity Proofing and establishing a reliable channel of communication. For purposes of establishing identity between an RA and a Subscriber, a Shared Secret may consist of an account PIN or online banking Account Password shared solely between the RA and the Subscriber, but not IdenTrust. For purposes of establishing identity between the Subscriber and IdenTrust necessary for Certificate Issuance, a Shared Secret consists of different Activation Data, which is shared among the RA, Subscriber, and IdenTrust.

Short-lived Subscriber Certificate: For Certificates issued on or after March 15, 2024 and prior to March 15, 2026, a Subscriber Certificate with a Validity Period less than or equal to 10 days (864,000 seconds). For Certificates issued on or after March 15, 2026, a Subscriber Certificate with a Validity Period less than or equal to 7 days (604,800 seconds).

Split-Knowledge Technique: A security procedure where no single Individual possesses the equipment, knowledge, or expertise to view, alter or otherwise have access to sensitive or confidential information in a particular PKI.

Sponsoring Organization: An Organization that has an affiliation with an Individual and has permitted the Individual to hold a TrustID Certificate that identifies the Sponsoring Organization and the fact of the Individual's affiliation with the Sponsoring Organization (see Affiliated Individual). In the case of Certificates issued to Electronic Devices, the Sponsoring Organization owns or controls the Electronic Device or the information asserted in the Certificate such as the Domain Name for a Certificate issued for a server. In the context of the CP, they are also called Applicant but from hereon they are referred to as Sponsoring Organizations.

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 Distinguished Name: The specific field in a Certificate containing the unique name-identifier for the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name or an IP Address 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.

Subordinate CA Certificate: A Certificate that is signed by the IdenTrust Root CA or other Subordinate CA's within the IdenTrust Root chain. Subordinate CA Certificates and their corresponding Public Keys may be embedded into software obtained or downloaded by the affirmative act of an Authorized Relying Party in order to establish a certification chain within the

TrustID PKI hierarchy.

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

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

Subscriber Certificate: See TrustID Certificate.

System: One or more pieces of equipment or software that stores, transforms, or communicates data.

Technically Constrained Subordinate CA Certificate: A Subordinate CA Certificate that uses a combination of Extended Key Usage and Name Constraint extensions as defined within the Certificate Profile 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 this CP-CPS when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

Token: A Cryptographic Module consisting of a hardware object (e.g., a "smart card"), often with memory and a microchip.

Top-Level Domain: From RFC 8499 (https://tools.ietf.org/html/rfc8499) "A Top-Level Domain is a zone that is one layer below the root, such as"com" or "jp".

Trusted Agent(s): Entity authorized to act as a representative of a Sponsoring Organization in verifying Applicant or PKI Sponsor identification during the registration process. Trusted Agents do not have automated interfaces with CAs. See Section 1.3.5.5.

Trusted Role(s): An individual employee or contractor of a CA or Delegated Third Party who has authorized access to any Certificate System or Root CA System.

TrustID Certificate: A TLS Certificate issued pursuant to this CP-CPS.

Valid Certificate: Certificate that passes the validation procedures specified in this CP-CPS which are in line with RFC 5280.

Validity Period: The intended term of validity of a Certificate, beginning with the date of Issuance ("Valid From" or "Activation" date), and ending on the expiration date indicated in the Certificate ("Valid To" or "Expiry" date). From Section 4.1.2.5 of RFC 5280: "The period of time from *notBefore* through *notAfter*, inclusive".

WHOIS: Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

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

Workstation: A device, such as a phone, tablet, or desktop or laptop computer, which is:

1. connected to the same network as CA Infrastructure and/or Network Equipment; and
2. capable of accessing CA Infrastructure and/or Network Equipment.

1.6.2 Acronyms

ACME: Automated Certificate Management Environment
AO: Authorizing Official
CA: Certification Authority
CAA: Certification Authority Authorization
CMA: Certificate Manufacturing Authority
CMS: Card Management System
CN: Common Name
CP: Certificate Policy
CPS: Certification Practice Statement
CRL: Certificate Revocation List
CSA: Certificate Status Authority
CT: Certificate Transparency
CVSS: Common Vulnerability Scoring System
DBA: Doing Business As
DN: Distinguished Name
DNS: Domain Name System
doS/DdoS: Denial of Service/Distributed Denial of Service
DSA: Digital Signature Algorithm
ECDSA: Elliptic Curve Digital Signature Algorithm
EKU: Extended Key Usage
EV: Extended Validation **FIPS:** Federal Information Processing Standard (U.S. Government)
FQDN: Fully Qualified Domain Name
gTLD: General Top-Level Domain
ICANN: Internet Corporation for Assigned Names and Numbers
ISO: International Standards Organization
ITU: International Telecommunications Union
NVD: National Vulnerability Database
LRA: Local Registration Agent
NIST: National Institute of Standards and Technology (U.S. Government)
OCC: Office of the Comptroller of the Currency
OCSP: Online Certificate Status Protocol
OID: Object Identifier
PED: PIN Entry Device
PIN: Personal Identification Number (e.g., an Account Password)
PIV: Personal Identity Verification
PKI: Public Key Infrastructure
PKIX: IETF Working Group on Public Key Infrastructure
PMA: The IdenTrust Policy Management Authority
QGIS: Qualified Government Information Source
QGTIS: Qualified Government Tax Information Source
RA: Registration Authority
RSA: Rivest-Shamir-Adleman cryptosystem
SAN: Subject Alternative Name
S/MIME: Secure Multipurpose Internet Mail Exchange
SSP: System Security Plan
TLS: Transport Layer Security
TTL: Time to Live

URI: Uniform Resource Identifier
URL: Uniform Resource Locator
X.500: The ITU-T (International Telecommunication Union-T) standard that establishes a distributed, hierarchical directory protocol organized by country, region, Organization, etc.
X.501: The ITU-T (International Telecommunication Union-T) standard for use of Distinguished Names in an X.500 directory.
X.509: The ITU-T (International Telecommunication Union-T) standard for Certificates. X.509, version 3, refers to Certificates containing or capable of containing extensions.

1.6.3 References

- The CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates (TLS BR)
- The CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates (EV TLS BR)
- The CA/Browser Forum Network and Certificate System Security Requirements (NetSec BR)
- Common CA Database (CCADB)
- The Apple Root Certificate Program
- The Chrome Root Program Policy
- The Microsoft Trusted Root Program
- The Mozilla Root Store Policy
- WebTrust Program for Certification Authorities WebTrust Principles and Criteria for Certification Authorities – SSL Baseline
- WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL
- WebTrust Principles and Criteria for Certification Authorities - Network Security
- WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security

1.6.4 Conventions

No stipulation.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

IdenTrust shall make Revocation information for its Publicly Trusted Subordinate Certificates and Subscriber Certificates available in accordance with this CP-CPS.

IdenTrust as the Issuing CA operates and maintains a Repository to support its TrustID PKI operations and to provide information concerning the status of all TrustID Certificates issued.

The Repository consists of documents and signed objects made available on this website https://www.identrust.com/support/documents/trustid.

2.2 Publication of Certification Information

The following IdenTrust CA information is published and publicly available in the Repository:

- Copy of the current CP-CPS;
- Archived copies of previously approved/published CP, CPS, CP-CPS; and
- Other information related to IdenTrust (Application forms, Product Datasheets, Agreements,

etc.).

The Repository with current and archived document versions is available on a 24X7 basis at:

https://www.identrust.com/support/documents/trustid

This CP-CPS document is structured in accordance with the framework outlined in RFC 3647.

This CP-CPS conforms to the latest published version of the TLS BR. In the event of any inconsistency between this CP-CPS, the TLS BR, the TLS BR takes precedence.

The following webpage is available for testing Subscriber Certificates - valid, revoked, and expired - chaining up to the IdenTrust Publicly-Trusted root: https://testssl.identrust.com/

2.3 Time or Frequency of Publication

IdenTrust develops, implements, enforces, and reviews its CP-CPS at least annually - updating it even when no other changes are necessary - to ensure the Issuing CA remains compliant with the latest TLS BR requirements and applicable browser root store policies.

The CP-CPS is reviewed and updated at least once every 366 days. Each revision is tracked by incrementing the version number and adding a dated changelog entry, even if no other changes are made.

When the Policy Management Authority (PMA) approves changes to the CP-CPS, IdenTrust incorporates these updates and publishes the revised version accordingly.

All information required by the CP-CPS is published promptly upon availability in the Repository in both PDF and Markdown formats. TrustID Certificates are made publicly accessible immediately after Acceptance by the Subscriber. Certificate status information is published in accordance with the requirements outlined in the CP-CPS.

2.4 Access Controls on Repositories

IdenTrust as Issuing CA makes its Repository publicly available in a read-only manner.

See Section 2.2.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

IdenTrust adheres to X.500, RFC 5280, and CA/Browser Forum naming requirements.

Names used in Certificates are X.501 Distinguished Names (DNs). Where DNs are required, Subscribers are assigned the appropriate DNs by IdenTrust, in accordance with the naming guidelines in Section 3.1.4 and Section 3.1.5. Certificates may also include other name forms in the SAN extension provided it is marked as non-critical.

3.1.2 Need for Names to Be Meaningful

Each field in the Certificate's Distinguished Name must be linked to the validated Domain Name of the Subscriber Organization.

3.1.3 Anonymity or Pseudonymity of Subscribers

IdenTrust does not issue TrustID certificates to anonymous or pseudonymous Subscribers; all Certificate Applicants must be reliably identified and authenticated in accordance with the requirements set forth in this CP-CPS.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using the X.500 series of specifications and ASN.1 syntax. FQDNs can be resolved through Domain Name services (DNS). Sections 4.1.2.4 and 4.2.1.7 of RFC 5280 describe how character sets and strings are to be interpreted in Issuer and Subject fields, and Subject Alternative Name (SAN) extension.

3.1.5 Uniqueness of Names

The IdenTrust enforces name uniqueness within the X.500 name space by assigning unique Certificate serial numbers.

3.1.6 Recognition, Authentication, and Role of Trademarks

An IdenTrust Applicant/PKI Sponsor is not guaranteed that its Certificate's Subject Name will contain any requested trademark, and an Applicant PKI Sponsor requesting a specific name may be required to demonstrate the right to the use of that name. IdenTrust may request evidence of ownership of trademarks or the findings and orders from courts or other tribunals.

3.2 Initial Identity Validation

IdenTrust as Issuing CA is responsible for performing the Identity Proofing of End Entities before the Issuance of TrustID Certificates. IdenTrust performs Identity Proofing itself, aided by its LRAs, or by elected Enterprise RAs from Sponsoring Organizations, or may designate one or more institutions as RAs.

All documents and data used to verify a TrustID Certificate must not accepted by the RA if they were obtained more than 825[1] days before the Certificate is issued.

For EV Certificates, the age of all data used to support issuance of an EV Certificate (before revalidation is required) shall not exceed these limits:

- Legal existence and identity – 398 days;
- Assumed name – 398 days;
- Address of Place of Business – 398 days;
- Verified Method of Communication – 398 days;
- Operational existence – 398 days;
- Domain Name – 398 days;
- Name, Title, Agency, and Authority – 398 days, unless a contract between IdenTrust and the Applicant specifies a different term, in which case, the term specified in such contract controls.
- The 398-day period set forth above shall begin to run on the date the information was collected by IdenTrust.
- IdenTrust may reuse a previously submitted EV Certificate Request, Subscriber Agreement, or Terms of Use, including use of a single EV Certificate Request in support of multiple EV

[1] 398 days when issued on or after March 15, 2026.

Certificates containing the same Subject to the extent permitted under a Subscriber Agreement.2.9 and Section 3.2.2.

IdenTrust repeats the verification process required for any information obtained outside the time limits specified above except when permitted otherwise under Section 4.2.1.

For validation of Domain Names and IP Addresses any reused data, document, or completed validation are obtained as described in Section 4.2.1.

3.2.1 Method to Prove Possession of Private Key

Applicants are required to prove possession of the Private Key corresponding to the Public Key in a Certificate request, which may be done by signing the request with the Private Key. An RSA *PKCS#10* Certificate signing request is used to establish that an Applicant or PKI Sponsor holds the Private Key that corresponds to the Public Key included in a Certificate. The *PKCS#10* is submitted by the Applicant/PKI Sponsor over a secure connection and verified by IdenTrust as part of the Certificate Issuance process as described below in Section 4. Proof of possession of the Private Key is established by verifying that the Applicant/PKI Sponsor's Digital Signature in the *PKCS#10* was created by the Private Key corresponding to the Public Key in the *PKCS#10*.

3.2.2 Authentication of Organization and Domain Identity

Requests by Sponsoring Organizations for Certificates are submitted electronically and must include the Organization's legal name and address. The minimum Identity Proofing required of a Sponsoring Organization includes confirmation that:

- The Sponsoring Organization legally exists and has conducted business from the address listed in the Certificate application; and
- The information contained in the Certificate application is correct.

The Identity Proofing process may include a review of official government records, an Attestation Letter, and/or engagement of a reputable third party vendor of business information to provide validation information concerning the Sponsoring Organization applying for the Certificate, such as:

- Legal company name;
- Registration Number (If included in the Subject as serial number)
- A registered Assumed Name (if included in the Subject)
- An organizational unit Name (if included in the Subject)
- An address of the Organization (if included in the Subject)
- Type of entity;
- Year of formation;
- State/region and country Jurisdiction of Incorporation;
- Names of directors and officers;
- Full business address;
- Telephone number;
- Proof of good standing in the jurisdiction where the Applicant is incorporated or otherwise organized; and

3.2.2.1 Authentication of the Individual-Organization Affiliation

The IdenTrust CA may Issue Certificates to Applicants affiliated to a Sponsoring Organization. A Sponsoring Organization must not be an Individual acting in a personal, non-business capacity.

The Sponsoring Organization need not be incorporated, but it must conduct business. An Individual acting in a business capacity as a sole proprietor, professional consultant, or fictitious entity (e.g., "DBA" as allowed by local law), may be considered "the Organization" for the purposes of populating the "O" attribute in the Subject field of the Certificate (for server Certificates, the DBA name of an Individual acting in a sole proprietorship must be verified and is required to populate the "O" attribute of the Certificate Profile). If the Applicant is located outside the United States of America, IdenTrust may impose, through the Subscriber Agreement, additional restrictions in view of other jurisdictions' laws governing privacy, consumer protection, and other rights of Individuals. For example, if an Applicant is located within the European community, the Subscriber Agreement may contain an additional attestation from the Applicant that the information provided shall be considered business data rather than personal data under *European Directive 95/46/EC* and/or that the Individual gives his/her unambiguous consent to the processing of such data by IdenTrust.

The affiliation between the Applicant and the Sponsoring Organization can be employment, agency, or a contractual relationship. After approval, an Applicant becomes a Subscriber. Because it is the Subscriber who holds the Private Key, any verifiable Digital Signature created by that Private Key is attributable to the Subscriber. Whether that Digital Signature can be viewed as the Sponsoring Organization's signature depends on whether the Subscriber as an Individual has authority to sign for the Sponsoring Organization in the transaction in question. That authority cannot be inferred from a Certificate issued by IdenTrust. IdenTrust does not Issue Certificates that assert roles or authorizations.

In other words, Certificates complying with this CP-CPS do not imply any grant of authority by the Sponsoring Organization. A Relying Party can infer from verification of a Digital Signature by reference to a Valid Certificate issued by IdenTrust that a Digital Signature is attributable to the Individual listed in that Certificate as the Subscriber. A Relying Party cannot, however, infer that the Individual as the Subscriber acted on behalf of the affiliated Sponsoring Organization from the Certificate; instead, additional documentation or evidence is required depending on the applicable law of agency.

Certificates issued by IdenTrust do not permit attribution of a Digital Signature to the Sponsoring Organization listed in that Certificate. However, LRAs and Trusted Agents will not approve Issuance of a Certificate to an Individual as the Subscriber without obtaining both of the following first with respect to the Certificate to be issued:

- The approval of the Sponsoring Organization with which that Individual as the Subscriber is affiliated. The approval enables the Sponsoring Organization to manage its internal PKI and infrastructure, but it is not in itself a grant of any authority. In its contract with IdenTrust or the RA, the Sponsoring Organization provides such approval of such, and the contract is required to be executed by an officer or similarly authorized representative of the Sponsoring Organization; and
- Verification of the existence of affiliation between the Sponsoring Organization and the Subscriber. This consists of verification of employment, contractual relationship, or agency. IdenTrust or the RA verifies this affiliation through a Sponsoring Organization's representative other than the PKI Sponsor, usually the Trusted Agent where such exists. Otherwise, IdenTrust or the RA initiates communication with the Sponsoring Organization using a Reliable Method of Communication. The contact used for verification within the Sponsoring Organization may be the human resources department or any Individual in a capacity within the Sponsoring Organization to confirm the affiliation.

IdenTrust or the RA records this confirmation in an auditable log.

When processing EV Certificates, the following additional checks are performed based on the Applicant:

- Verified Legal Opinion
- Verified Accountant Letter
- Face-to-face validation
- Independent confirmation from Applicant
- Qualified Independent Information Source (QIIS)
- Qualified Government Information Source (QGIS)
- Qualified Government Tax Information Source

3.2.2.2 Authentication of Subscribing Organization Identity

Before approving the inclusion of Sponsoring Organization information in a Certificate, IdenTrust verifies that the Sponsoring Organization legally exists, the physical address where it conducts business, the type of entity under which it operates, or any other Reliable Method of Communication where its representatives can be contacted.

LRAs or Trusted Agents verify the existence and name of a Sponsoring Organization in one of the following ways:

1. A reference to a source unrelated to the prospective Sponsoring Organization such as:
    - A secretary of state or other governmental registry such as a QGIS or QGTIS;
    - Commercial database of business information; or a
    - A third party database that is periodically updated, which IdenTrust has evaluated in accordance with Section 3.2.4.
2. Presentation to LRA of a copy of a document issued by a government agency attesting to the Sponsoring Organization's legal existence, together with reasonable proof of the authenticity of that document. Documents submitted for this purpose must be "fair on their face," i.e., bear no apparent indication of forgery, fraud, tampering, etc.;
3. In the case of an Organization that is not registered with a state regulatory agency (such as a partnership or unincorporated association), a copy of the partnership agreement, association rules, Assumed Name registration, or other document attesting to the Organization's existence;
4. LRA may independently obtain (without reference to the data provided by the Applicant or PKI Sponsor for a Certificate) the name, address, Email Address, and/or telephone number of the Organization, which are verified through a Reliable Method of Communication;
5. A site visit by an LRA or a third party who is acting as an agent for IdenTrust; or
6. An Attestation Letter by an authorized representative (e.g., a supervisor, administrative officer, information security officer, Authorizing Official, Certificate coordinator, etc.) of the Applicant/PKI Sponsor's employer that has been verified in accordance with this section, or by a person or entity certified by a government agency as being authorized to confirm Organization identities, provided that the Attestation Letter is checked to ensure legitimacy.

IdenTrust or, when applicable, RAs will keep evidence that their LRAs verified Organizational information including legal company name, type of entity, principal address (number and street, city, ZIP or postal code), Email Address or telephone number, and, when deemed necessary, Domain Name registration, a certified copy of the Certificate of registration issued by a Government Entity, date of formation, names of directors and officers.

IdenTrust reconfirms a Sponsoring Organization's existence based on the ongoing business relationship between IdenTrust and the Sponsoring Organization, which is maintained through correspondence or a payment stream and maintenance of a bank account.

For EV Certificates IdenTrust verifies that the physical address provided by the Applicant is an address where the Applicant or a Parent/Subsidiary Company conducts business operations (not, for example, a mail drop or P.O. box, or 'care of' (C/O) address, such as an address for an agent of the Organization), and is the address of the Applicant's Place of Business.

3.2.2.2.1 Verification of DBA or Tradename

If the PKI Sponsor wants to include a DBA or tradename, the PKI Sponsor must first prove that they have the right to use that name. To fulfill this requirement an LRA must request at least one piece of evidence from the following list that confirms ownership of the DBA or tradename during the verification process:

1. A letter/official legal document, phone call to an independently verified number, or an email from the domain registered to a government agency in the jurisdiction of the PKI Sponsor's Organization legal creation, existence, or recognition that validates the ownership of the DBA or tradename;
2. A letter/official legal document, phone call to an independently verified phone number, or an Email Address from the domain registered to a verifiable third party source that validates the ownership of the DBA or tradename;
3. A letter/official legal document, phone call to an independently verified phone number, or an Email Address from the domain registered to a government agency responsible for the management of such DBAs or tradenames;
4. An Attestation Letter accompanied by documentary support that validates the ownership of the DBA or Organization name; and
5. A Reliable Data Source.

All information obtained by this process will be uploaded to and retained electronically in the PKI Sponsor's application file in IdenTrust's or the RA's CA Infrastructure System. If the information is obtained through a phone call, IdenTrust documents the telephone number, the source it was obtained and verified through, and the name and title of the Individual that provided the information for the verification and place this information into the System through the related application account.

3.2.2.3 Verification of Country

IdenTrust verifies the country associated with the Subject by choosing one of the following processes:

- Through verification processes conducted by the LRA of the PKI Sponsor and the Organization in Section 3.2.2 and Section 3.2.2.1.
- Verifying the ccTLD with the Domain Name Registrar listed by the PKI Sponsor

If the PKI Sponsor applies for a Domain Name that contains a 2-letter country code (ccTLD) (e.g., www.identrust.uk as opposed to www.identrust.com), this confirmation will be sought from the Domain Name level to which the ccTLD applies. This means that IdenTrust cannot obtain verification from www.identrust.com if the PKI Sponsor is applying for a Domain Name from www.identrust.uk.

PKI Sponsors requesting a Certificate that will contain the *countryName* field and the other Sponsoring Organization will be verified by IdenTrust using the processes listed in Section 3.2.2 and Section 3.2.2.1.

IdenTrust may implement a process to screen proxy servers to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.

3.2.2.4 Validation of Domain Authorization or Control

Before issuing a TrustID Certificate, IdenTrust verifies the Applicant's control of the FQDN(s) or IP address(s) listed in the Certificate application using one or more of the validation methods listed below, maintaining a record of which of method was used, along with the relevant TLS BR version number used.

Effective March 15, 2026:

- DNSSEC validation back to the IANA DNSSEC root trust anchor must be performed on all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective. The DNS resolver used for all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective must:
    - Perform DNSSEC validation using the algorithm defined in RFC 4035 Section 5; and
    - Support NSEC3 as defined in RFC 5155; and
    - Support SHA-2 as defined in RFC 4509 and RFC 5702; and
    - Properly handle the security concerns enumerated in RFC 6840 Section 4.
- For e-mail Domain Validation methods described in Section 3.2.2.4.1, DNSSEC validation back to the IANA DNSSEC root trust anchor must be performed on all DNS CNAME, CAA, TXT queries attempting to obtain the Authorization Domain Name associated with the validation of domain authorization or control by the Primary Network Perspective and IdenTrust does not set local policy to disable DNSSEC validation.
- For all other Domain Validation methods, DNSSEC validation back to the IANA DNSSEC root trust anchor must be performed on all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective and IdenTrust must not use local policy to disable DNSSEC validation on any DNS query associated with the validation of domain authorization or control.
- DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of self-audits performed to fulfill the requirements in Section 8.7.
- DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of the logging requirements of Section 5.4.1.

Additional checks and verification will be made for EV Certificate applications as follows:

1. Verify Applicant's existence and identity, including;
    - Verify the Applicant's legal existence and identity (as described in Section 3.2.2.2),
    - Verify the Applicant's physical existence (business presence at a physical address), and
    - Verify the Applicant's operational existence (business activity).
2. Verify the Applicant is a registered holder, or has control, of the Domain Name(s) to be included in the EV Certificate;
3. Verify a reliable means of communication with the entity to be named as the Subject in the Certificate;

4. Verify the Applicant's authorization for the EV Certificate, including;
    - Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester,
    - Verify that a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and agreed to the Terms of Use; and
    - Verify that a Certificate Approver has signed or otherwise approved the EV Certificate Request.

3.2.2.4.1 Validating the Applicant as a Domain Contact

This method is no longer allowed. IdenTrust does not use this method.

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

This method is no longer allowed. IdenTrust does not use this method.

3.2.2.4.3 Phone Contact with Domain Contact

This method is no longer allowed. IdenTrust does not use this method.

3.2.2.4.4 Email to a Constructed Address

IdenTrust confirms the Applicant's control over the FQDN by

1. sending an email to one or more addresses created by using 'admin,' 'administrator,' 'webmaster,' 'hostmaster,' or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, and
2. including a Random Value in the email, and
3. receiving a confirming response utilizing the Random Value.

Each email may confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed.

The Random Value shall be unique in each email.

The email may be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient shall remain unchanged.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, IdenTrust may also Issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating wildcard Domain Names.

Effective March 15, 2028, IdenTrust will not use this domain validation method.

3.2.2.4.5 Domain Authorization Document

This method is no longer allowed. IdenTrust does not use this method.

3.2.2.4.6 Agreed-Upon Change to Website

This method is no longer allowed. IdenTrust does not use this method.

3.2.2.4.7 DNS Change

IdenTrust confirms the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT, or CAA record for either

1. an Authorization Domain Name; or
2. an Authorization Domain Name that is prefixed with a Domain Label that begins with an underscore character.

If a Random Value is used, IdenTrust shall provide a Random Value unique to the Certificate Request and shall not use the Random Value after

1. 30 days or
2. if the Applicant submitted the Certificate Request, the time frame permitted for reuse of validated information relevant to the Certificate such as in Section 4.2.1.

When using this method, IdenTrust implements Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective must observe the challenge information (i.e., Random Value or Request Token) as the Primary Network Perspective.

If IdenTrust or an Affiliate of IdenTrust operates a DNS zone to which Applicants can delegate (via CNAME) their underscore-prefixed Domain Label, IdenTrust ensures that each Applicant delegates to a unique FQDN within that zone. IdenTrust or Affiliates should not operate such a service, and should direct any Applicants using such a service to use the method described in Section 3.2.2.5.4 instead.

Note: Once the FQDN has been validated using this method, IdenTrust may also Issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.8 IP Address

This method is no longer allowed. IdenTrust does not use this method.

3.2.2.4.9 Test Certificate

This method is no longer allowed. IdenTrust does not use this method.

3.2.2.4.10 TLS Using a Random Value

This method is no longer allowed. IdenTrust does not use this method.

3.2.2.4.11 Any Other Method

This method is no longer allowed. IdenTrust does not use this method.

3.2.2.4.12 Validating Applicant as a Domain Contact

IdenTrust does not use this method.

3.2.2.4.13 Email to DNS CAA Contact

IdenTrust does not use this method.

3.2.2.4.14 Email to DNS TXT Contact

IdenTrust does not use this method.

3.2.2.4.15 Phone Contact with Domain Contact

This method is no longer allowed. IdenTrust does not use this method.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

IdenTrust does not use this method.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

IdenTrust does not use this method.

3.2.2.4.18 Agreed-Upon Change to Website v2

IdenTrust confirms the Applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file.

1. The entire Request Token or Random Value must not appear in the request used to retrieve the file, and
2. IdenTrust must receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Value:

1. Must be located on the Authorization Domain Name, and
2. Must be located under the "*/.well-known/pki-validation*" directory, and
3. Must be retrieved via either the "http" or "https" scheme, and
4. Must be accessed over an Authorized Port.

If IdenTrust follows redirects, the following apply:

1. Redirects must be initiated at the HTTP protocol layer.
    - Redirects must be the result of a 301, 302, or 307 HTTP status code response, as defined in Section 6.4 of RFC 7231, or a 308 HTTP status code response, as defined in Section 3 of RFC 7538. Redirects must be to the final value of the Location HTTP response header, as defined in Section 7.1.2 of RFC 7231.
2. Redirects must be to resource URLs with either via the "http" or "https" scheme.
3. Redirects must be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:

- IdenTrust must provide a Random Value unique to the Certificate Request.
- The Random Value must remain valid for use in a confirming response for no more than 30 days from its creation.

Except for Onion Domain Names, when IdenTrust performs validations using this method it implements Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective must observe the same challenge information (i.e., Random Value or Request Token) as the Primary Network Perspective.

Note: IdenTrust does not Issue Certificates for other FQDNs that end with all the labels of the

validated FQDN unless IdenTrust performs separate validations for each of those other FQDNs using authorized methods. This method is not suitable for validating Wildcard Domain Names.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

IdenTrust confirms the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555. The token (as defined in RFC 8555, Section 8.3) must not be used for more than 30 days from its creation. If IdenTrust follows redirects, the following apply:

1. Redirects must be initiated at the HTTP protocol layer. Redirects must be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects must be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.
2. Redirects must be to resource URLs with either the "http" or "https" scheme.
3. Redirects must be to resource URLs accessed via Authorized Ports.

Except for Onion Domain Names, when IdenTrust performs validations using this method, it implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective must observe the same challenge information (i.e. token) as the Primary Network Perspective.

Note: IdenTrust does not issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless IdenTrust performs separate validations for each of those other FQDNs using authorized methods. This method is not suitable for validating Wildcard Domain Names.

3.2.2.4.20 TLS Using ALPN

IdenTrust does not use this method.

3.2.2.4.21 DNS Labeled with Account ID - ACME

IdenTrust does not use this method.

3.2.2.4.22 DNS TXT Record with Persistent Value

Confirming the Applicant's control over a FQDN by verifying the presence of a Persistent DCV TXT Record identifying the Applicant. The record MUST be placed at the "_validation-persist" label prepended to the Authorization Domain Name being validated (i.e., "_validation-persist.[Authorization Domain Name]"). For this method, IdenTrust must not use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. This prohibition overrides the Authorization Domain Name definition. CNAME records may be followed when resolving the Persistent DCV TXT Record.

IdenTrust must confirm the Persistent DCV TXT Record's RDATA value fulfills the following requirements:

1. The RDATA value must conform to the issue-value syntax as defined in RFC 8659, Section 4.2; and
2. The issuer-domain-name value must be an Issuer Domain Name disclosed in Section 4.2.1.1; and
3. The issue-value must contain an accounturi parameter, where the parameter value is a unique URI (as described by RFC 8657, Section 3) identifying the account of the Applicant

which requested validation for this FQDN; and
4. The issue-value may contain a persistUntil parameter. If present, the parameter value must be a base-10 encoded integer representing a UNIX timestamp (the number of seconds since 1970-01-01T00:00:00Z ignoring leap seconds); and
5. The issue-value may contain additional parameters. IdenTrust ignore any unknown parameter keys.

If the persistUntil parameter is present, IdenTrust must evaluate its value. If the time of the check is after the time specified in the persistUntil parameter value, IdenTrust must not use the record as evidence of the Applicant's control over the FQDN.

For example, the Persistent DCV TXT Record might look like: _validation-persist.example.com IN TXT "authority.example; accounturi=https://authority.example/acct/123; persistUntil=1782424856"

For the purposes of Section 4.2.1, IdenTrust considers 10 days as the maximum validation data reuse period for validations completed using this method.

The following table shows how the persistUntil parameter affects whether a DNS record can be used for validation at different points in time:

Date/time of validation	PersistUntil	Usable for Validation	Explanation
2025-06-15T12:00:00Z	2026-01-01T00:00:00Z (1767225600)	Yes	Validation time is before persistUntil timestamp, so record is usable
2025-06-15T12:00:00Z	2025-01-01T00:00:00Z (1735689600)	No	Validation time is after persistUntil timestamp, so record is not usable
2025-06-15T12:00:00Z	(not present)	Yes	No persistUntil parameter present, so no time restriction applies

Example of how persistuntil parameters affects validation:

When using this method, IdenTrust implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective must observe a Persistent DCV TXT Record that demonstrates the Applicant's control over the domain and contains the same accounturi parameter as the Primary Network Perspective.

Note: Once the FQDN has been validated using this method, IdenTrust may also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.5 Authentication for an IP Address

IdenTrust as the Issuing CA shall confirm that before Issuance, it has validated each IP Address listed in the Certificate Application using at least one of the methods specified in this section.

Completed validations of Applicant authority may be valid for the Issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the period specified in the relevant requirement such as those in Section 4.2.1, before Certificate Issuance. For purposes of IP Address validation, the term Applicant includes the Applicant's parent company, subsidiary company, or Affiliate.

IdenTrust shall maintain a record of which IP validation method, including the relevant B.R. version number that was used to validate every IP Address.

3.2.2.5.1 Agreed-Upon Change to Website

IdenTrust confirms the Applicant's control over the requested IP Address by confirming the presence of a Random Value contained in the content of a file or webpage in the form of a meta tag under the "*/.well-known/pki-validation*" directory, or another path registered with IANA for the purpose of validating control of IP Addresses, on the IP Address that is accessible by the CA via HTTP/HTTPS over an Authorized Port.

The Random Value:

1. Must not appear in the request
2. Must be unique to the Certificate Request and
3. Must not be used after the longer of
    - 30 days or
    - if the Applicant submitted the Certificate Request, the timeframe permitted for reuse of validated information relevant to the Certificate such as those in Section 4.2.1.

When IdenTrust performs validations using this method, it must implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective must observe the same challenge information (i.e., Random Value or Request Token) as the Primary Network Perspective.

3.2.2.5.2 Email to IP Address Contact

IdenTrust confirms the Applicant's control over the IP Address by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value must be sent to an Email Address identified as an IP Address Contact.

Each email may confirm control of multiple IP Addresses.

IdenTrust may send the email identified under this section to more than one recipient provided that every recipient is identified by the IP Address Registration Authority as representing the IP Address Contact for every IP Address being verified using the email.

The Random Value shall be unique in each email.

IdenTrust may resend the email in its entirety, including re-use of the Random Value, provided that the communication's entire contents and the recipient(s) remain unchanged.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

Effective March 15, 2027, IdenTrust will not use this domain validation method.

3.2.2.5.3 Reverse Address Lookup

IdenTrust does not use this method.

3.2.2.5.4 Any Other Method

This method is no longer allowed. IdenTrust does not use this method.

3.2.2.5.5 Phone Contact with IP Address Contact

IdenTrust does not use this method.

3.2.2.5.6 ACME "http-01" method for IP Addresses

IdenTrust confirms the Applicant's control over the IP Address by performing the procedure for an "http-01" challenge in RFC 8738. When using this method, IdenTrust implements Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9.

3.2.2.5.7 ACME "tls-alpn-01" method for IP Addresses

IdenTrust does not use this method.

3.2.2.5.8 DNS TXT Record with Persistent Value in the Reverse Namespace

IdenTrust does not use this method.

3.2.2.6 Wildcard Domain Validation

Before issuing a wildcard Certificate with a FQDN, the control of the entire Domain Namespace delimited by the FQDN will be verified by an IdenTrust LRA through a combination of manual and automatic checks to determine whether the wildcard character is placed immediately to the left of a Reliable Data Source or Public Suffix. To perform such verification, the IdenTrust LRA will use the public list of suffixes available in https://publicsuffix.org/ and shall use additional sources as IdenTrust may specify to the IdenTrust LRA from time to time. For example, FQDNs such as "*.co.tz" or "*.k12.ut.us" cannot be accepted since in each case the wildcard is immediately to the left of a suffix in the list available at https://publicsuffix.org/.

For some gTLDs, the entire Domain Namespace may be controlled by one Subscribing Organization (e.g., ".Cisco," ".IBM"). If that rare case needs to be addressed, the process in the section below is completed first and the Subscribing Organization will provide written assertions about the rightful control over the entire Domain Namespace. See Section 3.2.2.6.1 below Verification of gTLD Domains

3.2.2.6.1 Verification of gTLD Domains

IdenTrust does not issue server Certificates containing general Top-Level Domain Names (gTLDs) that are not currently approved or in the process of being approved by the Internet Corporation for Assigned Names and Numbers (ICANN). FQDNs containing a gTLD that has not been approved will be rejected in the application process until ICANN finalizes the approval of the gTLD.

IdenTrust does not issue server Certificates for Reserved IP Addresses, or internal server names and will not issue them for the gTLD domains not approved on these grounds. IdenTrust does not issue server Certificates to Internal Names including those that may contain an unassigned gTLD.

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, IdenTrust evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The following factors are considered for this evaluation:

1. The age of the information provided,
2. The frequency of updates to the information source,
3. The data provider and purpose of the data collection,
4. The public accessibility of the data availability, and
5. The relative difficulty in falsifying or altering the data.

IdenTrust or the RA may rely upon an Attestation Letter attesting that Subject Information or other fact is correct. IdenTrust or the RA shall verify that the Attestation Letter was written by an accountant, lawyer, government official, or other reliable third party in the Applicant's jurisdiction customarily relied upon for such information.

An Attestation Letter shall include a copy of documentation supporting the fact to be attested. IdenTrust or the RA shall use a Reliable Method of Communication to contact the sender and to confirm the Attestation Letter is authentic.

3.2.2.8 CAA Records

See Section 4.2.1.1, CAA Checking.

3.2.2.9 Multi-Perspective Issuance Corroboration

Multi-Perspective Issuance Corroboration attempts to corroborate the determinations (i.e., domain validation pass/fail, CAA permission/prohibition) made by the Primary Network Perspective from multiple remote Network Perspectives before Certificate issuance. This process can improve protection against equally-specific prefix Border Gateway Protocol (BGP) attacks or hijacks.

IdenTrust may use either the same set, or different sets of Network Perspectives when performing Multi-Perspective Issuance Corroboration for the required

1. Domain Authorization or Control, and
2. CAA Record checks.

The set of responses from the relied upon Network Perspectives provide IdenTrust with the necessary information to allow it to affirmatively assess:

1. the presence of the expected
    - Random Value,
    - Request Token,
    - IP Address,
    - Contact Address, or
    - Persistent DCV TXT Record, as required by the relied upon validation method specified in Section 3.2.2.4, Section 3.2.2.5; and
2. IdenTrust's authority to issue to the requested domain(s), as specified in Section 4.2.1.1

Results or information obtained from one Network Perspective are not to be reused or cached when performing validation through subsequent Network Perspectives.

The network infrastructure providing Internet connectivity to a Network Perspective may be administered by the same organization providing the computational services required to operate the Network Perspective. All communications between a remote Network Perspective and IdenTrust will take place over an authenticated and encrypted channel relying on modern protocols (e.g., over HTTPS).

A Network Perspective may use a recursive DNS resolver that is not co-located with the Network

Perspective. However, the DNS resolver used by the Network Perspective must fall within the same Regional Internet Registry service region as the Network Perspective relying upon it. Furthermore, for any pair of DNS resolvers used on a Multi-Perspective Issuance Corroboration attempt, the straight-line distance between the two DNS resolvers must be at least 500 km. The location of a DNS resolver is determined by the point where unencapsulated outbound DNS queries are typically first handed off to the network infrastructure providing Internet connectivity to that DNS resolver.

IdenTrust may immediately retry Multi-Perspective Issuance Corroboration using the same validation method or an alternative method. When retrying Multi-Perspective Issuance Corroboration, IdenTrust does not rely on corroborations from previous attempts. There is no stipulation regarding the maximum number of validation attempts that may be performed in any period of time.

The "Quorum Requirements" table below describes quorum requirements related to Multi-Perspective Issuance Corroboration. If IdenTrust does not rely on the same set of Network Perspectives for both Domain Authorization or Control and CAA Record checks, the quorum requirements must be met for both sets of Network Perspectives. Network Perspectives are considered distinct when the straight-line distance between them is at least 500 km. Network Perspectives are considered "remote" when they are distinct from the Primary Network Perspective and the other Network Perspectives represented in a quorum.

IdenTrust may reuse corroborating evidence for CAA record quorum compliance for a maximum of 398 days. After issuing a Certificate to a domain, remote Network Perspectives may omit retrieving and processing CAA records for the same domain or its subdomains in subsequent Certificate requests from the same Applicant for up to a maximum of 398 days.

Quorum Requirements Table

# of Distinct Remote Network Perspectives Used	# of Allowed non-Corroborations
2-5	1
6+	2

Remote Network Perspectives performing Multi-Perspective Issuance Corroboration must rely upon networks (e.g., Internet Service Providers or Cloud Provider Networks) implementing measures to mitigate BGP routing incidents in the global Internet routing system for providing internet connectivity to the Network Perspective.

For server Certificates, IdenTrust requires Multi-Perspective Issuance Corroboration using at least four (4) remote Network Perspectives, and IdenTrust ensures that the requirements defined above in the in Quorum Requirements table are satisfied. If the requirements are not satisfied, then the server Certificate cannot be issued.

3.2.3 Authentication of Individual Identity

IdenTrust does not issue server Certificates to individuals, only to sponsoring Organizations.

3.2.4 Non-Verified Subscriber information

IdenTrust does not include unverified Subscriber information in TrustID Certificates. This principle is enforced by the Certificate Profiles described in Section 7, which only allow certain information to be included in Certificates. The processes described in Section 3 and Section 4 prevent any information that is not verified to be included in the Certificate.

3.2.5 Validation of Authority

Certificates issued to Subscribers do not assert authority to act on behalf of an Organization in an implied capacity.

IdenTrust may use the sources listed in Section 3.2.5.2

Provided that IdenTrust uses a Reliable Method of Communication, IdenTrust may establish the authenticity of the Certificate Request directly with the Applicant Representative or with an authoritative source within the Applicant's Organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that IdenTrust deems appropriate.

3.2.5.1 Verification of the Certificate Request

When evaluating the authenticity of a Certificate Request, IdenTrust or the Enterprise RA will establish the verification directly with the Applicant/PKI Sponsor. Any information collected during the verification process by IdenTrust or the Enterprise RA will be placed into the System for documentation purposes. The source of verification will depend upon the type of Certificate Requested.

If a Certificate Request is being submitted to an Enterprise RA, verification of the Certificate Request is completed by the Enterprise RA. The Enterprise RA will contact the PKI Sponsor via the company/Organization internal directory or telephone list that is maintained by the human resources department or similar authority. Equivalent processes to fulfill this verification may be approved by the PMA and documented by the Sponsoring Organization with Enterprise RAs. The Enterprise RA will request to speak to the PKI Sponsor at the Sponsoring Organization telephone number and upon confirming identity, will ask the PKI Sponsor to verify the validity of the request.

For EV Certificate applications, IdenTrust verifies:

1. Applicant's existence and identity, including;
   - Verification of the Applicant's legal existence and identity (as more fully set forth in Section 3.2.2.2),
   - The Applicant's physical existence (business presence at a physical address), and
   - The Applicant's operational existence (business activity).
2. The Applicant is a registered holder, or has control, of the Domain Name(s) to be included in the EV Certificate;
3. A reliable means of communication with the entity to be named as the Subject in the Certificate;
4. The Applicant's authorization for the EV Certificate, including;
   - The name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester,
   - That a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and agreed to the Terms of Use; and
   - That a Certificate Approver has signed or otherwise approved the EV Certificate Request.

3.2.5.2 Disclosure of Verification Sources

IdenTrust may use third party vendors to obtain regularly updated and current information from the government register provided that the third party obtains the information directly from the

government.

For validation of Organizations that apply for EV Server, at the time of Certificate Issuance, IdenTrust documents and publishes the applicable Incorporating Agency or Registration Agency used as validation source to validate the applying Organization at this location. The "Organization Verification Sources" document is located in the "Product Datasheets" section.

3.2.5.3 Reliability of Verification Sources

Before relying on a source of verification data to validate Certificate Requests, IdenTrust verifies its suitability as a Reliable Data Source.

The RA may rely upon an Attestation Letter attesting that Subject Information or other fact is correct. The RA shall verify that the Attestation Letter was written by an accountant, lawyer, government official, or other reliable third party in the Applicant's jurisdiction customarily relied upon for such information.

An Attestation Letter shall include a copy of documentation supporting the fact to be attested. The RA shall use a Reliable Method of Communication to contact the sender and to confirm the Attestation Letter is authentic.

3.2.5.4 Verification and Validation of Certificate Information Sources

In addition to the verification of information, by comparison to trusted information as described above, two additional verifications of information may be conducted before Issuance to verify the information provided by the PKI Sponsor:

- High risk domain requests will be checked against a third party authority as described in Section 4.2.1.3; and
- High-risk denials, as documented in Section 4.2.2, are prior requests that have been denied and are deemed as high risk due to suspected phishing or other fraudulent usage or concerns are maintained in an internal list. Subsequent Certificate Requests will be verified against this list. For EV Certificates, the following additional checks are performed based on the Applicant:
- Verified Legal Opinion
- Verified Accountant Letter
- Face-to-face validation
- Independent confirmation from Applicant
- Qualified Independent Information Source (QIIS)
- Qualified Government Information Source (QGIS)
- Qualified Government Tax Information Source

Should a third party vendor be utilized to confirm the information provided manually or electronically, IdenTrust or the RA will evaluate the third party source by these required criteria: 1. Data it contains that will be relied upon has been independently verified 2. The database distinguishes between self-reported data and data reported by independent information sources; and 3. Changes in the data that will be relied upon will be reflected in the database in no more than 12 months.

In addition, the following criteria will be taken into account while reviewing the information taken from the third party source:

- The age of the information provided;
- The frequency of updates to the third party database;
- The data provided and purpose of the data collection;
- The public accessibility of the data availability; and
- The relative difficulty in falsifying or altering the data.

3.2.6 Criteria for Interoperation

IdenTrust as the Issuing CA adheres to the following requirements:

- Operate a PKI that has undergone a successful compliance audit pursuant to Section 8;
- Issue Certificates interoperable with the profiles described in Section 7, and make Certificate status information available in compliance with this CP-CPS;
- Provide CA Certificate and Certificate status information to the Authorized Relying Parties; and
- Disclose all Cross-Certified Subordinate CA Certificates that identify the CA as the Subject, provided that it has arranged for or accepted the establishment of the trust relationship (i.e., the Cross-Certified Subordinate CA Certificate at issue).

3.2.6.1 Cross-Certification

Upon PMA approval, when cross-certification between an IdenTrust root with an external Certification Authority takes place, IdenTrust must inform End Entities of the uses allowed within the cross-certified PKI.

3.2.6.2 Verification and Validation of Information

Verification and validation of registration information shall consist of a comparison of registration information with trusted information, and an out-of-band confirmation process. The comparison may be performed electronically or through other trusted means (e.g., a manual review by an LRA after receiving a printout of the online application by mail).

The “trusted information” used for comparison for manual and automated electronic verification described in Section 3.2. Initial Identity Validation may consist of either

1. a database of user-supplied information previously compiled and maintained by IdenTrust or the RA based on an antecedent identification of and continuing relationship with the user;
2. information provided through third party vendors of such information; or
3. a Qualified Government Information Source or Qualified Government Tax Information Source.

Once a source is deemed to be within the acceptable parameters of accuracy and reliability it will be used for verification purposes.

The “out-of-band confirmation process” may consist of

1. delivery of a Shared Secret to a confirmed and trusted data point (e.g., street address, telephone number, or Email Address),
2. delivery in-person of a Shared Secret upon presentment of at least 2 acceptable forms of identification in accordance with Section 3.2.3.1,

3. use of a Shared Secret between the Individual identified in the application and the CA or RA pursuant to an antecedent identification and ongoing relationship,
4. presentation by the Applicant/PKI Sponsor during the application process of information that the CA or RA can be reasonably assured would be known only to the person identified in the application; or
5. another equivalent process.

Any documents received for the manual verification process will be inspected by IdenTrust for signs of alteration or falsification. The contents of the request will also need to be verified for quality and accuracy.

3.2.6.3 Validation of Email Address Authorization or Control

Email verification when required can be done in 2 ways; electronically and manually through a list submitted by a Trusted Agent. If the application for a Certificate requires email verification, the application cannot be approved until the specified steps for electronic or manual verification are complete.

IdenTrust verifies that Applicant controls the email accounts associated with TLS Certificates and that Email Address fields referenced in the Certificate have been authorized by the email account holder to act on the account holder's behalf.

IdenTrust does not delegate the verification of Email Addresses authorization or control. IdenTrust shall maintain a record of the validation method, including the relevant version number from the TLS BR that was used to validate every domain or Email Address in issued Certificates.

3.2.6.3.1 Electronic Verification of Email

3.2.6.3.1.1 Validating Control Over Email Address Via Email

Upon submission of an application via a secure online form, an automated email is dispatched to the specified Email Address provided within the application. Contained within this automated email is a link leading the Applicant/PKI Sponsor to a server-authenticated TLS secured website. Detailed within are instructions guiding the Applicant/PKI Sponsor to furnish a single-use email verification Random Value, which remains valid for a duration of 24 hours. Alongside this, the Account Password – created during the application process by the Applicant/PKI Sponsor – is required.

The Account Password, held exclusively by the Applicant/PKI Sponsor, and the Random Value shall remain valid for use in a confirming response for no more than 24 hours from its creation.

This act finalizes the verification process for the Email Address and subsequently triggers an automatic update of the verification status within the Applicant/PKI Sponsor's application record.

Should the allotted 24-hour window expire, rendering the Random Value void, a new Random Value shall be transmitted to the Applicant's Email Address, thereby rendering the previous Random Value invalid.

3.2.6.3.1.2 Manual Verification of Email

Enterprise RAs may furnish a list of authorized sponsored Applicants/PKI Sponsors. These Individuals have their Email Addresses verified by a Trusted Agent, drawing upon the internal insights of the Sponsoring Organization. The Trusted Agent employs internal databases and directories to ascertain the correctness of email information.

For server Domain validations, IdenTrust maintains a record of the TLS BR validation method used, including the relevant version number.

Completed validations of Applicant authority may be valid for the Issuance of multiple Certificates over time. In all cases, the validation is handled within the time period specified in Section 4.2.1 prior to Certificate Issuance.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

For End Entity Certificates, a request for Issuance of a new TrustID Certificate with a new Key Pair is available within 30 days before Certificate expiration.

For further information on the re-key process, see Section 4.7.

3.3.2 Identification and Authentication for Re-Key after Revocation

Revoked, or expired TrustID Certificates cannot be re-keyed, renewed, or updated. Applicants/PKI Sponsors without a valid TrustID Certificate will be re-authenticated by IdenTrust; or an LRA, Enterprise RA, or Trusted Agent, through a new TrustID Certificate application according to the corresponding Certificate based on Section 3.2, just as with an initial Applicant registration, and will be issued a new TrustID Certificate.

3.4 Identification and Authentication for Revocation Requests

The identity of the person submitting a Revocation Request in any other manner is authenticated in accordance with Section 4.9

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

A Certificate application may be submitted by various Individuals depending on the type of Certificate as described below:

- An Individual who is already a Subscriber of this type of Certificate.
- An Individual who is already a Subscriber, or who can fulfill the same requirements of a Subscriber though it does not obtain a human Certificate, and when appropriate, who has been authorized by the Sponsoring Organization to be the PKI Sponsor for the Device.

For EV Certificates IdenTrust may only issue to Applicants that meet the Private Organization, Government Entity, Business Entity and Non-Commercial Entity requirements as follows:

- Private Organization Subjects:
  1. The entity's legal existence is created or recognized by a by a filing with (or an act of) the Incorporating Agency or Registration Agency in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a certificate of incorporation, Registration Number, etc.) or created or recognized by a Government Agency (e.g. under a charter, treaty, convention, or equivalent recognition instrument);

2. The entity designated with the Incorporating or Registration Agency a Registered Agent, a Registered Office (as required under the laws of the Jurisdiction of Incorporation or Registration), or an equivalent facility;
3. The entity is not designated on the records of the Incorporating or Registration Agency by labels such as "inactive," "invalid," "not current," or the equivalent;
4. The entity has a verifiable physical existence and business presence;
5. The entity's Jurisdiction of Incorporation, Registration, charter, or license, and/or its Place of Business is not in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
6. The entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

- Government Entity Subjects:
  1. The entity's legal existence was established by the political subdivision in which the entity operates;
  2. The entity is not in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
  3. The entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.
- Business Entity Subjects:
  1. The entity is a legally recognized entity that filed certain forms with a Registration Agency in its jurisdiction, the Registration Agency issued or approved the entity's charter, certificate, or license, and the entity's existence can be verified with that Registration Agency;
  2. The entity has a verifiable physical existence and business presence;
  3. At least one Principal Individual associated with the entity is identified and validated by an Enterprise RA or an LRA of the RA identified in Section 1.3.2;
  4. The identified Principal Individual attests to the representations made in the Subscriber Agreement;
  5. IdenTrust verifies the entity's use of any assumed name used to represent the entity pursuant to the requirements of Section 3.2.2.3;
  6. The entity and the identified Principal Individual associated with the entity are not located or residing in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
  7. The entity and the identified Principal Individual associated with the entity are not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.
- Non-Commercial Entity Subjects:
  1. The Applicant is an International Organization entity, created under a charter, treaty, convention or equivalent instrument that was signed by, or on behalf of, more than one country's government; and
  2. The Applicant is not headquartered in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
  3. The Applicant is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

Subsidiary organizations or agencies of an entity that qualifies as a Non-Commercial Entity also qualifies for EV Certificates as a Non-Commercial Entity.

4.1.2 Enrollment Process and Responsibilities

Prior to the Issuance of a Certificate, IdenTrust obtains the following from the Applicant:

1. A Certificate Request;
2. An executed Subscriber Agreement and/or Terms of Use; and
3. Payment of any applicable fees

The Certificate Request and Subscriber Agreement or Terms of Use comply with Section 9.6.3. When applicable, IdenTrust obtain any additional documentation necessary to fulfill the Certificate Request.

One Certificate Request may suffice for multiple Certificates to be issued to the same Applicant, subject to the validation reuse periods described in Section 4.2.1, provided that each Certificate is supported by a valid, current Certificate Request signed by the appropriate Applicant Representative on behalf of the Applicant.

The Certificate Request contains a request from, or on behalf of, the Applicant for the Issuance of a Certificate, and a certification by, or on behalf of the Applicant that all of the information contained therein is correct.

IdenTrust may rely on a previously verified Certificate Request to issue a replacement Certificate if:

1. The previous Certificate being referenced was not revoked;
2. The expiration date of the replacement Certificate is the same as the previous Certificate being referenced; and
3. The Subject Information of the Certificate is the same as the previous Certificate being referenced.

IdenTrust has established enrollment processes that streamline the submission of registration information from the Applicant or PKI Sponsor. Submission options include:

- Direct entry via a dedicated website
- Bulk submission through a Trusted Agent
- Enterprise RA-facilitated bulk submission
- Secure forwarding by a RA to IdenTrust.

4.2 Certificate Application Processing

An Applicant/PKI Sponsor for a TrustID Certificate completes a TrustID Certificate application and provides requested information in a form prescribed by this CP-CPS.

Information in the Certificate application is verified as accurate before Certificates are issued as specified in Section 3.2.

4.2.1 Performing Identification and Authentication Functions

The Certificate Request may include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for the CA to obtain from the Applicant in order to comply with the TLS BR and this CP-CPS. In cases where the Certificate Request does not contain all the necessary information about the Applicant, the CA shall obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. IdenTrust shall establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

The Identity Proofing information for a Subscriber is collected and examined by IdenTrust, a Trusted Agent from the Organization sponsoring the Subscriber, Enterprise RA or an LRA of the RA identified in Section 1.3.2. Such information is verified according to the Identity Proofing processes described in Section 3.2 and Section 3.3.

Applicant information must include, but not be limited to, at least one Fully Qualified Domain Name or IP Address to be included in the Distinguished Name or Certificate's *subjectAltName* extension. If FQDN is only included in the *subjectAltName* extension, that extension must be marked as critical

The following Applicant roles are required for the issuance of an EV Certificate:

1. *Certificate Requester:* The EV Certificate request must be submitted by an authorized Certificate Requester.
2. *Certificate Approver:* The EV Certificate request must be approved by an authorized Certificate Approver.
3. *Contract Signer:* A Subscriber Agreement applicable to the requested EV Certificate must be signed by an authorized Contract Signer.
4. *Applicant Representative:* In the case where the CA and the Subscriber are affiliated, Terms of Use applicable to the requested EV Certificate must be acknowledged and agreed to by an authorized Applicant Representative.

The Applicant may authorize a single individual to hold multiple roles, and may also authorize multiple individuals to share any given role.

IdenTrust may use the documents and data provided in Section 3.2 to verify Certificate information or may re-use previous validations themselves provided that the data or document used in the prior validation is no more than the limits specified in Section 3.2

IdenTrust may reuse completed validations and/or supporting evidence performed in accordance with Section 3.2. Completed validation of organization identity in accordance with Section 3.2.2 shall be obtained no more than 825[2] days prior to issuing the Certificate. Validation of authority in accordance with Section 3.2.5 shall be obtained no more than 825[5] days prior to issuing the Certificate, unless a contract between the CA and the Applicant specifies a different term. For example, the contract may include the perpetual assignment of roles until revoked by the Applicant or CA, or until the contract expires or is terminated.

For validation of Domain Names and IP Addresses according to Section 3.2.2.4 and Section 3.2.2.5, any data, document, or completed validation used must be obtained within the maximum number of days prior to issuing the Certificate, as defined in the following table:

Domain Names and IP Addresses Data Reuse Periods

Certificate Issued on or After	Certificate Issued Before	Max Data Reuse Period
	March 15, 2026	398 days
March 15, 2026	March 15, 2027	200 days
March 15, 2027	March 15, 2029	100 days
March 15, 2029		10 days

[2] 398 days when issued on or after March 15, 2026.

4.2.1.1 CAA Checking

As part of the Server Certificate Issuance process, IdenTrust retrieves and process CAA records in accordance with RFC 8659 for each *dNSName* in the *subjectAltName* extension that does not contain an Onion Domain Name.

Some methods relied upon for validating the Applicant's ownership or control of the Subject Domain(s) (see Section 3.2.2.4) or IP address (see Section 3.2.2.5) to be listed in a Certificate require CAA records to be retrieved and processed from additional remote Network Perspectives before Certificate Issuance (see Section 3.2.2.9). To corroborate the Primary Network Perspective, a remote Network Perspective's CAA check response must be interpreted as permission to issue, regardless of whether the responses from both Perspectives are byte-for-byte identical. Additionally, IdenTrust may consider the response from a remote Network Perspective as corroborating if one or both of the Perspectives experience an acceptable CAA record lookup failure, as defined in this section.

When processing CAA records, IdenTrust process the issue, *issuewild*, and *iodef* property tags as specified in RFC 8659, although it is not required to act on the contents of the *iodef* property tag. Additional property tags may be supported but must not conflict with or supersede the mandatory property tags set out in this document. IdenTrust respects the critical flag and does not issue a Certificate if it encounters an unrecognized property tag with this flag set.

If Certificate Issuance takes place, it is done within the "TTL" field of the CAA record, or 8 hours, whichever is greater. This stipulation does not prevent IdenTrust from checking CAA records at any other time.

IdenTrust does not rely on any CAA record exception unless it is one of the following:

- CAA checking is optional for Certificates for which a Certificate Transparency Precertificate was created and logged in at least two public logs, and for which CAA was checked at time of Precertificate Issuance.
- CAA checking is optional for Certificates issued by a Technically Constrained Subordinate CA Certificate where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.

IdenTrust is permitted to treat a record lookup failure as permission to issue if:

- the failure is outside the IdenTrust's infrastructure; and
- the lookup has been retried at least once; and
- the domain's zone does not have a DNSSEC validation chain to the ICANN root.

IdenTrust documents potential Issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CA/Browser Forum on the circumstances and should dispatch reports of such Issuance requests to the contact(s) stipulated in the CAA *iodef* record(s), if present. CAs are not expected to support URL schemes in the *iodef* record other than mailto: or https:.

In case of failed CAA checking, the rejection transaction record will include:

- The FQDN(s) requested;
- Whether or not "identrust.com" or "www.identrust.com" were listed as one the trusted CA Domain Names in the CAA record; and
- Whether or not the Domain Name was on the denied or high-risk request lists.

For Enterprise RAs issuing server Certificates, this record will include the following information in

their rejection records:

- Applicant/PKI Sponsor's name as it appears in the Applicant/PKI Sponsor's request for a Certificate;
- Method of application (e.g., online, in-person, remote) for each data element accepted for proofing, including electronic forms;
- Source of verification (i.e., which databases used for cross-checks);
- Method of verification (e.g., online, in-person, remote);
- Date/time of verification;
- Fields that failed verification;
- All Identity Proofing data;
- Whether or not "identrust.com" or "www.identrust.com" were listed as one the trusted CA Domain Names in the CAA record; and
- Date/time of process completion.

4.2.1.2 Verification Against High Risk and Denied Request Lists

To ensure that requests for TrustID Certificates are properly verified, IdenTrust and RAs conduct 2 additional checks when necessary:

1. IdenTrust and RAs maintain internal lists of prior denied applications identified as posing a risk; and
2. IdenTrust and RAs will check high-risk domain requests against an authoritative third party list before Issuance.

Information returned from such checks is used during the application process by an LRA within IdenTrust or an RA when identifying potentially illegitimate Certificate Requests. If an RA is elected to perform verification processes, IdenTrust will verify that the RA's processes used to identify high-risk domain requests and prior denied requests provide a level of assurance that is equal to or exceeds the same level of assurance provided by the process described below.

- For OV Certificates, additional requirements as specified in Section 4.2.1; and
- For EV Certificates
  - **Verification Requirements:** IdenTrust verifies whether the Applicant, the Contract Signer, the Certificate Approver, the Applicant's Jurisdiction of Incorporation, Registration, or Place of Business:
    1. Is identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of the CA's jurisdiction(s) of operation; or
    2. Has its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of the CA's jurisdiction prohibit doing business.

    IdenTrust does not issue any EV Certificate to the Applicant if either the Applicant, the Contract Signer, or Certificate Approver or if the Applicant's Jurisdiction of Incorporation or Registration or Place of Business is on any such list.
  - **Acceptable Methods of Verification:** IdenTrust takes reasonable steps to verify with the following lists and regulations:

    US Government denied lists and regulations:
    1. BIS Denied Persons List
    2. BIS Denied Entities List
    3. US Treasury Department List of Specially Designated Nationals and Blocked Persons

4.2.1.3 High Risk Request Procedure

To prevent potential phishing, fraudulent use and to take further precautions against potential compromise, IdenTrust, and the RA maintains a list of prior high-risk requests and checks a third party authority list specifying current high-risk Domain Names. This list is used by LRAs to identify potential risks.

Should an LRA identify an application with any potential risk posed to IdenTrust or a Domain Name listed on the third party authority list, it will be flagged and brought to the attention of management to complete further internal verification. To prevent high-risk Issuance of a TrustID Certificate this internal verification will require one or more the following pieces of evidence:

- A Call to the Sponsoring Organization;
- Request further documentation from the Sponsoring Organization;
- Careful examination of the FQDN to confirm whether the intent of the Domain Registrant is to imitate or mislead customers of an FQDN on the high risk third party authority list to commit fraudulent or phishing activities (e.g., www.g00gle.com, www.1dentrust.com, etc.) and specific filters that are established at the System level to deny initial applications (e.g., non-US ASCII characters);
- Manual review of all documents and information provided; and/or
- Other verifiable proof as deemed necessary by RA or IdenTrust management.

4.2.1.4 Denied Request Procedure

TrustID Certificate applications that cannot pass this review will not be issued a TrustID Certificate. If the Certificate does not pass review, it will be added to a list of previously denied applications and kept for verification purposes of future TrustID Certificate applications.

4.2.2 Approval or Rejection of Certificate Applications

CAs shall not Issue Certificates containing Internal Names or Reserved IP Addresses, as such names cannot be validated according to Section 3.2.2.4 or Section 3.2.2.5. IdenTrust and RAs approve an Applicant/PKI Sponsor Certificate application if the Identity Proofing processes described in Section 3.2 and Section 3.3 are completed successfully.

IdenTrust does not Issue Certificates for Reserved IP Addresses, or internal server names and will not issue them for the gTLD domains not approved on these grounds.

Effective March 15, 2026, IdenTrust does not issue Certificates containing Domain Names that end in an IP Address Reverse Zone Suffix.

4.2.2.1 Final Cross-Correlation and Due Diligence

Enterprise RAs may perform the cross-correlation and due diligence for EV Certificates following the requirements of Section 1.3.2.1.

4.2.3 Time to Process Certificate Applications

For server Certificates, where the CAA record is found and it lists an explicit Issuing CA name or CA Domain Name, as the Issuing CA, the Issuance must be done within the time specified in the "*TTL*" field of the CAA record, or 8 hours, whichever is greater.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

4.3.1.1 Manual Authorization of Certificate Issuance for Root CAs

Certificate Issuance by the Root CA shall require an Individual authorized by the CA (i.e., the CA Infrastructure System operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a Certificate signing operation.

4.3.1.2 Linting of To-Be-Signed Certificate Content

IdenTrust has a technical control to verify that the to-be-signed Certificate corresponds to the to-be-signed Precertificate in the manner described in Section 3.2 of RFC 6962.

Methods used to produce a Certificate containing the to-be-signed Certificate content include, but are not limited to:

1. Sign the *tbsCertificate* with a "dummy" Private Key whose Public Key component is not certified by a Certificate that chains to a Publicly-Trusted CA Certificate; or
2. Specify a static value for the signature field of the Certificate ASN.1 SEQUENCE.

IdenTrust may implement its own Certificate Linting tools, but IdenTrust will use the Linting tools that have been widely adopted by the industry (see https://cabforum.org/resources/tools/).

4.3.1.3 Linting of Issued Certificates

IdenTrust may use a Linting process to test each issued Certificate.

4.3.1.4 Issuance Via Secure Website for Server Certificates

For each Certificate Issuance to an Applicant/PKI Sponsor or Subscriber, the following occurs during the same server-authenticated SSL/TLS session:

1. The Applicant/PKI Sponsor/Subscriber initiates the Certificate retrieval by accessing via a browser a URL (retrieval URL) provided by IdenTrust or the RA. In the resulting web session, the IdenTrust CA or RA Infrastructure System authenticates itself to the Subscriber and encrypts all communication utilizing a server-authenticated SSL/TLS encrypted channel verifiable by a Certificate issued by a distinct IdenTrust Certificate Authority natively trusted in browsers.
2. The Applicant/PKI Sponsor /Subscriber authenticates himself or herself to the web server used in the retrieval process by supplying the Activation Code delivered by IdenTrust or the RA together with the Account Password selected by the Applicant/ PKI Sponsor /Subscriber during the application process described in Section 4.1. This 2-factor authentication is required for all Certificate retrievals by an Applicant/PKI Sponsor /Subscriber from IdenTrust.

The PKI Sponsor generates the Key Pair for the Electronic Device and submits the *PKCS#10* Certificate Request as an initial step during registration. The process will also verify the Public Key of an Electronic Device that is requested has less than 2048-bit encryption and if it uses a known weak Private Key. If either or both are automatically detected in the secure session, the PKI Sponsor will be required to correct the determined issue before the server Certificate can be issued.

The Certificate Issuance process described in this section will ensure compliance with this CP-CPS:

1. IdenTrust has verified the source of the Certificate Request.
2. IdenTrust has confirmed the authenticity and authority of the source of information contained within the Subscriber's Certificates.
3. IdenTrust has built and signed the Subscriber's Certificates in a secure manner.
4. IdenTrust has delivered the Subscriber's Certificates, the necessary Subordinate CA, and Root CA Certificates to the Subscriber.
5. IdenTrust has published the Subscriber's Certificates to IdenTrust's Repository.

Upon Issuance of a TrustID Certificate, IdenTrust warrants to all Program Participants that:

1. Upon receiving a request for a Certificate, IdenTrust has managed the TrustID Certificate in accordance with these requirements;
2. IdenTrust has complied with all requirements in this CP-CPS when identifying the Subscriber and issuing the TrustID Certificate;
3. There are no misrepresentations of fact in the TrustID Certificate known to IdenTrust and IdenTrust has verified the information in the TrustID Certificate in accordance with Section 3.2;
4. Information provided by the Subscriber for inclusion in the TrustID Certificate has been accurately transcribed to the TrustID Certificate; and
5. The TrustID Certificate meets the material requirements of this CP-CPS.

For server Certificates, the Issuance of a Certificate verifies:

1. The PKI Sponsor has the right to use the Domain Name(s) at the time of application and Identity Proofing;
2. The PKI Sponsor was authorized to obtain that Certificate from the Domain Name administrator at the time of application and Identity Proofing;
3. The information included on the Certificate is accurate at the time of application and Identity Proofing;
4. The information included on the Certificate is not misleading;
5. The identity of the PKI Sponsor has been verified according to these Identity Proofing processes described in Section 3.2;
6. The PKI Sponsor has signed and is bound by the Subscriber Agreement;
7. IdenTrust will maintain a publicly accessible Repository for verification of the status of the server Certificate; and
8. IdenTrust will revoke the server Certificate for any of the reasons listed in Section 4.9.1.1.

These warranties are articulated in the Subscriber Agreement provided to the Applicant/PKI Sponsor/Subscriber during the registration process.

Alternative methods for the Issuance of Certificates are not implemented at this time.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

If Certificates are delivered to the Subscriber during an in-person session, no notification is required. Otherwise, Certificate retrieval links are sent to the Email Address provided by the Subscriber during the Certificate Application process.

When requested via ACME, Subscriber Certificates are made available to Subscribers via the ACME protocol as soon after issuance as reasonably possible.

4.4 Certificate Acceptance

At the time of application for a Certificate, Enterprise RA, IdenTrust, or the RA requires the Applicant/PKI Sponsor to sign the Subscriber Agreement. The Subscriber Agreement calls for the Subscriber to perform his responsibilities under this section in applying for, reviewing, and using the Certificate. The Subscriber is also required to request Revocation when appropriate.

4.4.1 Conduct Constituting Certificate Acceptance

Upon Issuance and installation of the TrustID Certificate, Subscribers are provided with the contents of the Certificate in a human-readable form for their review. IdenTrust requires the Subscriber to review the Certificate and affirmatively communicate Acceptance of its content at the end of the retrieval process. IdenTrust records the act of the Acceptance of the TrustID Certificate in accordance with Section 5.5.1.

By accepting a TrustID Certificate, the Subscriber warrants that all of the information provided by the Applicant/PKI Sponsor (and by its Sponsoring Organization, where applicable) and included in the TrustID Certificate, and all representations made by the Subscriber (and by its Sponsoring Organization, where applicable) as part of the application and Identity Proofing process, are true and not misleading.

4.4.2 Publication of the Certificate by the CA

Pursuant to Section 2.1, IdenTrust TrustID Certificates are published in the Repository upon Issuance. The Repository is publicly available.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Notification of Certificate Issuance to others is effectuated by the publication of the TrustID Certificate in a recognized Repository.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers who receive Certificates from the IdenTrust CA assert that they will comply with the TLS BR as well as those in this CP-CPS by either signing the Subscriber Agreement online or in paper copy; or, by undergoing a full registration process before receiving the Certificate. Additional information concerning the rights and obligations of Subscribers may be found in Section 9.6.3.

Key Usage is described in Section 6.1.7.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to Accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for each application and is not controlled by this CP-CPS. Relying Parties who rely on stale CRLs do so at their own risk. See Section 4.8.7.

Parties who rely upon the Certificates issued under this CP-CPS should preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the Digital Signatures on that data for as long as it may be necessary to verify the signature on that data.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

A Certificate may be renewed if the Key Pair has not reached the end of its validity, the Private Key has not been compromised, and the End Entity name and attributes are correct.

IdenTrust or the RA will send the Subscriber notice of pending Certificate expiration, in the form of a re-key/renewal notification, at least in 30-day intervals beginning 90 days before the expiration date of the Subscriber's Certificate. Renewal is allowed within 30 days of Certificate expiration.

Upon renewal, the remaining period of the Certificate being renewed is added to the new Certificate providing that the new Validity Period does not exceed the maximum allowed for the Certificate type.

4.6.2 Who May Request Renewal

Only the End Entity may request Certificate renewal.

4.6.3 Processing Certificate Renewal Requests

Renewal of a TrustID Certificate for a PKI Sponsor requires that the affiliation between the PKI Sponsor and their Sponsoring Organization is still valid at the time of renewal.

4.6.4 Notification of New Certificate Issuance to Subscriber

The notification procedures used by the IdenTrust or RA's are the same as with a new End Entity request.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Upon renewal and installation of the Certificate, Subscribers are to be provided with the contents of the Certificate in a human-readable form for their review. The Issuing CA should require that the Subscriber review the Certificate and affirmatively communicate Acceptance of its content at the end of the retrieval process. The Issuing CA records the act of the Acceptance of the TrustID Certificate in accordance with Section 5.5.1.

4.6.6 Publication of the Renewal Certificate by the CA

The Issuing CA's Certificates are to be published in a publicly available Repository.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No other entities are notified of Certificate Issuance by the CA.

4.7 Certificate Re-Key

Re-keying a Certificate consists of creating a new Certificate with a different Public Key (and serial number) while retaining the remaining content of the old Certificate that describes the Subject and assigning a new Validity Period to such Certificate. The new Certificate may be assigned different Key identifiers, specify a different CRL distribution point, and/or be signed with a different Key.

When IdenTrust updates the Key Pairs and Certificates for the Root CA Certificates are made available publicly via the Repository, which is disclosed in the End Entity and Subordinate CA Certificates themselves.

The Subject name in a Certificate that has been re-keyed does not change and the old Certificate need not be revoked since it does not violate the requirement for name uniqueness.

In addition, after Certificate re-key, the old Certificate is not revoked by IdenTrust, and the Subscriber may or may not revoke it. In any case, the System automatically prevents the Certificate to be re-keyed again, renewed, or modified.

4.7.1 Circumstance for Certificate Re-Key

Subscribers should plan on re-keying well in advance of the time when the period of validity of a Key Pair or Certificate described in Section 6.3.2 is scheduled to expire. Certificates will be re-keyed to the same period of validity as the original Certificate. Creating a new Key Pair and obtaining a new Certificate prevents a disruption in signing activities that would be caused if the Certificate were allowed to expire before attempting to re-key.

4.7.2 Who May Request Certification of a New Public Key

The original Subscribers are also entitled to request its re-key (See Section 3.3.1).

4.7.3 Processing Certificate Re-Keying Requests

For server Certificates, 30 days before the expiration period, the IdenTrust or the RA's system may automatically notify the Subscriber that he or she must request a Re-key and re-establish identity by presenting his or her valid TrustID Certificate.

IdenTrust will authenticate the Subscriber by using the Identity Proofing processes required for the corresponding Certificate in Section 3.2. Once the Subscriber is authenticated, IdenTrust will then follow the TrustID Certificate Issuance process described in Section 4.4.

4.7.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See Section 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

See Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

IdenTrust allows the modification of only Valid Certificates (i.e., Certificate is neither revoked nor expired). The new Certificate, with a new Key Pair, is issued with the same expiration date as the original Certificate.

In the case of Certificate replacement IdenTrust allows the replacement of Certificates when the Subscriber's Private Key has not been compromised and there are no changes to the Certificate. Note that in the case where a non-escrowed Private Key is lost or damaged, the Certificate cannot

be replaced or recovered and the identity of the Subscriber must be established through the initial registration process described in Section 3.2.

For server Certificate modification, PKI Sponsors may submit modification requests for adding, removing, and modifying the contents of the SAN including the FQDN(s). These types of additions that have not been verified will need to be established through the initial registration process described in Section 3.2 to complete the modification.

A Root and Subordinate CAs Certificates may be modified if approved in writing by the IdenTrust PMA.

4.8.2 Who May Request Certificate Modification

Subscribers with Valid Certificates are entitled to request email modification and replacements. See Section 3.2.3 and Section 4.1.1 for specific details.

4.8.3 Processing Certificate Modification Requests

Upon receiving an authenticated request from an authorized official of a Business Entity to add or remove FQDN(s), or to replace a lost or damaged Certificate for a business representative Subscriber, IdenTrust will issue a replacement Certificate and records the following Certificate replacement transaction data:

1. Certificate serial number;
2. Certificate common name;
3. Subject Alternative name;
4. Certificate Policy OID;
5. Date/time of completion of replacement process; and
6. All associated replacement data.

Modification of a Root CA Certificate or Subordinate CA Certificate requires that a request is made in writing to the IdenTrust PMA, to address interoperability concerns. Proposals to modify CA Certificates are processed as follows:

A survey of the applications deployed in the PKI and an analysis of whether the proposed modification creates interoperability concerns are performed. Any concerns raised by any PMA member or other designated relevant third party should be addressed by the IdenTrust Operations group. When there are no remaining concerns, the Root or Subordinate CA Certificate with the requested modifications is issued. The old CA Certificate will not be revoked unless all issues related to the transition from the old CA Certificate to the new CA Certificate have been resolved.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

See Section 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.6.7.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking Subscriber Certificates

IdenTrust may support Revocation of Short-lived Subscriber Certificates.

With the exception of Short-lived Subscriber Certificates, IdenTrust will revoke a Subscriber Certificate individually within 24 hours and use the corresponding *CRLReason* (See Section 7.2.2) if one or more of the following occurs:

1. The Subscriber requests in writing, without specifying a *CRLReason*, that IdenTrust revoke the Certificate (*CRLReason* "unspecified (0)" which results in no *reasonCode* extension being provided in the CRL);
2. The Subscriber notifies IdenTrust that the original Certificate Request was not authorized and does not retroactively grant authorization (*CRLReason* #9, *privilegeWithdrawn*);
3. IdenTrust obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (*CRLReason* #1, *keyCompromise*);
4. IdenTrust is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate, including but not limited to those identified in Section 6.1.1.3 (5) (*CRLReason* #1, keyCompromise);
5. IdenTrust obtains evidence that the validation of domain authorization or control for any Fully Qualified Domain Name or IP Address in the Certificate should not be relied upon (*CRLReason* #4, *superseded*).

With the exception of Short-lived Subscriber Certificates, IdenTrust should revoke a Subscriber Certificate within 24 hours and must revoke a Subscriber Certificate within 5 days and use the corresponding *CRLReason* (See Section 7.2.2) if one or more of the following occurs:

6. The Certificate no longer complies with the requirements in the relevant section of the TLS BR (*CRLReason* #4, superseded);
7. IdenTrust obtains evidence that the Certificate was misused (*CRLReason* #9, *privilegeWithdrawn*);
8. IdenTrust is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use (*CRLReason* #9, *privilegeWithdrawn*);
9. IdenTrust is made aware of any circumstance indicating that use of a FQDN or IP Address in the Certificate is no longer legally permitted (e.g. 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) (*CRLReason* #5, *CessationOfOperation*);
10. IdenTrust is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully Qualified Domain Name (*CRLReason* #9, privilegeWithdrawn);
11. IdenTrust is made aware of a material change in the information contained in the Certificate (*CRLReason* #9, *privilegeWithdrawn*);
12. IdenTrust is made aware that the Certificate was not issued in accordance with the TLS BR or the CA's Certificate Policy or Certification Practice Statement (*CRLReason* #4, superseded);
13. IdenTrust determines or is made aware that any of the information appearing in the Certificate is inaccurate (*CRLReason* #9, *privilegeWithdrawn*);
14. IdenTrust's right to Issue Certificates under the TLS BR expires or is revoked or terminated,

unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository (*CRLReason* "*unspecified* (0)" which results in no *reasonCode* extension being provided in the CRL);

15. Revocation is required by IdenTrust's Certificate Policy and/or Certification Practices Statement (*CRLReason* "*unspecified* (0)" which results in no *reasonCode* extension being provided in the CRL); or
16. IdenTrust is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (*CRLReason* #1, keyCompromise).

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

IdenTrust will revoke a Subordinate CA Certificate within 7 days if one or more of the following occurs:

1. The Subordinate CA requests Revocation in writing;
2. The Subordinate CA notifies IdenTrust that the original Certificate Request was not authorized and does not retroactively grant authorization;
3. IdenTrust obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
4. IdenTrust obtains evidence that the CA Certificate was misused;
5. IdenTrust confirms that the CA Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6. IdenTrust determines that any of the information appearing in the CA Certificate is inaccurate or misleading;
7. IdenTrust or the Subordinate CA ceases operations for any reason and has not arranged for another CA to provide Revocation support for the CA Certificate;
8. IdenTrust or the Subordinate CA's right to Issue Certificates under the TLS BR expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by IdenTrust's Certificate Policy and/or Certification Practice Statement; or
10. The technical content or format of the CA Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

4.9.2 Who Can Request Revocation

Different parties may request Certificate Revocation as follows:

- The Issuing CA may summarily revoke Certificates within its domain.
- An RA can request the Revocation of an End Entity's TrustID Certificate on behalf of the End Entity, the Sponsoring Organization, or other authorized party, or on its behalf.
- An End Entity is authorized to request the Revocation of his, her, or its Certificate, as is a Subscriber's Sponsoring Organization.
- When issued via ACME, Subscribers may request Certificate revocation either with the ACME 'account key" or with the Certificate's Private Key via the ACME Protocol's revocation interface as defined in Section 7.6 of RFC 8555.
- Additionally, Subscribers, Authorized Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the Issuing CA of

reasonable cause to revoke the Certificate. See Section 4.9.3. below.

In any case, notice should be provided to the Subscriber promptly after Revocation.

4.9.3 Procedure for Revocation Request

IdenTrust provides a process for Subscribers to request Revocation of their own Certificates as described in Section 1.5.3.

When the Private Key of a Subscriber's Certificate to be revoked is available, it may be revoked by sending Revocation that has a Digital Signature to the LRA, Trusted Agent, or Enterprise RA, establishing a Client-Authenticated SSL/TLS Encrypted Session with the RA or CA Infrastructure System.

If the Private Key is unavailable, Revocation can be initiated by contacting an LRA, Enterprise RA, or a Trusted Agent and completing an Identity Proofing process as described in Section 3.2.3. Revocation requests made via the ACME API are processed automatically. A Certificate will be revoked if the request meets any of the following criteria:

- It is signed with the private key corresponding to the certificate;
- It is signed with the account key of the Subscriber who originally requested the certificate; or
- It is signed with the account key of a Subscriber who has demonstrated control over all Subject Alternative Names listed in the Certificate.

See Section 1.5.2.1 for guidelines on reporting Certificate issues that may require Revocation.

The Subscriber or the PKI Sponsor is required to indicate the reason for the Revocation request as listed on Section 7.2.2.

4.9.4 Revocation Request Grace Period

There is no grace period for a TrustID Revocation request. All Participants are required to communicate a Certificate Revocation request as soon as it comes to their attention.

4.9.5 Time Within Which CA Must Process the Revocation Request

IdenTrust maintains a continuous 24x7 ability to communicate with Anti-Malware Organizations, Application Software Suppliers, and law enforcement agencies and respond to high-priority Certificate Problem Reports, such as reports requesting Revocation of Certificates used to sign malicious code, fraud, or other illegal conduct.

IdenTrust acknowledge receipt of plausible notices about Key Compromise signed with a Certificate issued IdenTrust or by an IdenTrust Subordinate CA.

Within 24 hours after receiving a Certificate Problem Report, IdenTrust will investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, IdenTrust will work with the Subscriber and any entity reporting the Certificate Problem Report or other Revocation-related notice to establish whether or not the Certificate will be revoked, and if so, a date on which IdenTrust will revoke the Certificate. The period from receipt of the Certificate Problem Report or Revocation-related notice to published Revocation must not exceed the time frame set forth in Section 4.9.1.1. The date selected by IdenTrust should consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm, adware, spyware, malware, software bug, etc.);
2. The consequences of Revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official should be addressed with higher priority); and
5. The relevant legislation.

4.9.6 Revocation Checking Requirements for Relying Parties

Following Certificate Issuance, a Certificate may be revoked for reasons stated in Section 4.9. Therefore, relying parties should check the Revocation status of all Certificates that contain a CDP or OCSP pointer.

Backdating the Revocation Date field is an exception to best practice described in Section 5.3.2 of RFC 5280; however, these Requirements specify the use of the Revocation Date field to convey the "invalidity date" to support Application Software Supplier software implementations that process the Revocation Date field as the date when the Certificate is first considered to be invalid.

4.9.7 CRL Issuance Frequency

CRLs must be available via a publicly-accessible HTTP URL (i.e., "published").

Within twenty-four (24) hours of issuing its first Certificate, the Issuing CA generate and publish either:

- a full and complete CRL; OR
- partitioned (i.e., "sharded") CRLs that, when aggregated, represent the equivalent of a full and complete CRL.

For the status of Subscriber Certificates, IdenTrust:

1. Update and publish a new CRL at least every:
   - seven (7) days if all Certificates include an Authority Information Access extension with an *id-ad-ocsp accessMethod* ("AIA OCSP pointer"); or
   - four (4) days in all other cases;
2. Update and publish a new CRL within twenty-four (24) hours after recording a Certificate as revoked.

For the status of CA Certificates, IdenTrust:

1. Update and publish a new CRL at least every twelve (12) months;
2. Update and publish a new CRL within twenty-four (24) hours after recording a Certificate as revoked.

IdenTrust will continue issuing CRLs until one of the following is true:

1. all Subordinate CA Certificates containing the same Subject Public Key are expired; or
2. the corresponding Subordinate CA Private Key is destroyed.

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9 Online Revocation/Status Checking Availability

When provided, OCSP responses shall conform to RFC 6960 and/or RFC 5019.

A Certificate serial is "assigned" if:

- a Certificate or Precertificate with that serial number has been issued by the Issuing CA; or
- a Precertificate with that serial number has been issued by a Precertificate Signing Certificate, as defined in Section 7.1.2.4 of the TLS BR, associated with the Issuing CA.

A Certificate serial is "unassigned" if it is not "assigned."

The following shall apply for communicating the status of Certificates and Precertificates which include an Authority Information Access extension with an *id-ad-ocsp accessMethod*.

OCSP Responders operated by IdenTrust support the HTTP GET method, as described in RFC 6960 and/or RFC 5019. IdenTrust may process the Nonce extension (1.3.6.1.5.5.7.48.1.2) in accordance with RFC 8954.

For the status of a Subscriber Certificate or its corresponding Precertificate:

- An authoritative OCSP response must be available (i.e., the responder must not respond with the "unknown" status) starting no more than 15 minutes after the Certificate or Precertificate is first published or otherwise made available.
- For OCSP responses with validity intervals less than sixteen hours, the IdenTrust shall provide an updated OCSP response prior to one-half of the Validity Period before the nextUpdate.
- For OCSP responses with validity intervals greater than or equal to sixteen hours, IdenTrust shall provide an updated OCSP response at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For the status of a Subordinate CA Certificate, IdenTrust shall provide an updated OCSP response at least every twelve months, and within 24 hours after revoking the Certificate.

The following shall apply for communicating the status of all Certificates for which an OCSP Responder is willing or required to respond.

OCSP responses must conform to RFC 6960 and/or RFC 5019. OCSP responses must either:

1. be signed by the IdenTrust CA that issued the Certificates whose Revocation status is being checked, or
2. be signed by an OCSP Responder which complies with the OCSP Responder Certificate Profile described in Section 7.1.2.4.

OCSP responses for Subscriber Certificates must have a validity interval greater than or equal to eight hours and less than or equal to ten days.

If the OCSP Responder receives a request for the status of a Certificate serial number that is "unassigned," then the responder should not respond with a "good" status.

4.9.10 Online Revocation Checking Requirements

IdenTrust supports an OCSP capability using the HTTP GET method as described in RFC 6960 and/or RFC 5019.

For the status of Subscriber Certificates:

1. OCSP responses have a validity interval greater than or equal to 8 hours;
2. OCSP responses have a validity interval less than or equal to 10 days;
3. For OCSP responses with validity intervals less than 16 hours, then the IdenTrust CA will update the information provided via an Online Certificate Status Protocol prior to one-half of the Validity Period before the *nextUpdate*; and
4. For OCSP responses with validity intervals greater than or equal to 16 hours, then the IdenTrust CA will update the information provided via an Online Certificate Status Protocol at least 8 hours prior to the *nextUpdate*, and no later than 4 days after the *thisUpdate*.

For the status of Subordinate CA Certificates, the IdenTrust CA will update information provided via OCSP:

1. At least every 12 months; and
2. Within 24 hours after revoking a Subordinate CA Certificate

If the OCSP Responder receives a request for the status of a Certificate serial number that is "unused", then the responder will not respond with a "good" status. If the OCSP Responder is for a CA that is not Technically Constrained in line with Section 7.1.5, the responder will not respond with a "good" status for such requests.

A Certificate serial number within an OCSP request is "assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous Key associated with that CA Subject, or "unused" if otherwise.

4.9.11 Other Forms of Revocation Advertisements Available

Upon explicit request, IdenTrust supports other methods for obtaining Certificate status information than those described in Section 4.8.7 in cases of

- IdenTrust mis-issued the Certificate,
- there is a suspected or actual compromise of the Applicant's or CA's Private Key.

IdenTrust reserves the right to make other forms of Revocation advertisement available to Relying Parties.

4.9.12 Special Requirements for Re-Key Compromise

When either an Issuing CA's or External CA's (i.e., Subordinate or Root) Certificate or Subscriber's Certificate is revoked because of compromise, or suspected compromise, of a Private Key, a CRL will be issued as soon as possible. See Section 4.9.1 Circumstances for Revocation.

Reports of Key Compromise to IdenTrust must include proof of Key Compromise in one of the following formats:

1. A Certificate signed request (CSR) with the CN "Proof of Key Compromise for IdenTrust," signed by the compromised Private Key, or
2. The compromised Private Key itself

Practices followed in the case of a CA Private Key compromised are explained in Section 5.7.3. Practices followed in the case of a Subscriber's Private Key compromised are explained in Section 4.9.3.

4.9.13 Circumstances for Suspension

Suspension is not available for any Certificate and the Repository must not include these Certificate types in a suspended state. See the Revoked Certificates Component table in Section 7.2.2.

4.9.14 Who Can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

Certificate suspension is not available.

4.9.16 Limits on Suspension Period

Certificate suspension is not available.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Revocation entries on the CRL or OCSP Response are only removed until after the expiry date of a revoked Certificate.

4.10.2 Service Availability

IdenTrust operates and maintains CRL and optional OCSP capability with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

IdenTrust Root CA Certificates, CRLs, and online TrustID Certificate status information are available for retrieval 24 hours a day, seven days a week, with a minimum of 99% availability overall per year, and scheduled downtime does not exceed 0.5% annually, excluding network outages.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

A Subscriber may terminate its subscription to Certificate services by allowing the term of a Certificate to expire without re-key.

Subscribers may also voluntarily revoke their Certificate as explained in Section 4.9.3. If a Subscriber terminates its Subscription during a Certificate's Validity Period, the Certificate is revoked.

Before the end of a subscription, IdenTrust or the RA will send the Subscriber notice of pending Certificate expiration, in the form of a re-key/renewal notification, at least in 30-day intervals beginning 90 days before the expiration date of the Subscriber's Certificate.

Renewal is allowed within 30 days of Certificate expiration.

Upon renewal, the remaining period of the Certificate being renewed is added to the new Certificate providing that the new Validity Period does not exceed the maximum allowed for the Certificate type.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

IdenTrust does not provide Key Escrow/Recovery for Server Certificates.

4.12.1.1 Circumstances for Private Key Recovery

IdenTrust does not currently support Key escrow or recovery using Key encapsulation techniques.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

IdenTrust developed, implements and maintains a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
5. Comply with all other security requirements applicable to the CA by law.

The Certificate Management Process shall include:

1. Physical security and environmental controls;
2. System integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
3. Network security and firewall management, including port restrictions and IP Address filtering;
4. User management, separate trusted-role assignments, education, awareness, and training; and
5. Logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

The IdenTrust CA Security Management Process must include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Based on the Risk Assessment, IdenTrust develops, implements, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes.

The security plan also takes into account then-available technology and the cost of implementing the specific measures and shall implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1 IdenTrust Physical Security Controls

5.1.1 Site Location and Construction

The construction and location of the building housing the IdenTrust CA Infrastructure System have been designed to offer security protection mechanisms consistent with facilities used to house high-value, sensitive information.

The IdenTrust CA Infrastructure System is housed in an unmarked secure data center, the perimeter of which is completely enclosed by fencing and access-controlled through a programmable electronic badging system. In addition, the perimeter of the building is secured with continuous surveillance cameras and intrusion sensors monitored 24x7x365. These measures provide high-risk protection. For disaster recovery, a second facility in a geographically diverse location provides similar protections. Physical security controls protecting the certification platform and Cryptographic Modules are described in the remainder of this section and apply to both sites. These physical security controls are intended as protection against intentional damage, theft, loss, and unauthorized use.

5.1.2 Physical Access

IdenTrust provides physical access controls designed to provide protection against unauthorized access to its CA Infrastructure System resources.

The building is located on fenced and video surveilled grounds. The Building entryways and passageways are also under continuous recorded video surveillance. The facility is actively monitored 24x7x365.

5.1.3 Power and Air Conditioning

The facility housing the IdenTrust CA, CSA, RAs, and Repositories equipment is supplied with air conditioning and power that is sufficient to provide a reliable operating environment.

Air conditioning is supplied by similarly redundant and separate Systems so that if one System fails, the building can be switched quickly to the other one.

5.1.4 Water Exposures

IdenTrust Systems are maintained in a facility which provides protection against water exposure and is constructed to Class-4 seismic standards.

5.1.5 Fire Prevention and Protection

The facility housing the IdenTrust CA, RAs, and Repositories equipment provide fire prevention and protection in accordance with local code. The facility is equipped with advanced fire response equipment including:

- Fire-resistant and fire-retardant construction materials;
- Advanced chemical, smoke, and heat-based detection systems;
- Fire suppression systems; and
- The building has a full complement of sensors that automatically alert both building staff and fire authorities if smoke is detected.

In addition, computer rooms (such as the Secure Room where CA, RAs, and Repositories Systems are housed) are equipped with riot doors, fire doors, and other doors resistant to forcible entry.

5.1.6 Media Storage

IdenTrust adheres to a "clean desk" Policy under which all hardcopy sensitive information is locked in file cabinets, desks, safes, or other furniture when it is not in use.

Access to storage safes located inside the IdenTrust Secure Room is controlled through Separation of Duties and Multi-Party Control. The safes have dual locks and require 2 Trusted Role employees for access; no Individual has the tools or information necessary to open a safe alone. All access to material inside the safes is documented through access logs. Any material placed into or removed from a safe is logged and signed for by 2 Trusted Role employees.

Server-based computer media containing sensitive materials is stored both within the Secure Room as described in Section 5.1.2, and at an offsite location, as described below.

The storage vault is a hardened site consisting of a tunnel bored into a solid granite mountain. Environment-related storage mechanisms include but are not limited to constant temperature and humidity, air circulation and filtration, prohibited storage of flammable items, ionization detectors, fire extinguishers, and independent power sources. The entrance is protected by multiple levels of security including gates, mantraps, and a 12,000-pound vault door.

There is only one point of ingress and egress for the facility and for the vault proper. Any attempt to use explosives to force the gates and vault door would be detected by heat detectors and seismic sensors that are connected to an alarm system. Card readers and/or sign-in logs are also utilized for physical access control and auditing.

An armed security force supports the vault. It is also under 24-hour electronic surveillance, and it is regularly patrolled by local law enforcement when not occupied. An armed guard escorts all persons entering the facility and the vault area. All access to the vault requires 24-hour advance notice.

Records are maintained in a temperature and humidity-controlled environment and the vault meets or exceeds all federal requirements for archival storage.

5.1.7 Waste Disposal

IdenTrust Policy prohibits any media from leaving organizational control that does contain or has contained sensitive data. Such media is destroyed as described below when it reaches end-of-life.

After it is no longer needed, all sensitive information is securely destroyed using procedures that are approved by the Security Office and are consistent with US federal regulations and guidelines. Employees are prohibited from destroying or disposing of potentially important records or information without specific management approval in advance.

All outdated or unnecessary copies of printed sensitive information are disposed of in a secure waste receptacle that is shredded onsite by a bonded company that specializes in disposing of sensitive information, under the direct observation of an IdenTrust Trusted Role employee.

Cryptographic Modules remain in locked safes within the Secure Room; sensitive backup tapes remain in the offsite secure location's vault before destruction. All Cryptographic Modules are zeroized after the Keys on them are no longer needed. If zeroization procedures fail, then they are physically destroyed. Destruction techniques vary depending on the medium in question.

5.1.8 Off-Site Backup

The IdenTrust CA Infrastructure System is backed up at the secured facility, using specialized backup software, to a local backup server. These System backups provide the capability to recover from a System failure. Incremental backups are performed daily. Full System backups are performed every week. Incremental and full backups are stored securely offsite: incremental backups are transported electronically to the disaster recovery site, and full backups are sent to the hardened, secure offsite storage vault described in Section 5.1.6 at least weekly.

5.2 Procedural Controls

5.2.1 Trusted Roles

All employees, contractors, and consultants of IdenTrust and RAs who have access to or control over cryptographic operations that may materially affect the Issuance, use, or Revocation of TrustID Certificates, including access to restricted operations of IdenTrust's CA and RA Systems, and Repository are for purposes of this CP-CPS, considered as serving in Trusted Roles. Such personnel include but are not limited to Administrators, Officers, Auditors, and Operators who oversee CA or RA operations.

IdenTrust Trusted Role personnel are appointed via "Trusted Role Appointment Letters" and are made aware to follow up on alerts of possible Critical Security Events and other security requirements.

Specifically, the generic roles in this CP-CPS translate into specific roles for the CA and RA, which include, but are not limited to:

- CA Administrator;
- RA Administrator;
- Quality Assurance Personnel;
- Local Registration Agent (LRA);
- System Administrator;
- Network Engineer;
- Security Officer;
- Software Engineer;
- Development Operations (DevOps);
- Customer Support Representative; and
- Operations Management Personnel.

The functions and duties performed by these persons are also separated and distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI. See Section 5.2.4.

5.2.1.1 CA Administrator

The CA Administrator's responsibilities and operating procedures, as they relate to CA Operations, are as follows:

- Installation, configuration, and maintenance of the CA software;
- Establishing and maintaining system accounts and configuring audit parameters;
- Installation and configuration of Repository software;
- Installation and configuration of the RA software (Internal RA only);
- Configuration of CRL parameters;

- Configuration of Certificate Profiles;
- Cross-Certified Subordinate CA Certificate, Root CA Certificate, and Subordinate CA Certificate Key management (performed under 2-person control); and
- Cross-certification paperwork and workflow of the Root CA and Subordinate CAs by the other Bridges.

The CA Administrator will ensure that the Root CA Keys will not be used to sign Certificates except in the following cases:

- Self-signed Certificate to represent the Root CA itself;
- Certificates for Issuing CAs and External CAs;
- Certificates for infrastructure purposes (e.g., administrative role Certificates, internal CA operational Certificates for Electronic Devices, and OCSP Response verification Certificates); and
- Certificates issued solely for the purpose of testing products with Certificates issued by the Root CA.

CA Administrators do not Issue to Subscribers.

IdenTrust will maintain redundancy in the role of CA Administrators. For the TrustID PKI, at least 2 CA Administrators are maintained in case a primary CA Administrator is on vacation, sick leave, etc.

5.2.1.2 RA Administrator

The RA Administrator of an RA is a Trusted Role with duties for the RA that are similar to those of the CA Administrator for IdenTrust, including the following responsibilities and operating procedures:

- Installation, configuration, and maintenance of software on the RA System;
- Key Generation and management of Keys and the Certificate lifecycle of the RA System; and
- Secure operation and management of the RA System, including patch management, backup, system logging, and physical and logical security.
- Within IdenTrust, the RA Administrator functions are performed by the System Administrator except for Key Management which would be performed by the CA Administrator.

5.2.1.3 Quality Assurance Personnel

As Quality Assurance Personnel roles perform functions that, if not carried out properly, can introduce security problems, whether accidentally or maliciously, controls are in place requiring approval from the Operations Management Personnel role prior to the introduction of code to Staging and Production environments. Quality Assurance Personnel have the following tasks:

- Develop and execute test plans;
- Identify and document defects;
- Conduct functional, regression, performance and user acceptance testing;
- Collaborate with cross-functional teams including developers, product managers and other stakeholders;
- Maintain test environments;
- Report and track quality metrics
- Lead Change Management from code freeze through Production deployment.

5.2.1.4 Local Registration Agent (LRA)

An LRA is a Trusted Role. The responsibilities and operating procedures for the LRA relating to CA and RA Operations are as follows:

- Verifying identity via review and approval of documents provided by the Applicant/PKI Sponsor/Subscriber or submitted by Trusted Agents if appropriate;
- Entering Applicant/PKI Sponsor/Subscriber information, verifying correctness, and approving requests;
- Securely communicating requests to and responses from the RA/CA Infrastructure System;
- Receiving and distributing Certificates;
- Authenticating identity upon request for Revocation and executing Revocation;
- Archiving of Subscriber authentication information (i.e., copies of paper forms, etc.);
- Operating of the LRA/RA systems and cryptographic hardware (including system backups and recovery, or changing recording media); and
- Generating of Cross-Certified Subordinate CA Certificate, the Root CA Certificate and Subordinate CA Certificates, re-keying, and Revocation (performed under 2-person control).

5.2.1.5 System Administrator

IdenTrust's System Administrators have Trusted Roles and are responsible for RA and CA operations not addressed by LRAs or Enterprise RAs and the following:

- Installation and configuration of operating systems, and databases;
- Installation and configuration of applications and initial setup of new accounts;
- Performance of system backups, software upgrades, patches, and system recoverability;
- Secure storage and distribution of backups and upgrades to an off-site location
- Performance of the daily incremental database backups; and
- Administrative functions such as time services and maintaining the database.

5.2.1.6 Network Engineer

IdenTrust's Network Engineers are Trusted Roles and responsible for:

- Initial installation and configuration of the network routers and switching; equipment, the configuration of initial host and network interface;
- Installation, configuration, and maintenance of firewalls, DNS, and load balancing appliances;
- Creation of devices to support recovery from catastrophic system loss; and
- Changing of the host or network interface configuration.

5.2.1.7 Security Officer

The IdenTrust Security Officers are Trusted Roles responsible for reviewing the audit logs recorded by CA, CSA, and RA systems and actions of administrators and operators during the performance of some of their duties. They also perform and oversee compliance audits to ensure compliance of the PKI with this CP-CPS.

A Security Officer reviews logs for events such as the following:

- Requests to and responses from the CA Infrastructure System;
- The Issuance of Certificates;
- Repeated failed actions;

- Requests for privileged information;
- Attempted access of system files, IdenTrust databases, or the RA database;
- Receipt of improper messages;
- Suspicious modifications;
- Performance of archive and delete functions of the audit log and other archive data as described in Section 5.4 and Section 5.5;
- Administrative functions such as compromise reporting; and
- For server Certificates, performing quarterly self-audits to monitor Certificate Issuance quality described in Section 8, Section 8.6, and Section 8.7.

The Security Officer also performs, or oversees, internal compliance audits to ensure that the CA, CSA, RA, and LRA systems are operating in accordance with this CP-CPS.

5.2.1.8 Software Engineer

The Software Engineers, also known as developers, have the following responsibilities:

- Build clean and efficient code based on user needs;
- Test software and debug for any issues;
- Collaborate with other developers, managers, systems personnel, product owners and UX designers in building software;
- Identify and deploy software tools, systems, and components;
- Implement quality assurance standards;
- Write and update technical documentation; and
- Handle incident response and incident management.

As Software Engineer roles perform functions that can introduce security problems if not carried out properly, whether accidentally or maliciously, controls are in place requiring approval from the Security Officer or from Operations Manager roles prior to the execution of any tasks that bridge Software Engineer roles.

5.2.1.9 Development Operations (DevOps)

The DevOps roles responsibilities are as follows:

- Build clean and efficient code based on user needs;
- Provide infrastructure and automation to support software development and deployment of applications;
- Coding to support process automation; i.e., infrastructure as code;
- Collaborate with other developers, managers, and technical operations;
- Identify and deploy software tools, systems, and components;
- Implement quality assurance standards;
- Write and update technical documentation; and
- Handle incident response and incident management.

As DevOps roles perform functions that can introduce security problems if not carried out properly, whether accidentally or maliciously, controls are in place requiring approval from the Security Officer or from Operations Manager roles prior to execution of any tasks that bridge DevOps roles.

5.2.1.10 Customer Support Representative

IdenTrust's Customer Support Representatives are Trusted Roles and perform the following duties:

- Troubleshooting of Certificate lifecycle events problems;
- Maintaining account information in the system that holds Subscriber information;
- Initiating Revocation processes; and
- Generating the External Root CA Certificate and Subordinate CA Certificate, re-keying, and Revocation (performed under 2-person control).

5.2.1.11 Operations Manager Personnel

A list of IdenTrust's Operations Managers (i.e., IdenTrust's Head of IdenTrust, and other Operations designees below the Head of Operations) is kept at all times as approved and authorized by the Head of IdenTrust. The Operations Manager performs the following duties:

- Provides internal audit oversight, and works closely with external auditors as needed;
- Handles approval/removal of Network, System and CA Administrators as well as Customer Support Representatives and LRAs;
- Acts as custodian of Activation Data for administrative Cryptographic Modules used with CA software;
- Works closely with the Security Officer to review requests for privileged information or sensitive system-related requests; and
- Participates as an active member of the Risk Management Committee.

As not all Operations Managers hold a Trusted Role, some of the requirements related to background checks do not apply to them.

5.2.2 Number of Persons Required per Task

The Issuing CA will utilize commercially reasonable practices to ensure that one person acting alone cannot circumvent safeguards.

IdenTrust has proper procedural and operational mechanisms in place to ensure that no single Individual may perform sensitive CA activities alone (known as Split-Knowledge Technique). These mechanisms apply principles of separation-of-duties/Multi-Party Control and require the actions of multiple persons to perform such sensitive tasks as:

- CA Key Generation;
- CA signing Key activation; and
- CA Private Key backup.

Physical and logical access controls are invoked to maintain Multi-Party Control over CA and CSA Cryptographic Modules (See Section 5.1.2 and Section 6.2.2). Generation, backup, or activation of the Certificate signing Private Keys require the actions of at least 2 Individuals, one of whom is a CA Administrator and the other who may not be a Security Officer.

5.2.3 Identification and Authentication for Each Role

The vetting of personnel in Trusted Roles is found below in Section 5.3.1 and Section 5.3.2. Identity Proofing for logical and physical access to CA Infrastructure System resources is described in this section. In accordance with IdenTrust's security policies, IdenTrust's CA personnel must first authenticate themselves before they are:

- included in the access list for any component of the CA Infrastructure System;

- included in the access list for physical access to a component of the CA Infrastructure System;
- issued a Certificate for the performance of their Trusted Role;
- given an account on a computer connected to the CA Infrastructure System; or
- otherwise granted physical or logical access to a component of the CA Infrastructure System.

Each of these access methods (Certificates and System accounts) is:

- directly attributable to the Individual;
- password/Account Password protected;
- not shared; and
- restricted to actions authorized for that role through the use of CA software, operating system, and procedural controls.

If accessed across shared networks, CA operations are secured, using hardware Cryptographic Modules, strong system authentication, and encrypted secure connections.

5.2.4 Roles Requiring Separation of Duties

IdenTrust maintains strict separation-of-duties/Multi-Party Controls for its Trusted Roles. These controls are audited annually by a third party auditor as part of the AICPA/CICA WebTrust Program for Certification Authorities audit described in Section 8.

Oversight of IdenTrust's Trusted Roles is performed by the Risk Management Committee, Operations Management, the human resources department, and Executive Management. IdenTrust maintains a list of Individuals performing each Trusted Role. The list is maintained by the highest-ranking Operations Manager (i.e., Head of IdenTrust or Head of Operations) and, for audit purposes, the Security Office maintains a current copy of the list.

5.3 Personnel Controls

IdenTrust and its RA, Trusted Agents, CMA, and Repository subcontractors implement personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and the satisfactory performance of their duties in a manner consistent with the requirements of this CP-CPS.

Contractor personnel engaged in performing functions for IdenTrust under this CP-CPS are required to meet all applicable requirements set forth in this CP-CPS, and SSP.

5.3.1 Qualifications, Experience, and Clearance Requirements

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor of the CA, the CA shall verify the identity and trustworthiness of such person.

Personnel who administer or operate components of the CA, CSA, and IdenTrust RA Systems and RA Systems, including LRAs are under the direct control of IdenTrust and meet the following requirements:

- Successful completion of appropriate training;
- Demonstrated ability to perform duties, as indicated by annual performance reviews;
- Trustworthiness, as initially determined by a background investigation;
- No other duties that would interfere or conflict with the duties of their Trusted Role;

- Not previously relieved of duties in a Trusted Role for reasons of negligence or non-performance of duties, as indicated by employment records;
- Not convicted of a felony offense, as indicated by a criminal background check; and
- Appointed in writing by Operations Management or pursuant to a written contract with IdenTrust or in a Certificate of incumbency, as evidenced by records maintained for such purpose by such Organization.

Each Enterprise RA and the Sponsoring Organization which employs and to which such Enterprise RA acts as a limited LRA shall be required under or pursuant to a contract by and among the Enterprise RA, Sponsoring Organization, and IdenTrust, to provide evidence of or representations and warranties to IdenTrust as to the following concerning such Enterprise RA:

- Successful completion of appropriate training programs as provided by IdenTrust;
- Demonstrated ability to perform duties, as indicated by annual performance reviews;
- No other duties that would interfere or conflict with the duties of their Enterprise RA Role;
- Passed Identity Proofing as per Section 3.2;
- The Sponsoring Organization that employees the Enterprise RA has authorized them and nominated them to fulfill the Enterprise RA functions for that entity; and
- A representative of the Sponsoring Organization that employees the Individual elected as the Enterprise RA has signed the Enterprise RA addendum asserting such contractual obligations.

5.3.2 Background Check Procedures

Persons appointed by IdenTrust to serve in Trusted Roles (with the exception of Enterprise RAs as explained above in Section 5.3.1) have undergone a local and national criminal background check, a drug test, and a financial status check through national credit bureau databases. Other checks are performed as described below for the purposes listed:

- Previous employers are contacted to determine whether the person is competent, reliable, and trustworthy;
- High schools, colleges, and universities are contacted to verify the highest or most relevant degree;
- Residency checks are performed to determine whether the person was and is a trustworthy neighbor;
- Driver's license records are checked through a commercial database to determine if the person has a record of serious or criminal violations; and
- A Social Security trace is performed to determine whether the person has a valid social security number. This check is required only if the country in which the duty is performed has social security number or a similar identifier.
- A criminal history check is performed through a commercial database, to determine that the person has no previous felony convictions;
- A credit history check is performed through a commercial database to determine that the person has not committed any fraud and is financially trustworthy; and
- Professional references are contacted to determine that the person is competent, reliable, and trustworthy.

The period of investigation covers at least the last 5 years for employment, education, criminal, and references, and the last 3 years for places of residence. Regardless of the date of award, the highest educational degree is verified.

Background checks are renewed periodically. If the initial or subsequent background checks

reveal a material misrepresentation by the Individual, substantially unfavorable comments from persons contacted, a criminal conviction, or personal financial problems, then it is brought to the attention of the Operations Manager and Security Officer who will evaluate the severity, type, magnitude, and frequency of the behavior or actions of the Individual, and determine the appropriate action to be taken, which may include removal from a Trusted Role.

RAs are obligated by contract and by this CP-CPS, to implement background check procedures equivalent to the ones explained above. To the extent that any of the foregoing cannot be met due to circumstances peculiar to that party, substantially similar procedures must be performed and may include background checks performed by government agencies or providers of such services in their jurisdictions.

5.3.3 Training Requirements and Procedures

IdenTrust shall provide all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the CA's CP and/or CPS), common threats to the information verification process (including phishing and other social engineering tactics), and the TLS BR.

IdenTrust shall maintain records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

IdenTrust shall require personnel wit Trusted Role duties to pass an examination provided by the CA on the information verification requirements.

Records of this training are upheld to ensure that personnel assigned to Validation Specialist duties maintain the proficiency needed to execute their responsibilities effectively.

Before authorizing a Trusted as described in Section 5.2.1 to undertake tasks, IdenTrust confirms the possession of essential skills.

IdenTrust requires that the relevant Trusted Role individual successfully complete an assessment conducted by the internal compliance team. This assessment evaluates their understanding of the information verification requisites outlined in the TLS BR for Server Certificates.

RAs are obligated by contract and by this CP-CPS to train its personnel and maintain a record of the training provided; specific additional areas are covered for each Trusted Role as outlined below.

5.3.4 Retraining Frequency and Requirements

All personnel in Trusted Roles shall maintain skill levels consistent with the CA's training and performance programs.

Any significant change to the CA and RA Systems requires that personnel receive additional training. Through a change control processes, (See Section 6.6) an awareness plan is prepared for any significant change to the Systems (e.g., a planned upgrade of CA equipment, software, or changes in procedures). All Trusted Role personnel undergo a retraining session once a year that includes a review of the applicable provisions of this CP- CPS under which they are operating, and a full review of all applicable policies and procedures.

Records are maintained documenting all Trusted Role personnel who have received training, including the level of training completed.

5.3.5 Job Rotation Frequency and Sequence

Job rotation is implemented when in the judgment of IdenTrust or RAs' management it is necessary to ensure the continuity and integrity of the IdenTrust's or RAs' ability to continually provide PKI-related services.

5.3.6 Sanctions for Unauthorized Actions

In the event of actual or suspected unauthorized action by a person performing duties with respect to the operation of the Issuing CA or RA, the Issuing CA should suspend his or her access to the Issuing CA Infrastructure System.

Failure of any employee or agent of IdenTrust or an RA to comply with the provisions of this CP-CPS, or federal regulations, whether through negligence or malicious intent, will subject such Individual to appropriate administrative and disciplinary actions, which may include termination as an employee or agent, and possible civil and criminal sanctions. Any person performing a Trusted Role who is cited by management for unauthorized actions, inappropriate actions, or any other unsatisfactory investigation results will be immediately removed from the Trusted Role pending management review. Subsequent to management review, and discussion of actions or investigation results with the employee, he or she may be reassigned to the Trusted Role, transferred to a non-Trusted Role, or dismissed from employment as appropriate.

5.3.7 Independent Contractor Requirements

IdenTrust shall verify that the Delegated Third Party's personnel involved in the Issuance of a Certificate meet the training and skills requirements of Section 5.3.3 and the document retention and event logging requirements of Section 5.4.1.

Independent contractors or Delegated Third Party personnel who are assigned to perform Trusted Roles are subject to the duties and all requirements of this CP-CPS, and are subject to the training requirements described in Section 5.3.3 and to the document retention and event logging requirements of Section 5.4.1.

5.3.8 Documentation Supplied to Personnel

CA and RA Personnel in Trusted Roles, including contractors, are provided with the documentation necessary to define and support the duties and procedures of the roles to which they are assigned. IdenTrust provides a copy of this CP-CPS, any relevant statutes, policies, and guidelines, and all technical and operational documentation needed to maintain, and integrate with the CA or RA Systems, as appropriate, as well as other relevant information to fulfill their tasks.

The information is available in print or online. The information provided consists of internal IdenTrust system and security documentation, IdenTrust policies and procedures, discipline-specific books, treatises and periodicals, and other information developed by or supplied to IdenTrust or the RA that is relevant to the role being performed.

RAs are obligated by contract and by this CP-CPS to provide to their personnel all relevant documentation, policies, contracts, and forms required to perform their jobs.

5.4 Audit Logging Procedures

For the purposes of the security audit, events related to the operation of the IdenTrust TrustID PKI are recorded as described in this section, whether the events are attributable to human action in

any role or are automatically invoked by the equipment that is used to register Applicants/PKI Sponsors; generate, sign and manage Certificates; and provide Revocation information.

Where possible, the audit data is automatically collected; when this is not possible, a logbook or other physical mechanism is used. All security logs, both electronic and non-electronic, are retained and maintained securely in accordance with the requirements of Section 5.5.2 and are made available during compliance audits.

IdenTrust conducts a human review of application and system logs at least once a month to validate the integrity of logging processes and ensure that monitoring, logging, alerting, and log integrity-verification functions are operating properly.

RAs are obligated by contract, and by this CP-CPS to configure their systems to automatically log the events described below. RAs are also required to maintain manual logging when automatic logging is not possible.

5.4.1 Types of Events Recorded

IdenTrust and each Delegated Third Party shall log all events related to the security of their Certificate Systems, and Root CA Systems. IdenTrust and each Delegated Third Party shall record events related to their actions taken to process a Certificate Request and to issue a Certificate, including all information generated and documentation received in connection with the Certificate Request; the time and date; and the personnel involved. IdenTrust shall make these records available to its Qualified Auditor as proof of the CA's compliance with the TLS BR.

IdenTrust records events related to the security of their Certificate Systems, and Root CA Systems. IdenTrust records events related to their actions taken to process a Certificate Request and to issue a Certificate, including all information generated and documentation received in connection with the Certificate Request; the time and date; and the personnel involved. IdenTrust makes these records available to its Qualified Auditor as proof of the CA's compliance with the TLS BR.

IdenTrust records at least the following events:

1. CA Certificate and Key lifecycle events, including:
    1. Key Generation, backup, storage, recovery, archival, and destruction;
    2. Certificate Requests, renewal, and re-key requests, and Revocation;
    3. Approval and rejection of Certificate Requests;
    4. Cryptographic device lifecycle management events;
    5. Generation of Certificate Revocation Lists;
    6. Signing of OCSP Responses (as described in Section 4.10); and
    7. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate lifecycle management events, including:
    1. Certificate Requests, renewal, and re-key requests, and Revocation;
    2. All verification activities stipulated in the TLS BR and this CP-CPS;
    3. Approval and rejection of Certificate Requests;
    4. Issuance of Certificates;
    5. Generation of Certificate Revocation Lists; and
    6. Signing of OCSP Responses (as described in Section 4.10).
    7. Multi-Perspective Issuance Corroboration attempts from each Network Perspective, minimally recording the following information:
        1. an identifier that uniquely identifies the Network Perspective used;
        2. the attempted Domain Name and/or IP address; and

        3. the result of the attempt (e.g., “domain validation pass/fail,” “CAA permission/prohibition”).
    8. Multi-Perspective Issuance Corroboration quorum results for each attempted Domain Name or IP Address represented in a Certificate Request (i.e., “3/4” which should be interpreted as “Three (3) out of four (4) attempted Network Perspectives corroborated the determinations made by the Primary Network Perspective).
3. Security events, including:
    1. Critical Security Events;
    2. Successful and unsuccessful PKI System access attempts;
    3. PKI and Security Support System actions performed;
    4. Security profile changes;
    5. Installation, update, and removal of software on the CA infrastructure System;
    6. System crashes, hardware failures, and other anomalies;
    7. Relevant router and firewall activities (as described in Section 5.4.1.1); and
    8. Entries to and exits from the CA facility.

IdenTrust logs records include the following elements:

1. Date and time of event;
2. Identity of the person making the journal record; and
3. Description of the event.

IdenTrust’s CA, CSA, and RA equipment automatically log all significant operational events, including those involving routers, firewalls, and other Network Boundary Control Systems, individual hosts, applications and databases; and physical security checkpoints.

IdenTrust staff members manually record all significant events that are not logged by the equipment.

RAs are obligated by contract and this CP-CPS, to record all significant events related to their operations.

For events recorded, the minimum information logged includes the following items: type of event, time of occurrence, the identity of the Individual or System that logged the event, who caused the event, and a success or failure indication. For some types of events, these minimums may be expanded to include items such as the source or destination of a message, or the disposition of a created object (e.g., a filename).

5.4.1.1 Router and Firewall Activities Log

Logging of router and firewall activities necessary to meet the requirements of Section 5.4.1 (Subsection 3.6) must at a minimum include:

1. Successful and unsuccessful login attempts to routers and firewalls; and
2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and
3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and
4. Logging of all System events and errors, including hardware failures, software crashes, and System restarts.

5.4.2 Frequency of Processing Log

IdenTrust Security Officers and System Administrators conduct reviews of all the audit log data through a combination of automated and manual means at least weekly. In order to ensure a thorough review of all data, the Security Officer selects all CA, CSA, and RA logs for review and a minimum of 25% of other security audit data generated since the last review for each category of audit data.

The Security Officer uses automated tools to scan logs for specific conditions. The Security Officer then reviews the output and produces a written summary of findings when significant events that require documentation occur. The reviews include the date, name of the reviewer, description of the event, details of findings, and recommendations for remediation or further investigation if appropriate. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. The reviews include CA, CSA, and RA activities that are listed as recorded in Section 5.4.1. These reviews are made available to IdenTrust's external auditor.

Restrictions are applied to the logs to prevent unauthorized access, deletion, or overwriting of data. Storage capability is monitored to ensure that sufficient space exists to prevent overflow conditions. Alerts are sent to a Security Officer if the space available becomes inadequate.

The security audit logs are moved monthly to the archive by Security Officer in accordance with Section 5.4.4.

RAs are obligated by contract, and by this CP-CPS, to implement controls that allow them to review logs consistent with practices outlined in this section. Enterprise RAs logs are collected electronically through the administrative interface provided by IdenTrust.

5.4.3 Retention Period for Audit Log

IdenTrust retains audit logs for at least 2 years of:

1. CA Certificate and Key lifecycle management event records Key Generation, backup, storage, recovery, archival, and destruction as set forth in Section 5.4.1 (1) after the later occurrence of:
    - the destruction of the CA Private Key; or
    - the Revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 *basicConstraints* extension with the *cA* field set to true and which share a common Public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records as set forth in Section 5.4.1 (2) after the expiration of the Subscriber Certificate;
3. Any security event records as set forth in Section 5.4.1 (3) after the event occurred. All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits.

Audit log information generated on CA, CSA, and RA equipment is kept on the equipment until the information is moved to the offsite archive facility described in in Section 5.1.8 for IdenTrust secure registration messaging Protocol details. There are 90 days of active logs remaining on the equipment for analysis. The oldest 30 days – e.g., logs dated between 90 and 120 days, are removed monthly to be archived by the Security Officer in accordance with Section 5.4.4. Electronic audit logs are deleted only after they have been backed up to archive media.

Only Security Officers are authorized to delete these logs and must first verify that the audit log data has been successfully backed up to archive media by checking hash values against the original and the backup copies.

RAs are obligated by contract, and by this CP-CPS, to implement controls that allow them to retain audit logs consistent with practices outlined in this section. Enterprise RAs logs are collected electronically through the administrative interface provided by IdenTrust.

5.4.4 Protection of Audit Log

The security audit logs are written simultaneously to separate network locations to ensure their safety and security. No Individual is given the permissions required to modify or delete files in all 3 locations. The log storage capability is monitored by the operating systems at each location to ensure that sufficient space exists to prevent overflow conditions. Logs for the current and 2 prior months are retained on each server and on the logging hosts to aid in troubleshooting. Alerts are sent to the System Administrators and to the Security Office if it appears that the space available will become inadequate.

The integrity of each archived audit log is ensured by the use of a checksum. The Security Office oversees procedures governing the archiving of all audit logs to ensure that archived data is protected from modification, deletion, or premature destruction. Each month, audit data and review summaries no longer needed on the hosts are archived and moved to a secure offsite storage location as described in Section 5.1.8. As described previously, the audit logs and related materials are stored separately from the daily backups, and access to the offsite data is restricted to Security Officers.

RAs are obligated by contract, and by this CP-CPS to implement controls that allow them to prevent unauthorized access, deletion, or overwriting of data; and to back up the audit logs in a manner consistent with practices outlined in this section.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries must be backed up or copied if in manual form.

IdenTrust makes a backup of each audit log monthly as described in Section 5.5.3 and Section 5.5.4. Backup copies of the audit logs and audit summary data are transferred to the secure offsite location in locked containers separate from all other storage containers. They are also stored separately and can be retrieved only by the Security Office.

RAs are obligated by contract, and by this CP-CPS to implement controls that allow them to backup audit logs consistent with practices outlined in this section. Enterprise RAs logs are collected electronically through the administrative interface provided by IdenTrust.

5.4.6 Audit Collection System (Internal vs. External)

Automated audit log collection systems are internal to the CA, CSA, RA, and Repository. These Systems invoke audit processes at System startup, which cease only at System shutdown. Processes are enforced technically through the operating system and a secondary monitoring application.

As described in Section 5.5.4, audit log collection systems are configured such that security audit data logs are protected against loss (e.g., overwriting or overflow of automated log files).

RAs are obligated by contract, and by this CP-CPS, to implement controls that allow them to ensure audit data are protected against loss in consistency with practices outlined in this section.

Enterprise RA logs are collected electronically through the administrative interface provided by IdenTrust.

5.4.7 Notification to Event-Causing Subject

IdenTrust provides no notice to the event-causing entity (i.e., Subscriber, Sponsoring Organization, or Device) that an event was audited.

5.4.8 Vulnerability Assessments

The Security Officers, System Administrators, and other operating personnel monitor attempts to violate the integrity of the CA Infrastructure System, including the equipment, physical location, and personnel. The audit logs are checked for anomalies that may indicate violations and are reviewed by the Security Office for events including but not limited to repeated failed actions, attempts to acquire privileged access, requests for privileged information, attempted access of System files, and unauthenticated responses. The Security Office also checks for continuity of the security audit data. Reviews of the security audit logs are conducted by the Security Office in accordance with Section 5.5.2.

IdenTrust undergoes or performs a vulnerability scan

1. within one week of receiving a request from the CA/Browser Forum,
2. after any System or network changes that the CA determines are significant, and
3. at least every 3 months, on public and private IP Addresses identified by the CA as the CA's Certificate Systems.

IdenTrust undergoes a Penetration Test on the CA's Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant;

IdenTrust records evidence that each Vulnerability Scan and Penetration Test was performed by a person or entity (or collective group thereof) with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test. See Section 8 for additional details.

5.5 Records Archival

5.5.1 Types of Records Archived

IdenTrust shall and each Delegated Third Party shall archive all audit logs (as set forth in Section 5.4.1).

Additionally, the CA and each Delegated Third Party shall archive:

1. Documentation related to the security of their Certificate Systems, and Root CA Systems; and
2. Documentation related to their verification, Issuance, and Revocation of Certificate Requests and Certificates.

IdenTrust retains and archives all data through the life of TrustID PKI Certificates. Archive records are sent to the vault 3 days a week and archived offsite for at least 7 years and 6 months. The archive records are designed to be sufficiently detailed to establish the proper operation of the PKI or the validity of any Certificate (including those revoked or expired) issued by IdenTrust.

IdenTrust maintains and archives that information and more in the following records, in either electronic or paper format. The use of electronic records is preferred, and paper records are

digitized whenever possible.

- CA accreditation;
- CP; CPS; or CP-CPS
- Contractual obligations and other agreements concerning operations of the CA;
- System and equipment configuration;
- Modifications and updates to System or configuration;
- Certificate Requests;
- Record of re-key;
- Revocation requests;
- Subscriber Identity Proofing data per Section 3.2.3;
- Documentation of receipt and Acceptance of Certificates;
- Export of Private Keys;
- Subscriber Agreements;
- Documentation of loading, shipping, receipt, and zeroizing of Cryptographic Modules;
- All Certificates issued or published;
- Security audit data in accordance with Section 5.4.1;
- All changes to the trusted Public Keys;
- All CRLs issued and/or published;
- All routine Certificate validation transactions;
- Other data or applications to verify archive contents;
- Documentation required by compliance auditors; and
- Subscriber encryption Private Keys that are archived/escrowed in accordance with this CPS.

RAs are obligated by contract, this CP-CPS to retain and archive data through the life of the contract with IdenTrust. After notification of the end of the Contract has occurred, IdenTrust will convene with the RA to agree on the terms to transfer the data to IdenTrust. The RA shall maintain the following records:

- Contractual obligations and other agreements concerning operations of the RA;
- Other agreements concerning the RA/LRA operations;
- RA System and equipment configuration;
- Modifications and updates to System or configuration;
- Certificate Requests;
- Security audit data in accordance with Section 5.4.1;
- Revocation requests;
- Subscriber Identity Proofing data per Section 3.2.3;
- Documentation of receipt and Acceptance of Certificates;
- Subscriber Agreements;
- Documentation of loading, shipping, receipt, and zeroizing of Cryptographic Modules; and
- Documentation required by compliance auditors.

Enterprise RAs logs are collected electronically through the administrative interface provided by IdenTrust.

5.5.2 Retention Period for Archive

Archived audit logs (as set forth in Section 5.5.1) shall be retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer.

Additionally, the CA shall retain, for at least 2 years:

1. All archived documentation related to the security of Certificate Systems, and Root CA Systems (as set forth in Section 5.5.1); and
2. All archived documentation relating to the verification, Issuance, and Revocation of Certificate Requests and Certificates (as set forth in Section 5.5.1) after the later occurrence of one of such records and documentation were last relied upon in the verification, Issuance, or Revocation of Certificate Requests and Certificates; or
3. the expiration of the Subscriber Certificates relying upon such records and documentation.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site. Software applications required to process the archive data will also be maintained for as long as necessary. After the minimum archive retention period, external RAs and PKI Service Providers are responsible for maintaining the authenticity and integrity of their own valuable documents.

Archive records are sent to the vault 3 days a week and archived offsite for at least 7 years and 6 months.

IdenTrust maintains copies of the applications that can read these types of files for at least the retention period.

RAs are obligated by contract, this CP-CPS to implement controls that allow them to retain records and copies of the application that can read those files for at least 7 years and 6 months.

5.5.3 Protection of Archive

No unauthorized Individual will be able to write to, modify, or delete the archive. However, archived records may be moved to another medium. The contents of the archive will not be released as a whole, except as required by law. Records of Individual transactions may be released upon request of any entities involved in the transaction or their legally recognized agents. Archive media will be stored in a separate, safe, secure storage facility.

Archived data is stored in a separate, offsite storage facility identified in Section 5.1.6. Records are uniquely identified. The media used for retaining the archived data is specifically chosen and tested to ensure that the archived data will be conserved on the same media for the minimum retention period defined in Section 5.5.2.

The contents of the archive will not be released as a whole, except as required by law, as described in Section 9.4. Access to the offsite storage facility is strictly limited to Individuals who have been authorized by the IdenTrust Head of Operations or the Security Office. IdenTrust maintains a list of people authorized to access the archive records and makes this list available to its auditors during compliance audits. Certain sensitive materials are stored in a physically separate area within the offsite storage location, and access to the materials is limited to IdenTrust's Security Officers. The IdenTrust Security Office oversees procedures governing the archival of the audit log to ensure that archived data is protected from deletion or destruction during the data retention period.

The integrity of the electronic archive data is protected through multiple means, while also ensuring that no transfer of medium will invalidate the applied checksum, and any attempt to modify the data will be evident. Repository information is archived in a human readable form. IdenTrust maintains copies of the applications that can read these types of files for at least the retention period.

RAs are obligated by contract, and by this CP-CPS to implement controls that allow them to protect the archive media from disclosure, modification, or destruction consistent with practices in this

section.

5.5.4 Archive Backup Procedures

Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies will be readily available within a short period of time.

All archive copies are stored in the offsite storage facility and are readily available within a short time in the event of loss or destruction of the primary data center or Secure Room.

5.5.5 Requirements for Times-Stamping of Records

CA archive records shall be automatically time-stamped as they are created.

See Section 6.8.

5.5.6 Archive Collection System (Internal or External)

Archived data is collected internally and stored in a separate, offsite storage facility identified in Section 5.1.6.

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

5.6 Key Changeover

An End Entity may only apply to renew his, her, or its TrustID Certificate within three months before the expiration of one of the Keys, provided the previous Certificate has not been revoked. An End Entity, the Issuing CA, or the RA may initiate this Key changeover process. Automated Key changeover is permitted.

When IdenTrust re-keys its signature Private Key and thus generates a new Public Key, it will make it publicly known in the Repository and notify the PMA, RAs, and Subscribers that rely on its CA Certificate, that it has changed its Keys.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

IdenTrust documents and maintains security incident response and compromise handling policies and procedures, as well as disaster recovery and business continuity plans. Such procedures and plans are available for onsite review by its auditors and major Authorized Relying Parties under appropriate non-disclosure agreements. Below is a synopsis of the incident response policies and procedures.

For each incident, an initial goal of the incident response plan is to determine the degree and scope of the incident. This includes a determination of the cause or source of the incident (e.g., internal System failure, external malicious attack, user error), and the potential severity of the harm caused by the incident. For all incidents, data is collected and analyzed to determine, among other things:

- Whether a crime has been committed, and if so, whether evidence can be collected that will be helpful to law enforcement;

- What data was disclosed or compromised, and whether there was a Private Key Compromise; and
- What steps need to be taken immediately to mitigate further damage.

For anticipated threats, IdenTrust maintains step-by-step procedures and task assignments for members of the incident response team, depending on the type of incident that is believed to have occurred. IdenTrust annually tests, reviews, and updates these procedures. Procedures are tested at least annually as part of the disaster recovery exercise.

5.7.1.1 Mass Revocation Plan

IdenTrust maintains a robust and actionable plan for mass revocation events, conducts annual tests on the procedure, and continuously integrates lessons learned to enhance future readiness.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

IdenTrust backs up essential information in near-real time to its disaster recovery site, as described in Section 5.1.8. IdenTrust also performs backups of all its production CA Infrastructure Systems daily, also as described in Section 5.1.8. Backup tapes and backups of Cryptographic Modules are stored offsite in a secure location. In the event of a disaster in which the primary data center becomes inoperative, the disaster recovery site can take over Certificate validation operations promptly and can provide all other essential CA operations within 72 hours. If both principal and backup CA operations become inoperative, IdenTrust's CA operations will be re-initiated on appropriate hardware using backup copies of software and Cryptographic Modules.

Re-initiation will occur according to one of the following contingencies:

- If the IdenTrust CA signature Keys are not destroyed, IdenTrust CA operations will be reestablished, giving priority to the ability to generate Certificate status information within the CRL Issuance schedule specified in Section 4.9.7.
- If the IdenTrust CA signature Keys are destroyed, IdenTrust CA operation will be reestablished as quickly as possible, giving priority to the generation of a new IdenTrust CA Key Pair and Certificate with new DN; the old IdenTrust CA Certificate will be revoked, and notification will be placed on a CRL as specified in Section 4.9.3; new Certificates will be issued.

Subscribers will be notified and instructed via email and a secure IdenTrust site (e.g., https://secure.identrust.com) on how to remove the old Root CA from their Certificate stores and install the new root in their Certificate stores.

If a CA (i.e., Root or Subordinate CA) cannot issue a CRL before the time specified in the *next-update* field of its currently valid CRL, then the Relying Parties and all CAs that have issued Certificates to the CA will be notified informally via telephone call immediately. This call will be followed formally by a Certificate-based communication if possible; otherwise, by a written letter sent via courier service.

A Subordinate CA Certificate will be revoked if Revocation services are not reestablished within a reasonable period of time. The period of time will be established by the highest-ranking IdenTrust Operations Manager and representatives from the IdenTrust's Risk Management Committee after analyzing the risk exposure at the time. However, the CA may be revoked at any time. As guidelines, this period should not exceed 18 hours after a Revocation has been requested of any Certificate issued under the CA; or 72 hours after the last CRLs next update, whichever occurs earlier.

When the Root CA Certificate is unable to issue a CRL, the highest-ranking IdenTrust Operations Manager and representatives from the IdenTrust Risk Management Committee will establish the risk exposure and determine whether to stand up a new Root CA Certificate. If a CA has requested Revocation of its Certificate by the root, the risk exposure must be considered as high, and within an 18-hour period after the Revocation has been requested, the procedures described in a prior paragraph in this section are used to revoke the old Root CA Certificate and to establish and promulgate the new Root CA Certificate.

5.7.3 Entity Private Key Compromise Procedures

IdenTrust has developed a Private Key Compromise plan to address the procedures that will be followed in the event of a compromise of the signature Private Key used by IdenTrust to issue TrustID Certificates. The plan includes procedures for (and documentation of) revoking all affected TrustID Certificates it has issued, and promptly notifying all Subscribers and all Relying Parties.

If IdenTrust signature Keys are compromised or lost (such that compromise is possible even though not certain), IdenTrust will:

- Immediately notify all CAs with whom it has cross-certified;
- Revoke all TrustID Certificates it has issued using that Key and provide appropriate notice;
- Generate a new IdenTrust Key Pair using appropriate procedures as outlined elsewhere in this CP-CPS;
- Distribute its new CA Certificate using the reliable out-of-band means allowed by this CP-CPS;
- Issue new CA Certificates to Subordinate CAs in accordance with this CP-CPS; and
- Ensure all CRLs are signed using the new Key.

IdenTrust will investigate what caused the compromise or loss, and what measures have been taken to preclude recurrence.

5.7.4 Business Continuity Capabilities After a Disaster

IdenTrust has a disaster recovery/business resumption plan in place (Business Continuity Plan or BCP) that allows IdenTrust to reconstitute the CA within 72 hours of catastrophic failure. IdenTrust's business continuity and disaster recovery plans allow for other nonessential Systems to be brought into operation later than 72 hours.

If for any reason the CA installation is physically damaged and all copies of the CA signature Key are destroyed as a result, IdenTrust will notify any applicable Policy authorities. Relying Parties may decide of their own volition whether to continue to use Certificates signed with the destroyed Private Key pending reestablishment of CA operation with new Certificates.

5.8 CA or RA Termination

In the event that it is necessary for IdenTrust or an RA to cease operation, all affected parties will be notified of the planned termination, promptly and as far in advance as is commercially reasonable. A termination plan will be created and submitted to the IdenTrust PMA. The termination plan will propose methods of minimizing the disruption to the operations of all parties caused by the planned termination and also include provisions for the termination of the RA, termination of contractual relationship with a sponsoring Organization with Enterprise RAs, termination of the Issuer CA and termination of the Root CA.

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

For CA Key Pairs that are either

1. used as a CA Key Pair for a Root CA Certificate or
2. used as a CA Key Pair for a Subordinate CA Certificate, where the Subordinate CA is not the operator of the Root CA or an Affiliate of the Root CA,

The CA Shall:

1. prepare and follow a Key Generation Script,
2. have a Qualified Auditor witness the CA Key Pair Generation process or record a video of the entire CA Key Pair Generation process, and
3. have a Qualified Auditor issue a report opining that the CA followed its Key Ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

For other CA Key Pairs that are for the operator of the Root CA or an Affiliate of the Root CA, the CA should:

1. prepare and follow a Key Generation Script and
2. have a Qualified Auditor witness the CA Key Pair Generation process or record a video of the entire CA Key Pair Generation process.

In all cases, the CA shall:

1. generate the CA Key Pair in a Physically Secured Environment as described in the CA's Certificate Policy and/or Certification Practice Statement;
2. generate the CA Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge;
3. generate the CA Key Pair within Cryptographic Modules meeting the applicable technical and business requirements as disclosed in the CA's Certificate Policy and/or Certification Practice Statement;
4. log its CA Key Pair Generation activities; and
5. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

Cryptographic Keying material used by IdenTrust to sign Certificates, CRLs, or status information is generated in FIPS 140-2 level 3 or higher validated Cryptographic Modules.

IdenTrust and CSA Key Generation ceremonies are performed in the Secure Room. The Key Generation ceremony is scripted, video-recorded, and witnessed by an internal auditor, attesting that keys were protected in a manner consistent with the requirements defined in Section 6.2.

The Root CA Key Pair Generation ceremony is witnessed by IdenTrust Qualified Auditor in order to observe the process and the controls over the integrity and confidentiality of the Root CA Key Pairs produced. The Qualified Auditor must then issue a report opining that the CA, during its Root CA Key Pair and Certificate generation process:

1. Documented its Root CA Key Generation and protection procedures in its Certificate Policy, and its Certification Practices Statement;
2. Included appropriate detail in its Root Key Generation Script;
3. Maintained effective controls to provide reasonable assurance that the Root CA Key Pair was generated and protected in conformity with the procedures described in its CP-CPS and with its Root Key Generation Script;
4. Performed during the Root CA Key Generation process, all the procedures required by its Root Key Generation Script.

The Key Generation ceremony is performed by personnel in Trusted Roles who use different security Keys at the appropriate time depending on whether Key Generation, Certificate generation, or a Cryptographic Module backup/cloning operation is being performed. The scripts and video recordings are made available to independent third party auditors during the annual audit for examination.

6.1.1.2 RA Key Pair Generation

No stipulation.

6.1.1.3 Subscriber Key Pair Generation

IdenTrust shall reject a Certificate Request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. IdenTrust is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. IdenTrust have previously been notified that the Applicant's Private Key has suffered a Key Compromise, using the procedure for Revocation request as described in Section 4.9.3 and Section 4.9.12;
5. The Public Key corresponds to an industry-demonstrated weak Private Key; at least the following precautions are implemented:
    1. In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), the CA shall reject all keys found at https://github.com/cabforum/Debian-weak-keys/.
    2. For each Key type (e.g., RSA, ECDSA) and size listed in the Repository. For all other keys meeting the requirements of Section 6.1.5 with the exception of RSA Key sizes greater than 8192 bits, IdenTrust shall reject Debian weak keys.
    3. In the case of ROCA vulnerability, the CA shall reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.
    4. In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), the CA shall reject weak keys which can be factored within 100 rounds using Fermat's factorization method.

Suggested tools for checking for weak keys can be found here:
https://cabforum.org/resources/tools/

If a server Subscriber Certificate includes an *extKeyUsage* extension with either the *id-kp-serverAuth* or *anyExtendedKeyUsage* values (as defined in RFC 5280), IdenTrust shall not generate the Key Pair on behalf of the Subscriber and must also not Accept a Certificate Request that uses a Key Pair

previously generated by the CA. IdenTrust reject a Certificate Request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. IdenTrust is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. IdenTrust have previously been notified that the Applicant's Private Key has suffered a Key Compromise, using the procedure for Revocation request as described in Section 4.9.3 and Section 4.9.12;
5. The Public Key corresponds to an industry-demonstrated weak Private Key; at least the following precautions are implemented:
    1. In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), IdenTrust shall reject all keys found at https://github.com/cabforum/Debian-weak-keys/ for each Key type (e.g. RSA, ECDSA) and size listed in the Repository. For all other keys meeting the requirements of Section 6.1.5 with the exception of RSA Key sizes greater than 8192 bits, IdenTrust shall reject Debian weak keys.
    2. In the case of ROCA vulnerability, IdenTrust shall reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.
    3. In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), IdenTrust shall reject weak keys which can be factored within 100 rounds using Fermat's factorization method.

Suggested tools for checking for weak keys can be found here:
https://cabforum.org/resources/tools/

6.1.2 Private Key Delivery to Subscriber

Parties other than the Subscriber shall not archive the Subscriber Private Key without authorization by the Subscriber.

If the CA or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an Organization not affiliated with the Subscriber, then the CA shall revoke all Certificates that include the Public Key corresponding to the communicated Private Key.

When the encryption Keys and Certificates are not escrowed, the System allows the Subscriber to generate the Private Keys in the same way signature Keys are generated. Non-escrowed encryption Private Keys will be generated and remain within the boundaries of the hardware or software Cryptographic Module where they are generated.

If IdenTrust or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an Organization not affiliated with the Subscriber, then IdenTrust shall revoke all Certificates that include the Public Key corresponding to the communicated Private Key.

6.1.3 Public Key Delivery to Certificate Issuer

The Subscriber's Public Key is delivered to IdenTrust or the RA (which in turn is delivered to IdenTrust) in a secure and trustworthy manner. Should the initial information be sent to an RA,

that information will be securely forwarded (through any form of digital communications) to IdenTrust. The delivery of the Public Key, in a *PKCS#10* structure, binds the Private and Public Keys, through a Digital Signature, and is submitted to the CA during a server-authenticated SSL/TLS encrypted session.

Before the retrieval process, an Enterprise RA enrolls applications in bulk (i.e., a bulk load file) of Applicants/PKI Sponsors and approves Issuance of a Certificate to the Subscribers and PKI Sponsors. Activation Code(s) is/are generated and sent via a verified channel to the Applicant/PKI Sponsor before the time of retrieval. The Applicant/PKI Sponsor uses the Activation Code(s) in a server-authenticated SSL/TLS encrypted session during which the Public Key is submitted to the RA/CA in a *PKCS#10* and a Certificate is returned back during the same session.

6.1.4 CA Public Key Delivery to Relying Parties

IdenTrust and its RAs ensure that Subscribers and Relying Parties receive and maintain the trust anchor(s) in a trustworthy fashion. Methods implemented for this delivery may include:

1. The Public Key may be delivered to Subscribers during the Certificate retrieval process for their own Subscriber's Certificates during the server-authenticated SSL/TLS encrypted session as part of a message formatted in accordance with the *PKCS#7*.
2. The Public Key may also be delivered through the cryptographic container in the major browsers. IdenTrust maintains a trust anchor for the TrustID program that is embedded in the browser through their CA Root programs. This process requires fulfilling specific requirements by the browser manufacturers including providing them with the trust anchor in a secure manner. Browsers distribute the trust anchor and any updates along with the standard distribution of their software in a secure manner.
3. Relying Parties may also obtain the trust anchor(s) (e.g., Root CA) Certificates from IdenTrust's secure website. An email or other communication may be sent to Participants directing them to download the trust anchor(s) Certificate at an https:// website secured with a valid server Certificate that chains to one of IdenTrust's Root CA Certificates in the browser. Alternatively, Subscribers and Relying Parties may be directed to an http:// website that is not secured in which case, IdenTrust will provide the hash or fingerprint via authenticated out-of-band sources (i.e., IdenTrust Customer Support)

In cases where the RA manages the insertion of the Certificate and Root CA into the Cryptographic Module, IdenTrust provides the trust anchor(s) Certificate securely to the RA using physical in-person delivery by an IdenTrust PKI Consultant during initial System setup. Then, the RA is obligated by contract, and by this CP-CPS to ensure the Subscriber receives the Root CA Certificate in a trustworthy fashion.

6.1.5 Key Sizes

For RSA Key Pairs the CA shall:

- Ensure that the modulus size, when encoded, is at least 2048 bits, and;
- Ensure that the modulus size, in bits, is evenly divisible by 8.

For ECDSA Key Pairs, the CA shall:

- Ensure that the Key represents a valid point on the NIST P-256, NIST P-384 or NIST P-521 elliptic curve.

No other algorithms or Key sizes are permitted.

For Keys corresponding to Root and Subordinate CAs:

- If the Key is RSA, then the modulus must be at least 4096 bits in length.
- If the Key is ECDSA, then the curve must be one of NIST P-256, P-384, or P-521.

For Keys corresponding to Subscribers:

- If the Key is RSA, then the modulus size, when encoded, is at least 2048 bits in and is evenly divisible by 8
- If the Key is ECDSA, then the curve must be one of NIST P-256, P-384, or P-521.

6.1.6 Public Key Parameters Generation and Quality Checking

For RSA Key Pairs: the CA shall confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent should be in the range between $2^{16}+1$ and $2^{256}-1$. The modulus should also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. (See NIST SP 800-89, Section 5.3.3).

For ECDSA Key Pairs: IdenTrust should confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. (See NIST SP 800-56A: Revision 3, Section 5.6.2.3.3 and 5.6.2.3.4).

Cryptographic Modules and associated software platforms used by CAs, the CSA, and Subscribers and RAs have been validated as conforming to FIPS 140-2 level 3 or higher and provide random number generation and onboard creation of 2048-bit Key lengths for RSA Public Key Generation.

When IdenTrust implements Elliptic Curve Public Key parameters, they will be selected from the set specified in Section 7.1.3 Algorithm Object Identifiers.

6.1.7 Key Usage Purposes (as per X509 v3 *keyUsage* Field)

IdenTrust does not use Private Keys corresponding to the Root CA Certificates to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (e.g., administrative role Certificates, internal CA operational device Certificates); and
4. Certificates for OCSP Response verification.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

IdenTrust shall implement physical and logical safeguards to prevent unauthorized Certificate Issuance. Protection of the CA Private Key outside the validated system or device specified in Section 6.2.7 must consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Key. IdenTrust shall encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted Key or Key part.

6.2.1 Cryptographic Module Standards and Controls

IdenTrust uses FIPS 140-2 level 3 or higher validated hardware Cryptographic Modules for the CA, the OCSP (CSA), and backup Cryptographic Modules. These modules do not allow the output of the

private asymmetric Key to plaintext.

The installation, removal, and destruction of all Cryptographic Modules holding CA (i.e., Root or Subordinate CA) and CSA Keys is documented in writing, approved by management, witnessed, and video recorded.

6.2.2 Private Key (N out of M) Multi-Person Control

IdenTrust and CSA signature Private Keys are stored in the Secure Room under multi-person control as described in Section 5.1.2. The PIN Entry Device Keys (PED Keys) are kept in a separate safe. At least one CA Administrator and one System Administrator are required, along with the additional presence of a Security Officer, to retrieve and activate the CA or CSA signature Private Keys.

For purposes of disaster recovery, backups of CA and CSA signature Private Keys are made under 2-person control and are stored in the Secure Room and in a secure off-site facility where 2-person controls are implemented as explained in Section 5.1.6, Section 5.1.8, and Section 5.2.2.

This separation-of-duties/Multi-Party Control prevents a single Individual from gaining access to a CA or CSA signature Private Keys.

The Individuals taking part in tasks that require 2-person control and separation of duties principles are Trusted Roles within IdenTrust. As such, their names are part of a list maintained within the Operations group and made available during audits (See Section 5.2.1).

6.2.3 Private Key Escrow

6.2.3.1 Escrow of CA Signature Private Key

IdenTrust does not escrow the CA Private Keys used to sign Certificates and CRLs

6.2.3.2 Escrow of Subscriber's Signature Private Keys

IdenTrust does not escrow Subscriber's signature Private Keys. RAs are prohibited under this CP-CPS from escrowing the signature Private Keys of Subscribers.

6.2.3.3 Escrow of Subscriber's Encryption Private Keys

Subscriber's encryption Private Keys may be escrowed to enable Key recovery. Encryption Private Key escrow is decided on an implementation specific basis.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Signature Private Keys

The backup of all other CA Keys is performed during a ceremony that is scripted, video recorded and witnessed under the same controls used for the original Key Generation. PED Keys are kept under 2-person control as explained in Section 5.2.2.

IdenTrust stores the Root CA and all other CA Private Keys and one of the copies in the Secure Room. The second backup of the Root CA and all other CA's signature Private Keys are kept in a secure off-site facility. Access to these Private Keys is documented as explained in Section 5.1.6.

6.2.4.2 Backup of Subscriber's Signature Private Key

A Subscriber may optionally back up his, her, or its own Private Key. If so, the Key must be copied and stored in encrypted form and protected at a level no lower than stipulated for the primary version of the Key.

6.2.5 Private Key Archival

IdenTrust does not archive its CA signature Private Keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

CA and CSA Private Keys are generated on FIPS 140-2 level 3 or higher validated Cryptographic Module that allows for a "cloning" process that creates a copy of the Private Keys. IdenTrust uses the cloning process to create one or more copies for purposes of business continuity. IdenTrust Private Keys are backed up in accordance with Section 6.2.4.

If IdenTrust becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an Organization not affiliated with the Subordinated CA, then IdenTrust will proceed to revoke all Certificates that include the Public Key corresponding to the communicated Private Key.

6.2.7 Private Key Storage on Cryptographic Module

The IdenTrust CA shall protect its Private Key in a System or device that has been validated as meeting at least FIPS 140-2 level 3 or higher validated Cryptographic Module, or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats.

6.2.7.1 Private Key Storage for CA Keys

IdenTrust's CA and CSA Private Keys are stored in Systems or devices that have been validated as meeting at least FIPS 140-2 level 3 or higher validated Cryptographic Modules.

6.2.8 Method of Activating Private Key

CA and CSA Private Keys are activated by using Activation Data stored securely and separately from the Cryptographic Modules in which they are kept. Activation of the Private Key requires a PED Key to be connected to the module. The PED Keys and Cryptographic Modules are stored in separate safes. PED Keys and Cryptographic Modules are retrieved and used always under 2-person control. The Private Key is activated by the use of the PED Key during a Key Generation ceremony.

Subscribers must protect their Private Key from unauthorized use with a strong password, whose constraints are consistent with FIPS 140-2 level 3 or higher validated Cryptographic Modules. Subscribers of Business Certificates are instructed to protect their Private Key from unauthorized use with a strong password. Subscribers are obligated by contract and by this CP-CPS to authenticate to the module before the activation of the Private Key, as well as to protect the password or other data used to activate it from disclosure.

6.2.9 Method of Deactivating Private Key

IdenTrust and CSA Cryptographic Modules when active are not exposed to unauthorized access. The modules are maintained in the Secure Room which requires 2-person control. In addition, the modules are enclosed in locked steel cabinets. When not in use, a module is deactivated via logout procedures, removed, and stored in accordance with Section 5.2.2.

Subscribers are notified of their obligation to not leave their Cryptographic Modules unattended or

open to unauthorized access while active. Subscribers are required to deactivate the modules either by a manual logout or by configuring a passive timeout that does it automatically.

6.2.10 Method of Destroying Private Key

Upon expiration or Revocation of a CA, CSA, or RA System Certificate, or other termination of use of the signature Private Key, all copies of the signature Private Key are securely destroyed by IdenTrust personnel in Trusted Roles. When no longer needed, all Private Keys are destroyed in accordance with the FIPS 140-validated zeroize destruction method that is part of the Cryptographic Module's design (physical destruction of the Cryptographic Module is not required).

Subscribers are notified of their obligation to destroy their signing Private Keys and are provided instructions on zeroizing, re-initializing, or destroying the Cryptographic Modules when they are no longer needed, or when the Certificates to which they correspond are expired or revoked.

To ensure future access to encrypted data, Subscriber encryption Private Keys are secured in long-term backups by IdenTrust.

6.2.11 Cryptographic Module Rating

Requirements for Cryptographic Modules are as stated above in Section 6.2.1.

6.3 Other Aspects of Key PAIR Management

6.3.1 Public Key Archival

No stipulation.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, shall represent an additional day. For this reason, Subscriber Certificates should not be issued for the maximum permissible time by default, in order to account for such adjustments.

IdenTrust Certificates and corresponding Keys Pairs have maximum Validity Periods as follows:

TrustID Certificated Operational and Key Usage Periods

Key Type	Private Key Usage Period(*)	Certificate Lifetime
Root CA	No stipulation	Up to 25 years
Subordinate CAs - Not cross-signed	No stipulation	Up to 15 years
Subordinate CAs - Cross-signed	No stipulation	Up to 5 years
CSA OCSP Responder	No stipulation	Up to 3 years
End Entity	No stipulation	See Note below

***** Subscriber Key Pair must be replaced in accordance with the provisions of Section 3.3.

Note:

- Up to 398 days when issued before March 15, 2026
- Up to 200 days when issued on or March 15, 2026
- Up to 100 days when issued on or after March 15, 2027
- Up to 47 days when issued on or after March 15, 2029

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

A pass-phrase, PIN, or other Activation Data is used to protect access to the Private Keys used by IdenTrust or Subscribers.

IdenTrust uses a manually-held Key share PED and PED Keys to activate its Private Keys for CAs and CSAs. The Activation Data meets the requirements of FIPS 140-2 level 3 or higher validated Cryptographic Module. The PED and PED Keys are held in the Secure Room under the 2-person controls to enforce Split-Knowledge Technique.

Subscribers are instructed to use strong passwords in accordance with the FIPS 140 guideline in accordance with the level of the Cryptographic Module.

6.4.2 Activation Data Protection

Activation Data for Cryptographic Modules used by CAs and CSAs are protected by keeping the PED Keys in separate safes inside of the Secure Room. Access to the Secure Room requires 2 Individuals in Trusted Roles. Access to the content in the safe requires a password and a Key, each one held by a different Individual to enforce Split-Knowledge Technique.

When Activation Data is in the form of a PIN or password, LRAs, Enterprise RAs, Subscribers and PKI Sponsors are notified of their obligation to protect Activation Data as follows:

- It should be memorized, not written down;
- If written down, it must be secured at the level of the data that the associated Cryptographic Module is used to protect, and will not be stored with the Cryptographic Module; and
- Activation Data must never be shared with or disclosed to another Individual.

Alternatively, Activation Data could be biometric in nature.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

All IdenTrust CA Infrastructure Systems for all accounts capable of directly causing Certificate Issuance, including CA, CSA, and RA server side, incorporate proper user Identity Proofing methodology. This methodology includes the use of user ID/password, Private/Public Key, and/or biometrics authentication schemes, plus Multi-Factor Authentication where such is supported. The use and enforcement of password security are in accordance with the IdenTrust security Policy and supporting security guidelines.

The IdenTrust SSP describes the self-protection techniques for user authentication, any policies that provide for bypassing user authentication requirements, single-sign-on technologies (host-to-host authentication servers, user-to-host identifier, and group user identifiers), and any compensating controls.

IdenTrust provides technical access controls designed to provide the least privilege and protections against unauthorized access to IdenTrust's CA Infrastructure System resources. Technical controls

are developed and implemented in accordance with best industry practices, federal law, regulations, and guidelines. IdenTrust describes its technical security controls in the SSP.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

For commercial off-the-shelf software, IdenTrust selects vendors that design and develop applications using formal development methodologies and as a consequence has received security certifications supporting their assertions.

IdenTrust develops some PKI software components. Standard development methodologies are used. Strict quality assurance is maintained throughout the process. Documentation is maintained supporting the process. Development and testing environments are maintained on separate servers in a separate network from the main operational environment with appropriate segregation rights restricting developers and testers from having access to production equipment.

When open source software is used, it is selected focusing on specific functionality, it goes through unit and integration testing on a controlled environment. Then, when it is used in development, the entire developed module goes through the standard change control process.

When utilizing third-party Linting software, IdenTrust monitors for updated versions of that software.

IdenTrust may perform Linting on the corpus of its unexpired, un-revoked Subscriber Certificates whenever it updates the Linting software.

6.6.2 Security Management Controls

IdenTrust has mechanisms in place to control and monitor the configuration of its CA, CSA, and internal RA Systems. IdenTrust installs its equipment and software in a controlled environment using a documented change control process. Software, when first loaded, is verified using file checksums provided by vendors at the file or file archive level. Upon installation time, and at least once every 24 hours, the integrity of the IdenTrust CA Infrastructure System must be validated.

Change control processes consist of a change control form that is processed, logged, and tracked for any changes to CA, CSA, and internal RA Systems, firewalls, routers, software, and other access controls. File modifications are controlled through the change control process. In this manner, IdenTrust can verify whether a change to the System has been evaluated for risk mitigation and authorized by management. Hashes for CA and CSA Systems files are recorded on installation and validated weekly thereafter as explained in the previous section. Host based intrusion detection is utilized to alert for changes to files. Notifications are monitored and are reviewed on a daily basis.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

IdenTrust equipment used for PKI activities shall adhere to the NetSec BR.

IdenTrust implements a multi-tiered network utilizing the principles of defense in depth including network segmentation, multi-tiered security including security and high security zones, and redundancy. This infrastructure contains firewalls, proxy servers, and intrusion detection systems; and permits only encrypted access via VPN, SSH, or equivalent-security tools.

Certificate Systems, and Security Support Systems are located in a combination of Security and High Security zones.

Any accounts, ports, or protocols added to the firewall configurations are documented, authorized, tested, and implemented in accordance with the IdenTrust System Security Plan and other IdenTrust policies and procedures. Firewalls are configured with a minimum number of accounts. Only services and protocols required to support CA, CSA and RA functions are enabled. Firewalls and Network Boundary Control devices are configured to allow access only by the addresses, ports, protocols, and commands required for the trustworthy provision of PKI services by such Systems. IdenTrust blocks all ports and protocols by default, and opens only the minimum necessary to enable CA, CSA, and RA functions. Any network software present on firewalls is required to their function. All CA, CSA, RA, and Repository computer Systems are located in a secure facility behind the previously mentioned multi-tiered infrastructure.

The IdenTrust CA Infrastructure is housed within a physically secured environment, with the Root CA system isolated on a separate physical network from all other CA components.

IdenTrust maintains a documented vulnerability management program designed to identify, assess, prioritize, and remediate vulnerabilities affecting certificate systems and supporting infrastructure in accordance with CA/Browser Forum Network Security Requirements. Vulnerabilities are evaluated based on severity, exploitability, asset criticality, and potential impact to the confidentiality, integrity, and availability of certificate services. Vulnerability resolution time shall be within:

Level	Time
Critical	7 days
High	30 days
Medium	60 days
Low	365 days

Any exceptions are assessed for risk and documented.

Recommended security patches to Certificate Systems are applied within six (6) months of the security patch's availability, unless IdenTrust documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

6.8 Time-stamping

The IdenTrust's CA system clock time is derived from multiple trusted third party time sources in accordance with applicable requirements and is used to establish time-stamps for the following:

- Initial validity time of a Certificate;
- Revocation of a Certificate;
- Posting of CRLs and CRL updates;
- OCSP responses; and
- System audit journal entries.

System time for servers providing CA and CSA services are updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every 60 minutes. Trusted external time sources operated by government agencies are used to maintain an average accuracy of one second or better.

Clock adjustments are auditable events listed with other events in the log available for auditors.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

IdenTrust meets the technical requirements set forth in Section 6.1.5 - Key Sizes, and Section 6.1.6 - Public Key Parameters Generation and Quality Checking.

IdenTrust Certificates are issued in accordance with the Certificate Profile guideline specified in this Section 7.

7.1.1 Version Number(s)

IdenTrust only issues X.509 Certificates, version 3 Certificates.

7.1.2 Certificate Content and Extensions

All TrustID Certificate contents and extensions are based on RFC 5280 and RFC 6818 when applicable.

7.1.2.1 Root CA Certificates

Root CA Certificate Profile

version: v3(2).
serialNumber: Unique non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature: See Section 7.1.3.2.
Issuer: Encoded value must be byte-for-byte identical to the encoded Subject.
validity: See Section 6.3.2.
***Subject*:** CN = Root Certificate name unique across all root Certificates issued by IdenTrust; O = IdenTrust; C = US.
subjectPublicKeyInfo: See Section 7.1.3.1.
signatureAlgorithm: Encoded value must be byte-for-byte identical to the *tbsCertificate.signature*.
authorityKeyIdentifier: Presence: Yes; Critical: No; Contains only the keyIdentifier field identical to the *subjectKeyIdentifer*.
basicConstraints: Presence: Yes; Critical: Yes; cA = true.
keyUsage: Presence: Yes; Critical: Yes; *digitalSignature, keyCertSign* and *cRLSign*.
subjectKeyIdentifier: Presence: Yes; Critical: No; Set as defined in Section 4.2.1.2 of RFC 5280.
extKeyUsage: Not present.
certificatePolicies: Not present.

7.1.2.2 Subordinate CA Certificates

7.1.2.2.1 Subordinate CA Certificates - Not cross-signed

version: v3(2).

serialNumber: Unique non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature: See Section 7.1.3.2.
Issuer: Must be byte-for-byte identical to the *subject* field of the Issuing CA.
validity: See Section 6.3.2.
Subject: **CN** = Subordinate CA's unique identifier name; **O** = Subordinate CA's Organization legal name or DBA; **OU** = {May} Subordinate CA's custom CA name; **C** = Two-letter ISO 3166-1 country code of Subordinate CA's Place of Business.
***subjectPublicKeyInfo*:** See Section 7.1.3.1.
signatureAlgorithm: Encoded value must be byte-for-byte identical to the *tbsCertificate.signature*.
authorityKeyIdentifier: Presence: Yes; Critical: No; Contains only the *keyIdentifier* field identical to the *subjectKeyIdentifer* field of the Issuing CA.
basicConstraints: Presence: Yes; Critical: Yes; cA = True; May contain the *pathlenConstraint* field.
certificatePolicies: Presence: Yes; Critical: No; Certificate Policy: Policy Identifier= anyPolicy {2.5.29.32.0}; Policy Qualifier Info: Policy Qualifier Id=id-qt-cps; Qualifier: HTTPS URL for the Issuing CA's Certificate Policy; Policy Qualifier Info:[3]; Policy Qualifier Id=User Notice; Qualifier: Notice Text=Subordinate CA text.
crlDistributionPoints: Presence: Yes; Critical: No; Contains the HTTP URL of the CA's CRL service.
keyUsage: Presence: Yes; Critical: Yes; *DigitalSignature*; *keyCertSign*; *cRLSign*.
subjectKeyIdentifier: Presence: Yes; Critical: No; Set as defined within in Section 4.2.1.2 of RFC 5280.
extKeyUsage: Presence: Yes; Critical: No; *id-kp-serverAuth*; *id-kp-clientAuth*[4].
authorityInformationAccess: Presence: Yes; Critical: No; May - *id-ad-ocsp* (OID 1.3.6.1.5.5.7.48.1): A HTTP URL of the Issuing CA's OCSP responder; *id-ad-caIssuers* (OID 1.3.6.1.5.5.7.48.2): A HTTP URL of the Issuing CA's certificate.
nameConstraints: Presence: May.

7.1.2.2.2 Subordinate CA Certificates - Cross-Signed

version: v3(2).
serialNumber: Unique non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature: See Section 7.1.3.2.
Issuer: Must be byte-for-byte identical to the *subject* field of the Issuing CA.
validity: See Section 6.3.2.
Subject: **CN** = Subordinate CA's unique identifier name; **O** = Subordinate CA's Organization legal name or DBA; **C** = Two-letter ISO 3166-1 country code of Subordinate CA's Place of Business.
subjectPublicKeyInfo: See Section 7.1.3.1.
signatureAlgorithm: Encoded value must be byte-for-byte identical to the ***tbsCertificate.signature***.
authorityKeyIdentifier: Presence: Yes; Critical: No; Contains only the ***keyIdentifier*** field identical to the *subjectKeyIdentifer* field of the Issuing CA.
basicConstraints: Presence: Yes; Critical: Yes; cA = True; May contain the *pathlenConstraint* field.
certificatePolicies: Presence: Yes; Critical: No; Certificate Policy: Policy Identifier= anyPolicy {2.5.29.32.0}.
crlDistributionPoints: Presence: Yes; Critical: No; Contains the HTTP URL of the CA's CRL service.
keyUsage: Presence: Yes; Critical: Yes; ***DigitalSignature***; ***keyCertSign***; ***cRLSign***.

[3]The ***Policy Qualifier Info-User Notice*** is not present on Certificates issued on or after September 15, 2023
[4]The ***id-kp-clientAuth*** *EKU* is optional in Subordinate Certificates issued before June 15, 2026, and is not present on Subordinate Certificates issued after that date.

subjectKeyIdentifier: Presence: Yes; Critical: No; Set as defined within in Section 4.2.1.2 of RFC 5280.
extKeyUsage: Presence: Optional; When present: Critical: No; ***id-kp-serverAuth***.
authorityInformationAccess: Presence: Yes; Critical: No; May - ***id-ad-ocsp*** (OID 1.3.6.1.5.5.7.48.1): A HTTP URL of the Issuing CA's OCSP responder; *id-ad-caIssuers* (OID 1.3.6.1.5.5.7.48.2): A HTTP URL of the Issuing CA's certificate.
nameConstraints: Presence: May.

7.1.2.3 End Entity Certificates

End Entity Certificate Profile

version: v3(2).
serialNumber: Unique non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature: See Section 7.1.3.2.
Issuer: Must be byte-for-byte identical to the *subject* field of the Issuing CA.
validity: See Section 6.3.2.
Subject: - Domain Validated (DV) - **CN** = {May}; when present, one owned/controlled Domain name derived from the ***subjectAltName***.
Subject: - Organization Validated (OV) - **CN** = {May}; when present, one owned/controlled Domain name derived from the ***subjectAltName***; **O** = Full legal name or DBA with full legal name in parenthesis of the entity controlling the **CN**; **C** = Two-letter ISO 3166-1 country code of Organization's Place of Business; **L** = City/locality name present if **S** is absent; **S** = State or province name present if **L** is absent.
Subject: - Extended Validation (EV) - **CN** = {May}; when present, one owned/controlled Domain name derived from the ***subjectAltName***; **O** = Full legal name or DBA with full legal name in parenthesis of the entity controlling the **CN**; **L** = City/locality name; **S** = State or province name; **C** = Two-letter ISO 3166-1 country code of Organization's Place of Business; ***serialNumber*** = Registration Number[5]; ***businessCategory*** = One of these values[6]; ***jurisdictionLocalityName*** = Information relevant to the jurisdiction of incorporation or registration.[7]; **jurisdictionStateOrProvinceName** = *Information relevant to the jurisdiction of incorporation or registration.*[8]; ***jurisdictionCountryName*** = Information relevant to the jurisdiction of incorporation or registration.[9].
subjectPublicKeyInfo: See Section 7.1.3.1.
signatureAlgorithm: Encoded value must be byte-for-byte identical to the *tbsCertificate.signature*.

[5] A Registration Number assigned by the Incorporating Agency / Registration Agency in the Jurisdiction of Incorporation / Registration. If the Incorporation Agency / Registration Agency does not provide a Registration Number, then the Date of Formation in any one of the common date formats will be included. If Date of Formation is not available for Government or Non-Commercial entities it will be indicated in the Subject.

[6] Private Organization, Government Entity, Business Entity, or Non-Commercial Entity.

[7] Country level: Include only country info (using ISO country code); do not include state, province, or locality.
State/province level: Include country (ISO code) and full state/province name; do not include locality.
Locality level: Include country (ISO code), full state/province name, and full locality name (if the state/province regulates local registration).

[8] Country level: Include only country info (using ISO country code); do not include state, province, or locality.
State/province level: Include country (ISO code) and full state/province name; do not include locality.
Locality level: Include country (ISO code), full state/province name, and full locality name (if the state/province regulates local registration).

[9] Country level: Include only country info (using ISO country code); do not include state, province, or locality.
State/province level: Include country (ISO code) and full state/province name; do not include locality.
Locality level: Include country (ISO code), full state/province name, and full locality name (if the state/province regulates local registration).

authorityInformationAccess: Presence: Yes; Critical: No; {May} - *id-ad-ocsp* (OID 1.3.6.1.5.5.7.48.1): A HTTP URL of the Issuing CA's OCSP responder *id-ad-caIssuers* (OID 1.3.6.1.5.5.7.48.2): A HTTP URL of the Issuing CA's certificate.
authorityKeyIdentifier: Presence: Yes; Critical: No; Contains only the *keyIdentifier* field identical to the *subjectKeyIdentifer* field of the Issuing CA.
certificatePolicies: Presence: Yes; Critical: No; Certificate Policy: Policy Identifier = One of these pairs: **TLS DV:** 2.23.140.1.2.1; 2.16.840.1.113839.0.6.5; **TLS OV:** 2.23.140.1.2.2; 2.16.840.1.113839.0.6.3; **TLS EV:** 2.23.140.1.1; 2.16.840.1.113839.0.6.9; Policy Qualifier Info: Presence: May; when present, it is included only in the policy information for the IdenTrust Policy OID and contains a single Policy Qualifier Id=id-qt-cps whose Qualifier is an HTTPS URL pointing to the Certificate Policy, Certification Practice Statement, or other online policy information provided by IdenTrust; no other policy qualifier is included[10].
extKeyUsage: Presence: Yes; Critical: No; *id-kp-serverAuth*, *id-kp-clientAuth*[11]
subjectAltName: Presence: Yes; Critical: No; dNSName fully qualified domain name(s) or wildcard name validated by the CA; or; iPAddress IPV4/IPV6 validated by the CA; when the *subject* field is an empty sequence, this extension is marked critical. Effective March 15, 2026, this extension must not contain a Domain Name that ends in an IP Address Reverse Zone Suffix.
nameConstraints: Presence: No.
keyUsage: Presence: Yes; Critical: Yes; *digitalSignature*; *keyEncipherment*[12].
basicConstraints: Presence: May; Critical: Yes; *cA* =False; ***pathLenConstraint*** must not be present.
crlDistributionPoints: Presence: Yes; Critical: No; Contains the HTTP URL of the CA's CRL service.
Signed Certificate Timestamp List: Presence: May; Critical: No; The Signed Certificate Timestamp List extension contents must be an OCTET STRING containing the encoded *SignedCertificateTimestampList*, as specified in Section 3.3. of RFC 6962; each *SignedCertificateTimestamp* included within the *SignedCertificateTimestampList* must be for a *PreCert LogEntryType* that corresponds to the current Certificate.
subjectKeyIdentifier: Presence: Yes; Critical: No; Set as defined within in Section 4.2.1.2 of RFC 5280.

7.1.2.4 OCSP Responder Certificates

OCSP Responder Certificate Profile

version: v3(2).
serialNumber: Unique non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature: See Section 7.1.3.2.
Issuer: Must be byte-for-byte identical to the ***subject*** field of the Issuing CA.
validity: *notBefore*: Minimum = One day prior to the time of signing; <Maximum= The time of signing; *notAfter*: Minimum= The time of signing; Maximum= unspecified.>
Subject: **CN** = Present; the content is an identifier for the certificate such that the certificate's name is unique across all certificates issued by IdenTrust **O** = CA Full legal name or DBA with full legal name in parenthesis of the entity controlling the CN; **C** = Two-letter ISO 3166-1 country code of Organization's Place of Business.

[10]Certificates issued before September 15, 2023 under earlier versions of this CP-CPS may also contain a Policy Qualifier ***Info-User*** Notice. The id-qt-cps Policy Qualifier is optional, consistent with the TLS Baseline Requirements, which mark policyQualifiers as NOT RECOMMENDED in Subscriber Certificates.
[11]The ***id-kp-clientAuth*** *EKU* is optional in Subscriber Certificates issued before March 15, 2027, and is not present Subscriber Certificates issued after that date.
[12]The ***keyEncipherment*** *keyUsage* is only present on RSA Certificates

subjectPublicKeyInfo: See Section 7.1.3.1.
signatureAlgorithm: Encoded value must be byte-for-byte identical to the *tbsCertificate.signature*.
authorityKeyIdentifier: Presence: Yes; Critical: No; Contains only the *keyIdentifier* field identical to the *subjectKeyIdentifer* field of the Issuing CA.
id-pkix-ocsp-nocheck: Presence: Yes; Critical: No; Must have an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500.
extKeyUsage: Presence: Yes; Critical: No; *id-kp-OCSPSigning*.
keyUsage: Presence: Yes; Critical: Yes: *digitalSignature*.
basicConstraints:_ Presence: May; Critical: Yes; *cA* =False; *pathLenConstraint* must not be present.
subjectKeyIdentifier: Presence: Yes; Critical: No; Set as defined within in Section 4.2.1.2 of RFC 5280.

7.1.3 Algorithm Object Identifiers

7.1.3.1 SubjectPublicKeyInfo

The ***AlgorithmIdentifier*** field within the ***SubjectPublicKeyInfo*** of IdenTrust Certificates matches exactly, byte for byte, one of the hexadecimal encodings defined Below:

7.1.3.1.1 RSA

Use the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters is to be present, and be an explicit null.

When encoded, the AlgorithmIdentifier for RSA keys must be byte-for-byte identical with the following hex-encoded bytes: 300d06092a864886f70d0101010500

7.1.3.1.2 ECDSA

Use the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters use the namedCurve encoding.

For P-256 keys, the namedCurve is secp256r1 (OID: 1.2.840.10045.3.1.7).
For P-384 keys, the namedCurve is secp384r1 (OID: 1.3.132.0.34).
For P-521 keys, the namedCurve is secp521r1 (OID: 1.3.132.0.35).

When encoded, the AlgorithmIdentifier for ECDSA keys must be byte-for-byte identical with the following hex-encoded bytes:

For P-256 keys, 301306072a8648ce3d020106082a8648ce3d030107. For P-384 keys, 301006072a8648ce3d020106052b81040022. For P-521 keys, 301006072a8648ce3d020106052b81040023.

7.1.3.2 Signature Algorithm Identifier

Objects signed by IdenTrust's CA Private Key conform to the one of these signature algorithms and encodings:

7.1.3.2.1 RSA

IdenTrust use one of the following signature algorithms and encodings. When encoded, the AlgorithmIdentifier are byte-for-byte identical with the specified hex-encoded bytes. - RSASSA-PKCS1-v1_5 with SHA-256: - Encoding: 300d06092a864886f70d01010b0500. - RSASSA-PKCS1-v1_5 with SHA-384: - Encoding: 300d06092a864886f70d01010c0500. -

RSASSA-PKCS1-v1_5 with SHA-512: - Encoding: 300d06092a864886f70d01010d0500. - RSASSA-PSS with SHA-256, MGF-1 with SHA-256, and a salt length of 32 bytes: - Encoding: 304106092a864886f70d01010a3034a00f300d06096086480165030402010500a11c301a06092a864886f70d010108300d06096086480165030402010500a203020120 - RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes: - Encoding: 304106092a864886f70d01010a3034a00f300d06096086480165030402020500a11c301a06092a864886f70d010108300d06096086480165030402020500a203020130 - RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes: - Encoding: 304106092a864886f70d01010a3034a00f300d06096086480165030402030500a11c301a06092a864886f70d010108300d06096086480165030402030500a203020140

7.1.3.2.2 ECDSA

IdenTrust shall use the appropriate signature algorithm and encoding based upon the signing key used.

If the signing key is P-256, the signature MUST use ECDSA with SHA-256. When encoded, the AlgorithmIdentifier MUST be byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040302.

If the signing key is P-384, the signature MUST use ECDSA with SHA-384. When encoded, the AlgorithmIdentifier MUST be byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040303.

If the signing key is P-521, the signature MUST use ECDSA with SHA-512. When encoded, the AlgorithmIdentifier MUST be byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040304.

7.1.4 Name Forms

Attribute values shall be encoded according to RFC 5280.

Certificates must not include metadata such as ‘.’, ‘-’, spaces, or any other indication that a value or field is absent, incomplete, or not applicable

The Issuing CA shall specify the format and content requirements for the names used in Certificates, including rules for Subject and issuer names, as well as any constraints or conventions for representing those names. By issuing TrustID Certificates, the IdenTrust CA represents that it followed the procedure set forth in this CP-CPS to verify that, as of the Certificate’s Issuance date, all of the Subject Information was accurate.

7.1.5 Name Constraints

IdenTrust may constrain the scope within which a Subordinate CA Certificate can Issue Certificates by using the Name Constraint extension.

Technically Constrained Subordinate CAs include the Extended Key Usage (EKU) extension that explicitly lists all the extended Key usages for which they are authorized to Issue Certificates. The anyExtendedKeyUsage KeyPurposeId is intentionally excluded from this extension.

7.1.6 Certificate Policy Object Identifier

IdenTrust, as the Issuing CA, includes at least one Policy OID in every Certificate it issues. Certificates issued under this CP-CPS shall contain one of the following sets of Policy OIDs:

TrustID Certificate Names, Types, and Policy OIDs		
Name	**Type**	**CA/Browser Forum OID / IdenTrust Policy OID**
Server Domain Validation	Server Authentication (DV)	2.23.140.1.2.1 / 2.16.840.1.113839.0.6.5\
Server Organization Validation	Server Authentication (OV)	2.23.140.1.2.2 / 2.16.840.1.113839.0.6.3\
Server Extended Validation	Server Authentication (EV)	2.23.140.1.1 / 2.16.840.1.113839.0.6.9\

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

Subscriber Certificates and Subordinate CA Certificates issued on or after September 15, 2023 shall not contain a User Notice policy qualifier[13]. Section 7.1.2.3 specifies the only policy qualifier permitted in Subscriber Certificates.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The Certificate policies extension specifies that the Certificate's usage is limited to one or more of the designated Certificate policies. The Certificate must be used strictly in accordance with the requirements of at least one of the listed policies.

7.2 CRL Profile

CRLs issued by IdenTrust comply with RFC 5280.

Minimally, IdenTrust issues either a “full and complete” CRL or a set of “partitioned” CRLs which cover the complete set of Certificates issued by the Issuing CA within 7 days of such CA issuing its first Certificate. When issuing only partitioned CRLs, the combined scope of those CRLs must be equivalent to that of a full and complete CRL.

7.2.1 Version Number(s)

IdenTrust issues version two (2) CRLs conforming to RFC 5280.

7.2.2 CRL and CRL Entry Extensions

Issuer: DN of issuer of CRL.
thisUpdate: The date and time when the Certificate revocation list validity begins.
nextUpdate: For Subordinate CAs: Up to ThisUpdate + 1 year; For Subscribers: Up to ThisUpdate + 10 days.
revokedCertificates: List of revoked Certificates, including the “Revoked Certificates Component” below.
CRLNumber: The serial number of this CRL in an incrementally increasing sequence of CRLs.
authorityKeyIdentifier: Is present and not marked critical; The *keyIdentifier* field is present and the value is identical to the *subjectKeyIdentifier* field of the Issuing CA.
CRLNumber: Present and not marked critical, containing an integer greater than or equal to zero (0) and less than 2^{159}, and convey a strictly increasing sequence.
issuingDistributionPoint: Used only on partitioned CRLs, marked critical.

[13] Policy Qualifier ***Info-User*** Notice is not present on Certificates issued on or after September 15, 2023

Revoked Certificates Component

serialNumber: Byte-for-byte identical to the serialNumber contained in the revoked Certificate.
revocationDate: The date and time revocation occurred. IdenTrust may update the revocation date in a CRL entry when it is determined that the Private Key of the Certificate was compromised prior to the revocation date that is indicated in the CRL entry for that Certificate.
crlEntryExtensions: Must include an RFC 5280 '*reasonCode*' field not marked critical, as follows:

- **0. *unspecified:*** Represented by the omission of a *reasonCode*. Must be omitted if the CRL entry is for a Certificate not technically capable of causing issuance;
- **1. *keyCompromise:*** Indicates that it is known or suspected that the Subscriber's Private Key has been compromised;
- **3. *affiliationChanged:*** Indicates that the Subject's name or other Subject identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised;
- **4. *superseded:*** Indicates that the Certificate is being replaced because: the Subscriber has requested a new Certificate, IdenTrust has reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the Certificate should not be relied upon, or IdenTrust has revoked the Certificate for compliance reasons;
- **5. *cessationOfOperation:*** Indicates that the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the Domain Name in the Certificate prior to the expiration of the Certificate;
- **6. *certificateHold:*** Must not be included;
- **9. *privilegeWithdrawn:*** Indicates that there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the Certificate Subscriber provided misleading information in their Certificate Request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

7.3 OCSP Profile

If an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that Certificate has been revoked, then the *revocationReason* field within the *RevokedInfo* of the *CertStatus* must be present.

The *CRLReason* indicated must contain a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1 Version Number(s)

The version number for requests and responses shall be version 1.

7.3.2 OCSP Extensions

IdenTrust OCSP services are operated in compliance with the standards defined in RFC 6960 and/or RFC 5019.

The *singleExtensions* field of an OCSP response does not include the *reasonCode* CRL entry extension (OID 2.5.29.21)

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

IdenTrust has a regularly scheduled compliance audit mechanism in place to ensure that the requirements of this CP-CPS and the CA/B Forum Baseline Requirements are implemented and enforced. IdenTrust's SSP describes how the security features and controls of its Systems are to be

tested and reviewed when significant modifications are made. IdenTrust is also subject to examination and the regulatory authority of the Office of the Comptroller of the Currency (OCC) under 12 U.SI § 867(c). IdenTrust's commercial practices are audited as required by the OCC and states where IdenTrust is licensed as a CA. Full or partial audit results may be released to the extent permitted by law, regulation, and contract or IdenTrust management.

8.1 Frequency or Circumstances of Assessment

The IdenTrust Issuing CA shall at all times:

1. Issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates;
2. Comply with the CA/B Forum Baseline Requirements;
3. Comply with the audit requirements set forth in this section; and

Be licensed as a CA in each jurisdiction where it operates, if licensing is required by the law of such jurisdiction for the issuance of Certificates.

IdenTrust has passed previous audits that have demonstrated compliance with this CP-CPS. IdenTrust may contract for periodic and aperiodic compliance audits or inspections of IdenTrust, Subordinate CA, or RA operations to validate that the subordinate entities are operating in accordance with the security practices and procedures described in the respective CPSs, Registration Practices Statements (RPSs), SSPs, and Privacy policies and Procedures (PPPs).

IdenTrust Operations related to its own CA, CSA and RA are audited annually against the criteria of the WebTrust Program for Certification Authorities. (WebTrust for CA), developed by the American Institute for Certified Public Accounts and CPA Canada (formerly the Canadian Institute of Chartered Accountants). These audits provide an unbroken sequence of Audit Periods that shall not exceed one year in duration.

Certificates that are capable of being used to issue new Certificates are either

1. Technically Constrained in line with Section 7.1.4 and audited in line with Section 8 only in regard to self-audits, or
2. unconstrained and fully audited in line with all remaining CA/Browser Forum Baseline Requirements.

A Certificate is deemed capable of being used to issue new Certificates if it contains an X.509v3 basicConstraints extension, with the cA boolean set to true and is therefore by definition a Root CA Certificate or a Subordinate CA Certificate.

Sponsoring Organizations with Enterprise RAs will produce the records necessary for a quarterly assessment of their server Certificates by the IdenTrust security office.

If the IdenTrust CA lacks a current audit report demonstrating compliance with one of the audit schemes listed in Section 8.4, it must complete a point-in-time readiness assessment under one of those schemes before issuing any Publicly-Trusted Certificates. This assessment must be conducted no more than twelve (12) months prior to issuing the first certificate and must be followed by a full audit under the same scheme within ninety (90) days of issuance.

8.2 Identity/Qualifications of Assessor

The IdenTrust CA's audit shall be performed by a Qualified Auditor.

To perform the compliance audit, IdenTrust engages the services of a professional auditing firm having the following qualifications:

1. **Focus and experience:** Auditing must be one of the firm's principal business activities. Moreover, the firm must have experience in auditing secure information systems and Public Key Infrastructures (PKI).
2. **Expertise:** The firm must have a staff of auditors trained and skilled in the auditing of secure information systems. The staff must be familiar with PKI, certification Systems, and the like, as well as Internet security issues (such as management of a security perimeter), operations of secure data centers, personnel controls, and operational risk management. The staff must be large enough to have the necessary depth and range of expertise required to audit IdenTrust's operations, or the Sponsoring Organizations with Enterprise RAs registration functions, in a competent manner.
3. **Reputation:** The firm must have a reputation for conducting its auditing business competently and correctly.
4. **Disinterest:** The firm has no financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against IdenTrust (or the RA being audited). In the case of a Sponsoring Organizations with Enterprise RAs internal auditing group, the auditing group must be independent of the group being audited.
5. **Rules and standards:** The firm must conform to applicable standards, rules, and best practices promulgated by the American Institute of Certified Public Accountants (AICPA), the Institute of Chartered Accountants of England and Wales (ICAEW), the International Accounting Standards adopted by the European Commission (IAS), Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), or another qualified auditing standards body, and must require its audit professionals to do the same.

In addition, the members of the firm's staff performing the audit are contractually subject to the following requirements:

1. **Professional qualifications:** Each external auditing professional performing the audit must be a member of the AICPA, CICA, ICAEW, ISSA, (ISC)2, IIA, or ISACA. In addition, at least one staff member must be qualified as a Certified Information Systems Auditor, AICPA Certified Information Technology Professional (CPA.CITP) or have another recognized information security auditing credential.
2. **Primary responsibility:** The external auditing professional assigned by the auditing firm to take the lead in the audit must have the audit as his or her primary responsibility until the audit is completed. That staff member and IdenTrust will agree on a project plan before beginning the audit to ensure that adequate staff, other resources, and time are provided.
3. **Conformity to professional rules:** Each external professional active in auditing IdenTrust must conform to the ethical and other professional rules of the AICPA, CICA, ICAEW, ISSA, (ISC)2, IIA, or ISACA or those of the applicable other qualified auditing standards body.
4. **Professional background:** The external professionals assigned to perform the audit must be trained to a standard generally accepted in the auditing field. They should also be familiar with PKI and other information security technologies and their secure operation. IdenTrust's operations are audited to ensure that IdenTrust conforms to this CP-CPS and familiarity with those documents is necessary for performing the audit for either IdenTrust or an RA. The auditor that IdenTrust has selected for past audits has in every case been one of the large, well-known auditing firms. IdenTrust expects to continue this practice while changing from time to time the specific firm selected and expects that its Assessor's Relationship to Assessed Entity

IdenTrust's compliance auditors are representatives from the OCC, independent security audit firms specializing in information systems and network security, and private, unaffiliated, and nationally recognized accounting firms.

IdenTrust has a contractual relationship with the auditing firm for the performance of the audit, but otherwise, auditors are independent, unrelated entities having no financial interest in each other. Auditors maintain a high standard of ethics designed to ensure impartiality and the exercise of independent professional judgment, subject to disciplinary action by their licensing bodies. The auditor(s) have no other relationships with IdenTrust or its officers and directors, including financial, legal, social, or other relationships that would constitute a conflict of interest.

IdenTrust will maintain these standards when conducting audits of Sponsoring Organizations with Enterprise RAs.

8.3 Assessor's Relationship to Assessed Entity

The Compliance Inspector(s) and IdenTrust establish a contractual relationship for the performance of the inspection to provide an unbiased, independent evaluation.

8.4 Topics Covered by Assessment

IdenTrust's engagement of its Qualified Auditors as specified in Section 8.2 requires them to audit IdenTrust's operations for conformity to this CP-CPS, and every Memorandum of Agreement (MOA) between IdenTrust and other PKIs, if any.

The IdenTrust CA undergoes its annual audit in accordance with the "WebTrust Principles and Criteria for Certification Authorities" v2.2 or newer, and either

- "WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security" v2.7 or newer; or
- "WebTrust Principles and Criteria for Certification Authorities – SSL Baseline" v2.8 or newer and "WebTrust Principles and Criteria for Certification Authorities – Network Security" v1.0 or newer.

incorporating periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of this audit scheme. See Section 5.4.

CA WebTrust is performed by an accredited public accountant or nationally recognized accounting firm and any Auditing Standard audit must be performed by a Certified Information Systems Auditor or a Certified Information Systems Security Professional.

Sponsoring Organizations with Enterprise RAs will comply with this CP-CPS, and their contracts with IdenTrust.

8.4.1 CA Assessment

IdenTrust undergoes a conformity assessment audit for compliance with these Requirements performed in accordance with the WebTrust for CAs v2.2 or newer" and "WebTrust for Certification Authorities – Network Security – Version 1.0 or newer schemes.

IdenTrust incorporates periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit is conducted by a Qualified Auditor, as specified in Section 8.2.

8.5 Actions Taken as a Result of Deficiency

For audits of IdenTrust operations, if the auditor finds discrepancies between how IdenTrust is designed or is being operated or maintained as a CA, the requirements of this CP-CPS, or any applicable MOAs, the following actions will be performed:

- The auditor will note the discrepancy;
- The auditor will notify the IdenTrust PMA about the discrepancy;
- The PMA will address any identified discrepancies with IdenTrust; and
- IdenTrust will correct any deficiencies noted during compliance reviews, as specified by the PMA or PMO including proposing a remedy and expected time for completion.

Also, if irregularities are found during OCC compliance audits, the OCC may require appropriate remedial action or terminate IdenTrust operations after appropriate notice to existing clients. The results of compliance audits will not be made public except as described in Section 8.6. Results of the C&A review will be made available to the IdenTrust PMA to approve or disapprove after consideration.

8.6 Communication of Results

The Audit Report shall state explicitly that it covers the relevant systems and processes used in the Issuance of all Certificates that assert one or more of the Policy identifiers listed in Section 7.1.6. IdenTrust shall make the Audit Report publicly available.

IdenTrust must make its Audit Report publicly available no later than three months after the end of the Audit Period. In the event of a delay more than three months, the CA shall provide an explanatory letter signed by the Qualified Auditor.

The results of IdenTrust's compliance audit and the C&A are fully documented, and reports resulting from it are submitted to the PMA within 30 calendar days of the date of their completion. Such reports will identify the CP, and/or and CP-CPS used in the assessment including their dates and version numbers.

IdenTrust posts its auditor's CA WebTrust certification on its website in accordance with applicable AICPA audit-reporting standards. Audit information that might pose an immediate threat of harm to Program Participants or that could potentially compromise the future security of IdenTrust's operations, is not made publicly available.

IdenTrust makes its Audit Report publicly available no later than 3 months after the end of the Audit Period. In the event of a delay greater than 3 months, and if so, requested by an Application Software Supplier, IdenTrust shall provide an explanatory letter signed by the Qualified Auditor.

8.7 Self-Audits

During the period in which the IdenTrust Issuing CA is actively issuing Certificates, IdenTrust conducts quarterly self-audits to ensure compliance with this CP-CPS and the CA/B Forum Baseline Requirements. Each audit reviews a randomly selected sample consisting of either one Certificate or at least three percent of the Certificates issued since the last audit, whichever is greater. To verify the technical accuracy of the selected Certificates, IdenTrust performs independent linting, regardless of any prior linting conducted on those Certificates.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Notice of any fee charged to a Subscriber or Authorized Relying Party must be brought to the attention of that entity.

9.1.1 Certificate Issuance or Renewal Fees

IdenTrust and RAs may establish and charge a reasonable TrustID Certificate Issuance fee for providing Identity Proofing, registration, and Certificate Issuance services to potential End Entities.

9.1.2 Certificate Access Fees

IdenTrust does not impose any Certificate access fees on Subscribers with respect to the content of their own TrustID Certificate(s) or the status of such TrustID Certificate(s).

9.1.3 Revocation or Status Information Access Fees

IdenTrust may establish and charge a reasonable fee for providing TrustID Certificate status information services. Fees will not be assessed for the CRL. Fees may be assessed for Certificate validation services via OCSP based upon Authorized Relying Party agreements negotiated between IdenTrust and the validating party.

9.1.4 Fees for Other Services

IdenTrust and RAs may establish and charge other reasonable fees. However, no fee may be charged for access to review the provisions of this CP-CPS. IdenTrust reserves the right to set any reasonable fees for any other services that it may offer.

9.1.5 Refund Policy

Refunds are not provided unless other arrangements are specifically made through Subscriber Agreements. Any fees collected for Certificate applications that are not approved will be refunded.

9.1.5.1 Monetary Amounts

All monetary values used in this Policy are in United States Dollars (USD).

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Unless otherwise provided in a separate writing or contract, IdenTrust maintains Commercial General Liability insurance and Professional Liability/Errors and Omissions insurance for a total maximum aggregate liability on all TrustID Certificates issued under this Policy and for all transactions relying on TrustID Certificates of up to 10 million USD.

Such insurance is maintained with a company rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies each of the members of which are so rated).

9.2.2 Other Assets

CAs and RAs shall maintain reasonable and sufficient financial resources to maintain operations, fulfill duties, and address commercially reasonable liability obligations to entities described in

Section 1.3.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Subject to any stipulations regarding the confidentiality of such information included in any applicable legal agreement between IdenTrust, CAs, RAs, LRAs, and Trusted Agents shall keep confidential all such labeled information they receive as part of fulfilling their responsibilities under this CP-CPS.

9.3.2 Information Not Within the Scope of Confidential Information

TrustID Certificates and related status information (including CRLs), or Organization information appearing in them or in public directories, are not considered confidential. Information contained on a single TrustID Certificate, and related status information, will not be considered confidential when the information is used in accordance with the purposes of providing CA services and carrying out the provisions of this CP-CPS. However, such information may not be used by any entity that is not an Authorized Relying Party or for any unauthorized purpose (e.g., mass, unsolicited emailing, junk email, spam, etc.). A TrustID Certificate should only contain information that is relevant and necessary to effect transactions with the Certificate.

9.3.3 Responsibility to Protect Confidential Information

9.3.3.1 Private Key Information

Private Keys are sensitive and confidential information and, therefore, Private Keys should be held in the strictest confidence. Under no circumstances will any Private Key appear unencrypted outside the Cryptographic Module

9.3.3.2 CA and RA Information

All non-public information stored locally on IdenTrust and/or RA equipment (not in the Repository) is considered confidential for the purposes of this CP-CPS. Access to this information will be restricted to those with an official need-to-know to perform their official duties. Any information pertaining to IdenTrust management of TrustID Certificates, such as compilations of Certificate information, shall be treated as confidential.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

IdenTrust publishes a privacy Policy providing information about IdenTrust's data protection practices at:

https://www.identrust.com/privacy.html.

9.4.1.1 Permitted Acquisition of Private Information

IdenTrust or the RA should collect only such personal information about an End Entity or

Sponsoring Organization that is necessary for the Issuance of a TrustID Certificate to the End Entity. For the purpose of proper administration of TrustID Certificates, IdenTrust or the RA may request non-Certificate information to be used in issuing and managing Certificates (e.g., identifying numbers, business or home addresses, and telephone numbers). However, such information will only be used for purposes of Certificate management and Issuance, unless otherwise permitted by the Subscriber. Collection of personal information may be subject to collection, maintenance, retention, and protection requirements of state and federal law.

9.4.1.2 Opportunity of Owner to Correct Private Information

End Entities must be given access and the ability to correct or modify their personal or Organization information. IdenTrust or the RA must provide this information on appropriate requests, but only after taking proper steps to authenticate the identity of the requesting party.

9.4.2 Information Treated As Private

Confidential information about Subscribers and their Subscribing Organization that is not publicly available in the contents of a Certificate, CRL, or in the LDAP Directory including information that links a Subject pseudonym to the real identity of a Subject Individual is considered private.

9.4.3 Information Not Deemed Private

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

9.4.3.1 Publication of Server Certificates

When applicable, IdenTrust complies with Certificate Transparency (CT) publishing new, renewed, and replaced TrustID server Certificates (DV, OV, and EV) into at least 3 public Certificate Transparency logs created for this purpose.

9.4.4 Responsibility to Protect Private Information

IdenTrust is responsible for protecting the confidentiality of private information that is in its possession, custody, or control with the same degree of care that it exercises with respect to its own information of like importance, but in no event less than reasonable care, and shall use appropriate safeguards and otherwise exercise reasonable precautions to prevent the unauthorized disclosure of private information.

IdenTrust requires the same from any service providers who handle private information on its behalf.

See Section 9.3.2. for further details.

9.4.5 Notice and Consent to Use Private Information

PKI Service Providers will not disclose any information deemed confidential to any third party, except when:

- authorized by this CP-CPS;
- required to disclose by law, governmental rule or regulation, or court order; or
- when necessary to effect an appropriate use of a TrustID Certificate.

All requests for disclosure of information considered confidential under Section 9.4 must be made in writing. IdenTrust may choose to further define or restrict its disclosure of Certificate-related

information. Unless prohibited by law, a PKI Service Provider will give all interested persons or parties reasonable prior written notice before disclosing any information considered confidential under Section 9.4 Non-disclosure of confidential information will remain an obligation notwithstanding the status of a TrustID Certificate (current or revoked) or the status of IdenTrust.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Participants may be required to participate in, and bear financial responsibility for, a centrally administered Alternative Dispute Resolution (ADR) process as outlined in this CP-CPS.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

A Private Key will be treated as the sole property of the legitimate holder of the TrustID Certificate containing the corresponding Public Key. "TrustID" is registered in the U.S. Patent and Trademark Office as a mark of IdenTrust, Inc. and is used by IdenTrust Services, LLC with the permission of IdenTrust, Inc. This CP-CPS is the intellectual property of IdenTrust Services, LLC, protected by copyright and other law regarding intellectual property, and may be used only pursuant to a license or other express permission from IdenTrust Services, LLC and then only in accordance with the provisions of this CP-CPS. Any other use of the above without the express permission of the owner is strictly prohibited.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

By issuing a Certificate, the CA makes the Certificate warranties listed herein to the following Certificate Beneficiaries:

1. The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate;
2. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root CA Certificate in software distributed by such Application Software Supplier; and
3. All Relying Parties who reasonably rely on a Valid Certificate. IdenTrust represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, IdenTrust has complied with the TLS BR and this CP-CPS in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

1. **Right to Use Domain Name or IP Address:** That, at the time of Issuance, the CA:
    1. implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's *subject* field and *subjectAltName* extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control);
    2. followed the procedure when issuing the Certificate; and
    3. accurately described the procedure in the CA's CP, CPS and/or CP-CPS;
2. **Authorization for Certificate:** That, at the time of Issuance, the CA:

    1. implemented a procedure for verifying that the Subject authorized the Issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject;
    2. followed the procedure when issuing the Certificate; and
    3. accurately described the procedure in the CA's CP, CPS and/or CP-CPS;
3. **Accuracy of Information:** That, at the time of Issuance, the CA:
    1. implemented a procedure for verifying the accuracy of all of the information contained in the Certificate;
    2. followed the procedure when issuing the Certificate; and
    3. accurately described the procedure in the CA's CP, CPS and/or CP-CPS;
4. **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA:
    1. implemented a procedure to verify the identity of the Applicant in accordance with Section 3.2;
    2. followed the procedure when issuing the Certificate; and
    3. accurately described the procedure in the CA's CP, CPS and/or CP-CPS;
5. **Subscriber Agreement:** That, if IdenTrust and Subscriber are not Affiliated, the Subscriber and IdenTrust are parties to a legally valid and enforceable Subscriber Agreement that satisfies the TLS BR, or, if IdenTrust and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
6. **Status:** That IdenTrust maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
7. **Revocation:** That IdenTrust will revoke the Certificate for any of the reasons specified in the Section 4.9.1.

The Root CA shall be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with the TLS BR, and for all liabilities and indemnification obligations of the Subordinate CA under the TLS BR, as if the Root CA were the Subordinate CA issuing the Certificates.

IdenTrust as the Issuing CA adheres to above listed warranties.

Such warranties shall be made as of:

1. the time of the Subscriber's Acceptance of the TrustID Certificate; and
2. the time that the Subscriber's TrustID Certificate is used during its Operational Period.

9.6.1.1 Authorized Relying Party Warranties

An Issuing CA may provide a validation warranty to an Authorized Relying Party for a per transaction amount for transactions in which the Authorized Relying Party exercises Reasonable Reliance on a TrustID Certificate. In such instances, the Issuing CA warrants that:

- The Issuing CA has issued and managed the TrustID Certificate in accordance with this Policy;
- The Issuing CA complied with the requirements of this CP-CPS when verifying the identity of the Subscriber;
- There are no material misrepresentations of fact in the TrustID Certificate known to the Issuing CA, and the Issuing CA has taken steps as required under this Policy to verify the information contained in the TrustID Certificate;
- The Issuing CA has taken all steps required by this Policy to ensure that the Subscriber's submitted information has been accurately transcribed to the TrustID Certificate;

- Information provided by the Issuing CA concerning the current validity of the TrustID Certificate is accurate and that validity has not been diminished by the Issuing CA's failure to promptly revoke the TrustID Certificate in accordance with Section 4.9; and;
- The TrustID Certificate meets all material requirements of this CP-CPS.

These warranties apply to any Authorized Relying Party who:

1. relies on a TrustID Certificate in an electronic transaction in which the TrustID Certificate played a material role in verifying the identity of one or more persons or devices;
2. exercises Reasonable Reliance on that TrustID Certificate; and
3. follows all procedures required by this Policy and by the applicable Authorized Relying Party Agreement for verifying the status of the TrustID Certificate.

These warranties are made to the Authorized Relying Party as of the time the Repository is referenced to determine TrustID Certificate validity, and only if the TrustID Certificate is valid and not revoked at that time

IdenTrust, in its sole discretion, may provide a validation warranty as described above to an Authorized Relying Party by expressly including such a warranty in the applicable Authorized Relying Party Agreement.

9.6.2 RA Representations and Warranties

IdenTrust must ensure that all its RAs comply with all the relevant provisions of this CP-CPS. IdenTrust shall continue to be responsible for any matters delegated to an RA, although an IdenTrust and an RA may enter into an indemnification agreement in accordance with Section 9.6.

9.6.3 Subscriber Representations and Warranties

IdenTrust shall require, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.

Prior to the Issuance of a Certificate, the CA shall obtain, for the express benefit of the CA and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with the CA, or
2. The Applicant's acknowledgement of the Terms of Use.

IdenTrust shall implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement must apply to the Certificate to be issued pursuant to the Certificate Request. IdenTrust may use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement may be used for each Certificate Request, or a single Agreement may be used to cover multiple future Certificate Requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use.

The Subscriber Agreement or Terms of Use must contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to the CA, both in the Certificate Request and as otherwise requested by the CA in connection with the Issuance of the Certificate(s) to be supplied by the CA;

2. **Protection of Private Key:** An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated Activation Data or device, e.g., Password or Token);
3. **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. **Use of Certificate:** An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
5. **Reporting and Revocation:** An obligation and warranty to:
    1. promptly request Revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and
    2. promptly request Revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
6. **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon Revocation of that Certificate for reasons of Key Compromise.
7. **Responsiveness:** An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. **Acknowledgment and Acceptance:** An acknowledgment and Acceptance that the CA is entitled to revoke the Certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if Revocation is required by the CA's CP, CPS, or the CA/B Forum Baseline Requirements.

IdenTrust Subscriber Agreement contains provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the obligations and warranties listed above.

9.6.4 Relying Party Representations and Warranties

Before relying on or using a TrustID Certificate issued under this CP-CPS, an Authorized Relying Party is obligated to:

9.6.4.1 Use of Certificates for Appropriate Purpose

Ensure that the TrustID Certificate and intended use are appropriate under the provisions of this CP-CPS, and the applicable Authorized Relying Party Agreement;

9.6.4.2 Verification Responsibilities

Use the TrustID Certificate only in accordance with the certification path validation procedure specified in X.509 and PKIX;

9.6.4.3 Revocation Check Responsibility

Check the status of the TrustID Certificate by Online Status Check or against the appropriate and current CRL, as applicable, in accordance with the requirements stated in Section 4.10;

9.6.4.4 Reasonable Reliance

For Digital Signatures created during the Operational Period of a TrustID Certificate, an Authorized Relying Party has a right to rely on the Certificate only under circumstances constituting Reasonable Reliance as defined in Section 1.6.1;

9.6.4.5 Consequences of Relying on Revoked Certificate

If an Authorized Relying Party relies on a TrustID Certificate that was expired or that the Authorized Relying Party knew or should have known was revoked at the time of reliance (e.g., a decision to rely on a revoked TrustID Certificate based on the reasons for Revocation, information from other sources, or specific business considerations pertaining to the Authorized Relying Party), the Authorized Relying Party does so at its own risk and, in so relying, waives any warranties that any PKI Service Provider may have provided;

9.6.4.6 Consequences of Breach

An Authorized Relying Party found to have acted in a manner counter to these obligations will forfeit all claims he, she or it may have against any PKI Service Providers; and

9.6.4.7 Other Agreements

Without forming any limitation on any provisions of this CP-CPS, an Authorized Relying Party's obligations will be governed by the Authorized Relying Party Agreement between the Authorized Relying Party and IdenTrust.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimer of Warranties

EXCEPT FOR THOSE WARRANTIES EXPRESSLY PROVIDED IN THIS CP-CPS OR THAT MAY BE EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT BY IDENTRUST, IDENTRUST:

1. DISCLAIMS ANY AND ALL OTHER WARRANTIES OF ANY TYPE, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY, CORRECTNESS OR ACCURACY OF INFORMATION PROVIDED, OR FITNESS FOR A PARTICULAR PURPOSE; AND
2. THAT ITS SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR FREE, OR THAT DEFECTS WILL BE CORRECTED.

IDENTRUST MAKES NO WARRANTY THAT ANY IDENTRUST SERVICES WILL MEET ANY EXPECTATIONS.

The foregoing provisions of Section 9.6.1 shall not form any limitation on any limitations or disclaimers of IdenTrust, set forth under other provisions of this CP-CPS, or any agreement between IdenTrust and an End Entity. Further, the provisions of Section 9.6.1 may be limited by applicable law, in which case such provisions shall be construed to apply to the maximum possible extent permissible under such law.

If IdenTrust's performance of any obligation under this CP-CPS is prevented or delayed by an event beyond such IdenTrust's reasonable control, including without limitation, crime, fire, flood, war, terrorism, riot, acts of civil or military authority (including governmental priorities), severe weather, strikes or labor disputes, or by disruption of telecommunications, power or Internet services not caused by such IdenTrust, then IdenTrust will be excused from such performance to the extent it is necessarily prevented or delayed thereby.

9.8 Limitations of Liability

This CP-CPS establishes an open-but-bounded PKI. PKI Service Providers will not be liable to any person who relies upon a Certificate unless such liability is clearly established by contract, special warranty, or law.

UNLESS OTHERWISE SPECIFIED IN THIS SECTION 9.8, IDENTRUST WILL NOT BE LIABLE TO YOU UNDER ANY CIRCUMSTANCES WITH RESPECT TO ANY SUBJECT MATTER HEREOF UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY, OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE OR EXEMPLARY DAMAGES OF ANY KIND (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUE OR GOODWILL OR ANTICIPATED PROFITS OR LOST BUSINESS), REGARDLESS OF WHETHER IDENTRUST KNEW OR HAD REASON TO KNOW OF THE POSSIBILITY THEREOF.

In addition to any other provisions of this CP-CPS, or an applicable agreement between IdenTrust and an End Entity, the liability of IdenTrust shall be limited as described below:

Except with respect to TrustID EV Certificates and unless otherwise provided in a separate writing or contract, the total, maximum, aggregate liability of an Issuing CA or RA for all TrustID Certificates issued under this Policy and for all transactions relying on TrustID Certificates is $10,000,000

Except with respect to the TrustID EV Certificate and unless otherwise provided in a separate contract executed by an officer of IdenTrust Services, LLC, the maximum potential liability for an Issuing CA or RA to any Authorized Relying Party with respect to anyone TrustID Certificate upon which the Authorized Relying Party relies will be limited to:

1. $100,000 per transaction, and
2. $250,000 for all transactions in which the Authorized Relying Party relies on the TrustID Certificate.

With respect to relying on any single TrustID EV Certificate, the maximum aggregate liability for an Issuing CA or RA to any Relying Party or Subscriber will be limited to $2,000 per Subscriber or Relying Party per TrustID EV Certificate.

UNLESS OTHERWISE SPECIFIED IN THIS SECTION, IDENTRUST WILL NOT BE LIABLE TO YOU UNDER ANY CIRCUMSTANCES WITH RESPECT TO ANY SUBJECT MATTER HEREOF UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY, OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE OR EXEMPLARY DAMAGES OF ANY KIND (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUE OR GOODWILL OR ANTICIPATED PROFITS OR LOST BUSINESS), REGARDLESS OF WHETHER IDENTRUST KNEW OR HAD REASON TO KNOW OF THE POSSIBILITY THEREOF.

9.9 Indemnities

Neither IdenTrust nor its agents assume financial responsibility for improperly used Certificates.

Without forming any limitation on any other provision of this CP-CPS or any agreement between IdenTrust and an End Entity:

1. a Relying Party under an IdenTrust TrustID Relying Party Agreement shall indemnify IdenTrust under the applicable terms and conditions of any indemnification provision therein; and
2. a Subscriber under an IdenTrust TrustID Subscriber Agreement shall indemnify IdenTrust under the applicable terms and conditions of any indemnification provision therein.

Notwithstanding any limitations on its liability to Subscribers and Authorized Relying Parties, IdenTrust understands and acknowledges that the Application Software Suppliers who have a Root CA Certificate distribution agreement in place with IdenTrust do not assume any obligation or potential liability of IdenTrust under the TLS Baseline Requirements or that otherwise might exist because of the Issuance or maintenance of TrustID Certificates or reliance thereon by Authorized Relying Parties or others. IdenTrust will defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a TrustID Certificate issued by IdenTrust, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a TrustID Certificate issued by IdenTrust where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a TrustID Certificate that is still valid or displaying as trustworthy:
(1) a TrustID Certificate that has expired, or
(2) a TrustID Certificate that has been revoked (but only in cases where the Revocation status is currently available from IdenTrust online, and the application software either failed to check such status or ignored an indication of revoked status).

9.10 Term and Termination

9.10.1 Term

This CP-CPS shall remain in effect until a new CP-CPS is approved by the IdenTrust PMA or termination of this CP-CPS is communicated via the IdenTrust's Repository.

9.10.2 Termination

The requirements of this CP-CPS remain in effect through the end of the archive period for the last Certificate issued. The conditions and effects resulting from the termination of this CP-CPS are communicated via IdenTrust's Repository.

9.10.3 Effect of Termination and Survival

The conditions and effects resulting from termination of this CP-CPS will be communicated via IdenTrust's Repository upon termination outlining the provisions that may survive termination of the document and remain in force. The responsibilities for protecting business confidential and private personal information shall survive termination, and the terms and conditions for all existing Certificates shall remain valid for the remainder of the Validity Periods of such Certificates.

9.11 Individual Notices and Communications with Participants

All parties shall use commercially reasonable methods to communicate with each other. All communication among Participants shall be in writing or via Digitally Signed communication. If in writing, the communication shall be signed on the appropriate Organization letterhead. If electronic, a Digital Signature shall be made using a Private Key whose companion Public Key is certified using a Certificate meeting the requirements set in this CP-CPS.

9.11.1 Notices by Individual Participants to IdenTrust

Notices by Individual Participants to IdenTrust shall be made by at least one of the following methods, with the choice between methods to be made by the Participant:

1. by Digitally Signed communication sent from the Participant to IdenTrust via email to Registration@IdenTrust.com, which communication will be deemed effective when acknowledged via email by IdenTrust; or
2. by written communication sent from the Participant to IdenTrust via internationally recognized overnight courier to IdenTrust Registration, 5225 Wiley Post Way, Suite 450, Salt Lake City, UT 84116, which such communication will be deemed effective when delivered as evidenced by written confirmation of receipt as recorded by the courier.

9.11.2 Notices by IdenTrust to Individual Participants

Notices by IdenTrust to Individual Participants shall be made by at least one of the following methods, with the choice between methods to be made by IdenTrust:

- by Digitally Signed communication sent from IdenTrust to the Participant via email to any Email Address of the Participant submitted to IdenTrust during the Participant's registration, contracting, or Certificate lifecycle maintenance interactions with IdenTrust, which communication shall be deemed effective when sent by IdenTrust; or
- by written communication sent from IdenTrust to Participant via U.S. Postal Service mail of the first class to any physical address of Participant that Participant submitted to IdenTrust during the Participant's registration, contracting, or Certificate lifecycle maintenance interactions with IdenTrust.

9.11.3 Notices Delivery Method

The method(s) of providing notice between each CA (other than IdenTrust) and Participants (other than IdenTrust) shall be set forth in the CA's CPS or CP-CPS, provided that at a minimum the CA must provide a physical address at which notice by via internationally recognized overnight courier will be deemed effective when delivered as evidenced by written confirmation of receipt as recorded by the courier.

9.12 Amendments

This CP-CPS is reviewed by IdenTrust PMA at least annually. Errors, updates, or suggested changes to this CP-CPS should be communicated to the contact mentioned in Section 1.5.2. Such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.1 Procedure for Amendment

For an amendment of this CP-CPS to become effective, it must first be approved by the IdenTrust PMA in accordance with Section 1.5.4. Amendments in the CP-CPS will most frequently reflect amendments and timing driven by the CP-CPS changes, typically once a year in accordance with the CP-CPS. Changes that may materially affect Subscribers or Relying Parties are subject to a public comment period before consideration by the IdenTrust PMA. Other amendments such as editorial or typographical corrections, changes to the contact details, or other such minor changes will not be submitted to IdenTrust PMA and no comment period will be necessary.

After the PMA accepts changes, IdenTrust's PMA Chair will submit the document for final preparation and publication. Before publication, the document is redacted for sensitive information that can post security risks. The redacted document is the Public CP-CPS version. The final and accepted copy of this CP-CPS, as amended to date, is Digitally Signed by the chair of the IdenTrust PMA and archived securely. The redacted copy is posted online for reference and downloading by Relying Parties, Subscribers, and the general public.

IdenTrust may employ additional safeguards to ensure adequate version control over the authoritative text of this CP-CPS and ensure that the authenticity of that text is verifiable.

Audits of IdenTrust operations are conducted according to the original and Digitally Signed version in effect during the time of the operations in question, but subsequent and previous versions are available to the auditors for reference, as necessary.

9.12.2 Notification Mechanism and Period

IdenTrust will notify interested Participants of proposed changes, the final date for receipt of comments, and the proposed effective date of the change. Comments may be filed with IdenTrust within the comment period. Decisions with respect to the proposed changes are at the sole discretion of IdenTrust.

A copy of this CP-CPS is available in electronic form on the internet at https://www.identrust.com/support/documents/trustid

9.12.3 Circumstances under Which OID Must Be Changed

OIDs will be changed in this CP-CPS if the PMA determines that a change is required.

9.13 Dispute Resolution Provisions

9.13.1 Specific Provisions/ Incorporation of Policy

IdenTrust must ensure that its agreements with RAs and End Entities contain appropriate provisions that

- incorporate the provisions of this CP-CPS by reference, or
- provide to the respective contracting parties the protections established by this CP-CPS.

9.14 Governing Law

The enforceability, construction, interpretation, and validity of this CP-CPS will be governed by the laws of the United States of America and the law of the State of Utah, without regard to its conflicts of law principles.

9.15 Compliance with Applicable Law

This CP-CPS shall be subject to applicable national, state, local, and foreign laws, rules, regulations, ordinances, decrees, and orders including but not limited to restrictions on exporting or importing software, hardware, or technical information.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CP-CPS shall constitute the entire understanding and agreement between the parties with respect to the transactions contemplated and supersedes any and all prior or contemporaneous oral or written representation, understanding, agreement, or communication concerning the subject matter hereof. No party is relying upon any warranty, representation, assurance, or inducement not expressly set forth herein and none shall have any liability in relation to any representation or other assurance not expressly set forth herein unless it was made fraudulently. Without prejudice to any liability for fraudulent misrepresentation, no party shall be under any liability or shall have any remedy in respect of misrepresentation or untrue statement unless and to the extent that a claim lies for breach of a duty set forth in this CP-CPS.

9.16.2 Assignment

Except where specified by other contracts, Participants may not assign any of their rights or obligations under this CP-CPS or applicable agreements without the written consent of IdenTrust.

9.16.3 Severability

Should it be determined that one section of this CP-CPS is incorrect or invalid, the other sections of this CP-CPS shall remain in effect until the CP-CPS is updated. The process for updating this CP-CPS is described in Section 9.12.1.

In the event IdenTrust becomes aware of a conflict between the CP-CPS and a law, regulation, or government order (hereinafter 'Law') of any jurisdiction in which IdenTrust operates or issues TrustID Certificates, IdenTrust will modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction.

This applies only to operations or Certificate Issuances that are subject to that Law. In such an event, IdenTrust will immediately (and before issuing a TrustID Certificate under the modified requirement) include in this section a detailed reference to the Law requiring a modification of this CP-CPS under this section and the specific modification to this CP-CPS implemented by IdenTrust. IdenTrust will also (before issuing a TrustID Certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CP-CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the public mailing list and is indexed in the public mail archives available at https://cabforum.org (or such other Email Addresses and links as the CA/B Forum may designate), so that the CA/Browser Forum may consider possible revisions to the TLS BR accordingly.

Any modification to IdenTrust practice enabled under this section will be discontinued if and when the Law no longer applies, or this CP-CPS is modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to this CP-CPS, and a notice to the CA/Browser Forum, as outlined above, will be made within 90 days.

9.16.4 Enforcement (Attorney Fees and Waiver of Rights)

No waiver of any breach or default or any failure to exercise any right hereunder shall be construed as a waiver of any subsequent breach or default or relinquishment of any future right to exercise such right. The headings in this CP-CPS are for convenience only and cannot be used in interpreting this CP-CPS.

Except where an express time frame is set forth in this CP-CPS, no delay or omission by any PKI Participant to exercise any right, remedy, or power it has under this CP-CPS shall impair or be construed as a waiver of such right, remedy, or power. A waiver by any party of any breach of this CP-CPS shall not be construed to be a waiver of any other or repeated breach of this CP-CPS. Bilateral agreements between PKI Service Providers and other PKI Participants may contain additional provisions governing enforcement; provided, however, that in no event can such additional provisions alter the rights of IdenTrust hereunder.

9.16.5 Force Majeure

IDENTRUST SHALL NOT INCUR LIABILITY IF IT IS PREVENTED, FORBIDDEN, OR DELAYED FROM PERFORMING, OR OMITS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF:

- ANY PROVISION OF ANY APPLICABLE LAW, REGULATION OR ORDER;
- CIVIL, GOVERNMENTAL OR MILITARY AUTHORITY;
- THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER SYSTEM OPERATED BY ANY OTHER PARTY OVER WHICH IDENTRUST HAS NO CONTROL;
- FIRE, FLOOD, OR OTHER EMERGENCY CONDITION;
- STRIKE;
- ACTS OF TERRORISM OR WAR;
- ACT OF GOD; OR
- OTHER SIMILAR CAUSES BEYOND ITS REASONABLE CONTROL.

9.17 Other Provisions

No stipulation.