



# **TrustID<sup>®</sup>**

## **Certification Practice Statement**

**IdeaTrust Services LLC.**

**Version 4.9.2**

**December 04, 2024**

## Table of Contents

1	INTRODUCTION .....	11
1.1	OVERVIEW .....	11
1.2	DOCUMENT NAME AND IDENTIFICATION.....	12
1.2.1	Alphanumeric Identifier .....	15
1.2.2	Object Identifier .....	16
1.3	PKI PARTICIPANTS.....	17
1.3.1	Certification Authorities.....	17
1.3.2	Registration Authorities .....	18
1.3.3	Subscribers .....	19
1.3.4	Relying Parties.....	20
1.3.5	Other Participants .....	20
1.4	CERTIFICATE USAGE.....	21
1.4.1	Appropriate Certificate Uses.....	21
1.4.2	Prohibited Certificate Uses .....	23
1.5	POLICY ADMINISTRATION .....	24
1.5.1	Organization Administering this CPS Document.....	24
1.5.2	Contact Person .....	24
1.5.3	Person Determining CPS Suitability for the Policy .....	24
1.5.4	CPS Approval Procedures.....	24
1.6	DEFINITIONS AND ACRONYMS .....	25
1.6.1	Definitions .....	25
1.6.2	Acronyms .....	40
1.6.3	References.....	42
1.6.4	Conventions .....	42
2	PUBLICATION AND REPOSITORY RESPONSIBILITIES.....	43
2.1	REPOSITORIES.....	43
2.2	PUBLICATION OF CERTIFICATION INFORMATION .....	43
2.2.1	Interoperability .....	43
2.3	TIME OR FREQUENCY OF PUBLICATION .....	44
2.4	ACCESS CONTROLS ON REPOSITORIES .....	44
3	IDENTIFICATION AND AUTHENTICATION.....	45
3.1	NAMING.....	45

3.1.1	Types of Names .....	45
3.1.2	Need for Names to Be Meaningful .....	46
3.1.3	Anonymity or Pseudonymity of Subscribers .....	47
3.1.4	Rules for Interpreting Various Name Forms .....	47
3.1.5	Uniqueness of Names .....	48
3.1.6	Recognition, Authentication, and Role of Trademarks .....	49
3.2	INITIAL IDENTITY VALIDATION .....	50
3.2.1	Method to Prove Possession of Private Key .....	51
3.2.2	Authentication of Organization Identity .....	52
3.2.3	Authentication of Individual Identity .....	64
3.2.4	Non-Verified Subscriber information .....	72
3.2.5	Validation of Authority .....	72
3.2.6	Criteria for Interoperation .....	72
3.3	IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS .....	76
3.3.1	Identification and Authentication for Routine Re-key .....	76
3.3.2	Identification and Authentication for Re-Key after Revocation .....	76
3.4	IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS .....	77
4	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS .....	78
4.1	CERTIFICATE APPLICATION .....	78
4.1.1	Who Can Submit a Certificate Application .....	78
4.1.2	Enrollment Process and Responsibilities .....	79
4.2	CERTIFICATE APPLICATION PROCESSING .....	83
4.2.1	Performing Identification and Authentication Functions .....	83
4.2.2	Approval or Rejection of Certificate Applications .....	84
4.2.3	Time to Process Certificate Applications .....	86
4.2.4	Final Cross-Correlation and Due Diligence .....	86
4.3	CERTIFICATE ISSUANCE .....	86
4.3.1	CA Actions During Certificate Issuance .....	87
4.3.2	Notification to Subscriber by the CA of Issuance of Certificate .....	90
4.4	CERTIFICATE ACCEPTANCE .....	91
4.4.1	Conduct Constituting Certificate Acceptance .....	91
4.4.2	Publication of the Certificate by the CA .....	91
4.4.3	Notification of Certificate Issuance by the CA to Other Entities .....	91

- 4.5 KEY PAIR AND CERTIFICATE USAGE .....91
  - 4.5.1 Subscriber Private Key and Certificate Usage .....91
  - 4.5.2 Relying Party Public Key and Certificate Usage.....92
- 4.6 CERTIFICATE RENEWAL.....92
  - 4.6.1 Circumstance for Certificate Renewal.....92
  - 4.6.2 Who May Request Renewal .....92
  - 4.6.3 Processing Certificate Renewal Requests .....92
  - 4.6.4 Notification of New Certificate Issuance to Subscriber .....93
  - 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate .....93
  - 4.6.6 Publication of the Renewal Certificate by the CA .....93
  - 4.6.7 Notification of Certificate Issuance by the CA to Other Entities.....93
- 4.7 CERTIFICATE RE-KEY .....93
  - 4.7.1 Circumstance for Certificate Re-Key .....93
  - 4.7.2 Who May Request Certification of a New Public Key .....93
  - 4.7.3 Processing Certificate Re-Keying Requests.....93
  - 4.7.4 Notification of New Certificate Issuance to Subscriber .....95
  - 4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate .....95
  - 4.7.6 Publication of the Re-Keyed Certificate by the CA.....95
  - 4.7.7 Notification of Certificate Issuance by the CA to Other Entities.....95
- 4.8 CERTIFICATE MODIFICATION.....95
  - 4.8.1 Circumstance for Certificate Modification.....95
  - 4.8.2 Who May Request Certificate Modification .....96
  - 4.8.3 Processing Certificate Modification Requests .....96
  - 4.8.4 Notification of New Certificate Issuance to Subscriber .....96
  - 4.8.5 Conduct Constituting Acceptance of a Modified Certificate .....96
  - 4.8.6 Publication of the Modified Certificate by the CA .....96
  - 4.8.7 Notification of Certificate Issuance by the CA to Other Entities.....96
- 4.9 CERTIFICATE REVOCATION AND SUSPENSION .....96
  - 4.9.1 Circumstances for Revocation .....96
  - 4.9.2 Who Can Request Revocation.....99
  - 4.9.3 Procedure for Revocation Request .....99
  - 4.9.4 Revocation Request Grace Period.....102
  - 4.9.5 Time Within Which CA Must Process the Revocation Request .....102

4.9.6	Revocation Checking Requirements for Relying Parties .....	103
4.9.7	CRL Issuance Frequency .....	103
4.9.8	Maximum Latency for CRLs .....	104
4.9.9	Online Revocation/Status Checking Availability .....	104
4.9.10	Online Revocation Checking Requirements .....	105
4.9.11	Other Forms of Revocation Advertisements Available .....	106
4.9.12	Special Requirements for Re-Key Compromise .....	106
4.9.13	Circumstances for Suspension .....	106
4.9.14	Who Can Request Suspension .....	106
4.9.15	Procedure for Suspension Request .....	106
4.9.16	Limits on Suspension Period .....	107
4.10	CERTIFICATE STATUS SERVICES .....	108
4.10.1	Operational Characteristics .....	108
4.10.2	Service Availability .....	108
4.10.3	Optional Features .....	109
4.11	END OF SUBSCRIPTION .....	109
4.12	KEY ESCROW AND RECOVERY .....	109
4.12.1	Key Escrow and Recovery Policy and Practices .....	109
4.12.2	Session Key Encapsulation and Recovery Policy and Practices .....	110
5	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS .....	111
5.1	PHYSICAL SECURITY CONTROLS .....	112
5.1.1	Site Location and Construction .....	113
5.1.2	Physical Access .....	114
5.1.3	Power and Air Conditioning .....	116
5.1.4	Water Exposures .....	116
5.1.5	Fire Prevention and Protection .....	116
5.1.6	Media Storage .....	116
5.1.7	Waste Disposal .....	117
5.1.8	Off-Site Backup .....	118
5.2	PROCEDURAL CONTROLS .....	118
5.2.1	Trusted Roles .....	118
5.2.2	Number of Persons Required per Task .....	126
5.2.3	Identification and Authentication for Each Role .....	126

- 5.2.4 Roles Requiring Separation of Duties..... 127
- 5.3 PERSONNEL CONTROLS ..... 128
  - 5.3.1 Qualifications, Experience, and Clearance Requirements ..... 128
  - 5.3.2 Background Check Procedures..... 129
  - 5.3.3 Training Requirements and Procedures..... 129
  - 5.3.4 Retraining Frequency and Requirements ..... 131
  - 5.3.5 Job Rotation Frequency and Sequence..... 131
  - 5.3.6 Sanctions for Unauthorized Actions..... 131
  - 5.3.7 Independent Contractor Requirements..... 132
  - 5.3.8 Documentation Supplied to Personnel ..... 132
- 5.4 AUDIT LOGGING PROCEDURES..... 132
  - 5.4.1 Types of Events Recorded ..... 132
  - 5.4.2 Frequency of Processing Log..... 141
  - 5.4.3 Retention Period for Audit Log ..... 141
  - 5.4.4 Protection of Audit Log ..... 142
  - 5.4.5 Audit Log Backup Procedures ..... 142
  - 5.4.6 Audit Collection System (Internal vs. External)..... 142
  - 5.4.7 Notification to Event-Causing Subject ..... 143
  - 5.4.8 Vulnerability Assessments ..... 143
- 5.5 RECORDS ARCHIVAL ..... 144
  - 5.5.1 Types of Records Archived ..... 144
  - 5.5.2 Retention Period for Archive ..... 145
  - 5.5.3 Protection of Archive ..... 145
  - 5.5.4 Archive Backup Procedures ..... 145
  - 5.5.5 Requirements for Times-Stamping of Records ..... 145
  - 5.5.6 Archive Collection System (Internal or External) ..... 145
  - 5.5.7 Procedures to Obtain and Verify Archive Information ..... 145
- 5.6 KEY CHANGEOVER ..... 146
- 5.7 COMPROMISE AND DISASTER RECOVERY ..... 146
  - 5.7.1 Incident and Compromise Handling Procedures ..... 146
  - 5.7.2 Computing Resources, Software, and/or Data Are Corrupted ..... 147
  - 5.7.3 Entity Private Key Compromise Procedures ..... 147
  - 5.7.4 Business Continuity Capabilities After a Disaster ..... 149

5.8	CA OR RA TERMINATION .....	150
5.8.1	Termination of RA .....	150
5.8.2	Termination of Contractual Relationship with a Sponsoring Organization with Enterprise RAs....	150
5.8.3	Termination of Issuer CA.....	151
5.8.4	Termination of Root CA.....	151
6	TECHNICAL SECURITY CONTROLS.....	152
6.1	KEY PAIR GENERATION AND INSTALLATION .....	152
6.1.1	Key Pair Generation .....	152
6.1.2	Private Key Delivery to Subscriber .....	153
6.1.3	Public Key Delivery to Certificate Issuer .....	154
6.1.4	CA Public Key Delivery to Relying Parties.....	155
6.1.5	Key Sizes .....	156
6.1.6	Public Key Parameters Generation and Quality Checking .....	156
6.1.7	Key Usage Purposes (as per X509 v3 Key Usage Field) .....	156
6.2	PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS .....	158
6.2.1	Cryptographic Module Standards and Controls.....	158
6.2.2	Private Key (N out of M) Multi-Person Control.....	159
6.2.3	Private Key Escrow .....	159
6.2.4	Private Key Backup.....	159
6.2.5	Private Key Archival.....	160
6.2.6	Private Key Transfer Into or From a Cryptographic Module.....	161
6.2.7	Private Key Storage on Cryptographic Module.....	161
6.2.8	Method of Activating Private Key .....	162
6.2.9	Method of Deactivating Private Key .....	162
6.2.10	Method of Destroying Private Key.....	162
6.2.11	Cryptographic Module Rating .....	162
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT .....	163
6.3.1	Public Key Archival .....	163
6.3.2	Certificate Operational Periods and Key Pair Usage Periods .....	163
6.4	ACTIVATION DATA.....	164
6.4.1	Activation Data Generation and Installation .....	164
6.4.2	Activation Data Protection.....	164
6.4.3	Other Aspects of Activation Data.....	164

6.5	COMPUTER SECURITY CONTROLS .....	164
6.5.1	Specific Computer Security Technical Requirements .....	164
6.5.2	Computer Security Rating .....	165
6.6	LIFE CYCLE TECHNICAL CONTROLS .....	165
6.6.1	System Development Controls.....	165
6.6.2	Security Management Controls .....	166
6.6.3	Life Cycle Security Controls.....	167
6.7	NETWORK SECURITY CONTROLS .....	167
6.8	TIME-STAMPING.....	168
7	CERTIFICATE, CRL, AND OCSP PROFILES.....	168
7.1	CERTIFICATE PROFILE .....	168
7.1.1	Version Number(s).....	168
7.1.2	Certificate Content and Extensions.....	168
7.1.3	Algorithm Object Identifiers .....	186
7.1.4	Name Forms .....	188
7.1.5	Name Constraints.....	200
7.1.6	Certificate Policy Object Identifier .....	201
7.1.7	Usage of Policy Constraints Extension .....	201
7.1.8	Policy Qualifiers Syntax and Semantics.....	201
7.1.9	Processing Semantics for the Critical Certificate Policies Extension.....	202
7.1.10	Inhibit Any Policy Extension .....	202
7.2	CRL PROFILE.....	202
7.2.1	Version Number(s).....	203
7.2.2	CRL and CRL Entry Extensions .....	203
7.3	OCSP PROFILE .....	205
7.3.1	Version Number(s).....	205
7.3.2	OCSP Extensions.....	205
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS .....	206
8.1	FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT .....	206
8.2	IDENTITY/QUALIFICATIONS OF ASSESSOR .....	206
8.3	ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY.....	208
8.4	TOPICS COVERED BY ASSESSMENT.....	208
8.4.1	CA Assessment .....	209



8.4.2	Signing Service Assessment .....	209
8.4.3	Timestamp Authority Assessment .....	209
8.5	ACTIONS TAKEN AS A RESULT OF DEFICIENCY .....	209
8.5.1	Actions Taken as a Result of Internal Audit Deficiency.....	210
8.6	COMMUNICATION OF RESULTS .....	210
8.6.1	Communication of Internal Audit Results.....	211
8.7	SELF-AUDITS .....	211
8.8	REVIEW OF DELEGATED THIRD PARTIES.....	211
9	OTHER BUSINESS AND LEGAL MATTERS .....	212
9.1	FEES .....	212
9.1.1	Certificate Issuance or Renewal Fees.....	212
9.1.2	Certificate Access Fees.....	212
9.1.3	Revocation or Status Information Access Fees .....	212
9.1.4	Fees for Other Services .....	212
9.1.5	Refund Policy.....	212
9.2	FINANCIAL RESPONSIBILITY.....	212
9.2.1	Insurance Coverage.....	212
9.2.2	Other Assets .....	212
9.2.3	Insurance or Warranty Coverage for End-Entities .....	213
9.3	CONFIDENTIALITY OF BUSINESS INFORMATION .....	213
9.3.1	Scope of Confidential Information.....	213
9.3.2	Information Not Within the Scope of Confidential Information.....	213
9.3.3	Responsibility to Protect Confidential Information .....	213
9.4	PRIVACY OF PERSONAL INFORMATION.....	213
9.4.1	Privacy Plan .....	213
9.4.2	Information Treated As Private.....	214
9.4.3	Information Not Deemed Private .....	214
9.4.4	Responsibility to Protect Private Information .....	214
9.4.5	Notice and Consent to Use Private Information.....	214
9.4.6	Disclosure Pursuant to Judicial or Administrative Process .....	214
9.4.7	Other Information Disclosure Circumstances .....	214
9.5	INTELLECTUAL PROPERTY RIGHTS.....	215
9.6	REPRESENTATIONS AND WARRANTIES .....	215

9.6.1	CA Representations and Warranties.....	215
9.6.2	RA Representations and Warranties.....	217
9.6.3	Subscriber Representations and Warranties .....	218
9.6.4	Relying Party Representations and Warranties .....	220
9.6.5	Representations and Warranties of Other Participants .....	221
9.7	DISCLAIMER OF WARRANTIES.....	221
9.8	LIMITATIONS OF LIABILITY.....	221
9.9	INDEMNITIES .....	222
9.10	TERM AND TERMINATION .....	223
9.10.1	Term .....	223
9.10.2	Termination.....	223
9.10.3	Effect of Termination and Survival.....	223
9.11	INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS .....	223
9.11.1	Notices by Individual Participants to IdenTrust .....	223
9.11.2	Notices by IdenTrust to Individual Participants .....	224
9.11.3	Notices Delivery Method .....	224
9.12	AMENDMENTS.....	224
9.12.1	Procedure for Amendment .....	224
9.12.2	Notification Mechanism and Period .....	225
9.12.3	Circumstances under Which OID Must Be Changed.....	225
9.13	DISPUTE RESOLUTION PROVISIONS .....	225
9.13.1	Specific Provisions/ Incorporation of Policy.....	225
9.14	GOVERNING LAW .....	225
9.15	COMPLIANCE WITH APPLICABLE LAW.....	225
9.16	MISCELLANEOUS PROVISIONS .....	225
9.16.1	Entire Agreement.....	225
9.16.2	Assignment.....	225
9.16.3	Severability.....	226
9.16.4	Enforcement (Attorney Fees and Waiver of Rights) .....	226
9.16.5	Force Majeure .....	226
9.17	OTHER PROVISIONS.....	226
9.17.1	Legal Validity of Certificates.....	226
APPENDIX A: Enterprise RAs as LRAs Auditing and Security Standards.....		228

# 1 INTRODUCTION

## 1.1 OVERVIEW

This TrustID Certification Practice Statement (CPS) describes the 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 the IdenTrust TrustID Certificate Policy Month dd, 2024 (herein referred to as the “TrustID CP,” “CP” or “Policy”).

In particular, this CPS addresses the following:

- The roles, responsibilities, and relationships among IdenTrust, Trusted Agents, RAs, Certificate Manufacturing Authorities (CMAs), Repositories, Subscribers, Relying Parties, and the Policy Management Authority (PMA) (referred to collectively as “Program Participants”);
- Obligations and operational responsibilities of the Program Participants; and
- IdenTrust’s policies and practices for the Issuance, delivery, management, and use of TrustID Certificates to verify Digital Signatures.

Hierarchies for which this CPS applies including Root CA Certificates, Subordinate CA Certificates, and End Entity Certificate types are disclosed in the “IdenTrust TrustID Certificate Hierarchy” table of the [“IdenTrust Downloads and Drivers”](#) webpage.

The copy of the 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, the document referenced in Annex A of the Policy Copy, the document referenced in Annex B of 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 © 2024 IdenTrust Services, LLC. All rights reserved.
- C. PKI Participants (see [Section 1.3](#) of the Policy Copy) 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 Certificate Policy”, 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

This CPS was approved for publication on December 04, 2024, by the IdenTrust Policy Management Authority (PMA). The following table contains subsequent revisions:

TrustID CPS Document Versions		
Version	Date	Summary of Changes/Comments
Prior versions of this CPS can be found in the “Policies – Archived” Section of the <a href="#">IdenTrust TrustID Document Library</a> .		
4.7.7	April 26, 2021	<ol style="list-style-type: none"> <li>Section 1.6.1 and 3.2.2: Added Attestation Letter as proofing method for Subject Identity Information.</li> <li>Section 1.6.1 updated Critical Vulnerability definition.</li> <li>Section 4.2.1: Update to clarify the age of documentation for EV Code Signing Certificates.</li> <li>Section 3.2.2.4.3: Updated reference based on Updates to include TLS BR v1.7.4.</li> <li>Section 5.2.1.: Updates relevant to CA facilities surveillance.</li> <li>Appendix B, Added “ISGR” as Subordinate CA of DST X3.</li> <li>Section 9.6.1.: updates relevant to TLS BR v1.7.4.</li> <li>Updates to Trusted Roles to allow cross responsibilities between Systems Administrators and PKI Consultants. See Section 5.2.1 Trusted Roles</li> </ol>
4.7.8	June 4, 2021	<ol style="list-style-type: none"> <li>Updates for Code Signing: <ul style="list-style-type: none"> <li>Minimum key size 3072 bit for RSA.</li> <li>Add Code Signing Certificates (Non-EV).</li> </ul> </li> </ol>
4.7.9	August 6, 2021	<ol style="list-style-type: none"> <li>Section 4.7.3: Renewal notification updates.</li> <li>Addition of Code Signing Subordinate CAs.</li> <li>Remove optional OU from server Certificates.</li> <li>Section 4.9.12: Updates to reflect methods demonstrating private key-compromise.</li> <li>Update Section 3.2.2.5.4 for FQDN validation method.</li> <li>Support of ECDSA for Code Signing Certificates.</li> </ol>
4.8.0	January 27, 2022	<ol style="list-style-type: none"> <li>Update Section 3.2.2. adding extended validation sources.</li> <li>Updates to Section 6.3.2 for validity periods on human Certificates to be maximum of 825 days effective April 1, 2022.</li> <li>Appendix B: Add TrustID EV Code Signing CA 3.</li> </ol>
4.8.1	April 11, 2022	<ol style="list-style-type: none"> <li>Update Key Sizes in Section 6.1.5.</li> <li>Update Operational and Key Usage Validity Periods in Section 6.3.2.</li> <li>Appendix B: <ol style="list-style-type: none"> <li>Update current active Subordinate CAs.</li> <li>Remove expiration dates.</li> </ol> </li> </ol>
4.8.2	May 12, 2022	<ol style="list-style-type: none"> <li>Add CA/B Forum OID for Time-Stamping Certificates on Section 1.2.2</li> <li>Update CAA record on Sections 4.2 and 4.2.2.1</li> </ol>
4.8.3	May 27, 2022	<ol style="list-style-type: none"> <li>Updates to Section 4.9.10 and 4.10.1 to better reflect compliance.</li> <li>Section 6.3.2 update table.</li> </ol>
4.8.4	December 2, 2022	<ol style="list-style-type: none"> <li>Addition of new definitions to Section 1.6.1.</li> <li>Cosmetic updates in Sections 1.2, 3.1.1, 3.1.2, 3.1.5.5, 3.2.2.5, 7.2.1, 7.4.1.1, 7.4.1.2.</li> <li>Updates for verification of FATCA Certificates in Sections 3.2, and 3.2.9.</li> <li>Add revocation requests from Software Suppliers in Section 4.9.1.1.2.</li> <li>Updates for revocation reason codes in Section 4.9.3.</li> </ol>

TrustID CPS Document Versions		
Version	Date	Summary of Changes/Comments
		<ul style="list-style-type: none"> <li>6. Updates to revoke Code Signing Certificates in Section 4.9.11.</li> <li>7. Updates to Key Sizes in Section 6.1.5.</li> <li>8. Updates to CSA OCSP Responder Certificate Operational Period in Section 6.3.2.</li> <li>9. Updates to match the TrustID CP Section 7.1.3.1.</li> <li>10. Cleanup updates in Sections 2.2, 3.1.1, 7.1.4, and 8.1.</li> <li>11. Add Code Signing Certificates in Section 7.1.4.2.2.</li> <li>12. Add new paragraph for Self-Audits in Section 8.7.</li> <li>13. Update Insurance Coverage details in Section 9.2.1.</li> <li>14. Update Section 9.8 to be in line with the TrustID CP.</li> <li>15. Appendix A, Removed as Certificate Profiles are covered in Section 7.1.</li> <li>16. Appendix B, was C, added new disclosed Subordinate CA: Booz Allen Hamilton BA CA 02.</li> </ul>
4.8.5	January 26, 2023	<ul style="list-style-type: none"> <li>1. Add a reference to CA/B Network Security requirements in Section 2.2.2</li> <li>2. Update Non-Repudiation references for Key Usage as optional</li> </ul>
4.8.6	September 1, 2023	<p>Updates based on the TLS BR v2.0.0 and S/MIME BR v1.0.0, 1.0.1:</p> <ul style="list-style-type: none"> <li>1. 1.2.2 Updated names and added S/MIME OIDs</li> <li>2. 1.3.2.1 Added Section</li> <li>3. 1.5.2 Moved reference to Section 4.10.2</li> <li>4. 1.5.5.5 Moved to Section 2</li> <li>5. 1.6.1, 1.6.2 Added/Updated definitions/acronyms</li> <li>6. 2, 2.1, 2.2, Updates for repositories</li> <li>7. 2.3 Updates for Time or Frequency of Publication</li> <li>8. 3.1.3.1, 3.2.3.2 Added Sections</li> <li>9. 3.1.4 Updates for Uniqueness of Names</li> <li>10. 3.2.2, 3.2.2.1 Updates for Organization validation</li> <li>11. 3.2.6 Updates for Criteria of Interoperation</li> <li>12. 3.2.6.3 Updated for Validation of Email Address Authorization/Control</li> <li>13. 3.2.10 Added Section</li> <li>14. 4.1, 4.2.1, 4.2.2 Updates for Certificate application</li> <li>15. 4.9.3.7 Updates for General Guidance</li> <li>16. 4.9.7.1, 4.9.7.2, added sections</li> <li>17. 4.9.10 Updates for Certificate revocation</li> <li>18. 4.10.2 Updates for Service Availability</li> <li>19. 5.2.1 Update to better reflect Trusted Roles</li> <li>20. 5.2.1.1.5 Added Software Engineer Role</li> <li>21. 5.2.1.1.6 Added DevOps Role</li> <li>22. 5.3.3 Updates for Training Requirements</li> <li>23. 5.4.3 Updates for Retention Period Log</li> <li>24. 5.5. Updates for Records Archival</li> <li>25. 5.7 Updates for Comprise and Disaster Recovery</li> <li>26. 6.1.1 Updates for Key Pair Generation and Installation</li> <li>27. 6.1.2 Updates for Private Key Delivery to Subscriber</li> <li>28. 6.3.2 Updates for Certificate Operational Periods</li> <li>29. 6.7 Updates for Network Security Controls</li> <li>30. 7.0 Updates for Certificate Profiles adding reference to the TLS BR and S/MIME BR.</li> <li>31. 8.0 Updates for Compliance Audit</li> </ul>

TrustID CPS Document Versions		
Version	Date	Summary of Changes/Comments
		32. 8.1. Updates for Identity/Qualifications of Assessor 33. 8.3 Added Section 34. 8.4 Updates for Topics Covered by Assessment 35. 8.8 Added Section 36. 9.4.1, 9.4.2, 9.4.4, 9.4.5, Updates for Privacy Plan 37. 9.6.1 Updates for CA Representations 38. 9.6.3 Updates for Subscriber Representations 39. Appendix B, added new Root CAs for elliptic curve cryptography, new Subordinate CA for Code Signing and new Subordinate CA's for S/MIME Certificates.
4.8.7	September 11, 2023	Updates to Section 7 – Certificate Profiles for S/MIME BR v1.0.0 and TLS BR 2.0.0
4.8.8	September 14, 2023	Minor updates on Section 7.1.2 with proper language for subjectKeyIdentifier field
4.8.9	October 25, 2023	Updates in Object Identifier (OID) Section 1.2.2 Updates to Certificate Use in Section 1.4.1.1 Updates to Certificate Profiles Sections 6.1.7.2; 6.1.7.3; 6.1.7.4; 6.1.7.7; 7.1.2.4; 7.1.2.7 and 7.1.2.8.
4.9.0	March 12, 2024	1. 1.1.2 Add Multipurpose Profile and Strict Profile for S/MIME OIDs 2. 6.1.1 added details for CA Key Pair Generation 3. 3.2.2 Update to reflect Reliable Method of Communication
4.9.1	September 30, 2024	1. 1.2 Removed older than 3 year references 2. 1.2.1 Update to reference Root CA's in Appendix B 3. 1.2.2, 1.3.1, 1.3.2, 1.3.2.1, 1.3.5.1, 1.5.3, Update headers to align with RFC-3647 format 4. 1.2.2, 1.4.1.1, 1.4.1.2, 3.1.1, 3.1.2, 3.2.3 Update order by Certificate type and removed Personal Hardware 5. 1.3.2, 1.3.2.1 Update RA activities 6. 1.4 Added Certificate Usage details 7. 1.5.2, 4.9.3 Update guideline for revocation requests 8. 1.6.1 Added definitions 9. 1.6.2 Added acronyms 10. 2.1, 2.2 Aligned sections to better reflect intended purpose 11. 2.3 Removed redundant last paragraph 12. 3.1.2, 3.2, 3.2.2.1, 3.2.2.2, 3.2.6.4, 3.2.6.5.2, 4.1.2.2.1.3, 4.2.1, 4.2.2.2, 7.1.4.2.2 Updated Server Extended Validation references 13. 3.2.2.4, 3.2.2.4.2, 3.2.2.4.4, 3.2.2.4.7, 3.2.2.4.8, 3.2.2.4.18, Updated details for Domain Authorization methods 14. 3.2.2.8.1 4.2.2 Added and updated reference to CAA Records for Server and S/MIME certificates 15. 3.2.3.2 Added reference to physical identity documents 16. 3.2.3.3.1 Update to reflect S/MIME Organization Verification Sources 17. 3.2.3.6, 3.2.3.7 Removed Role-Based certificate references 18. 3.2.5 Update to reflect S/MIME Reliable Method of Communication 19. 4.1.2 Update to Enrollment Process and Responsibilities 20. 4.2.2 Added footnote for S/MIME CAA Record checking 21. 4.2.4 added references for final cross-correlation and due diligence 22. 4.9.1.1 Update to reflect revocation for Short-lived certificates 23. 4.9.3 Moved revocation reason details to Section 7.2.2

TrustID CPS Document Versions		
Version	Date	Summary of Changes/Comments
		<p>24. 4.9.7 Update CRL Issuance Frequency details</p> <p>25. 5.2.1, 5.2.1.1.5, 5.2.1.1.6, 5.2.4 Update Trusted Roles</p> <p>26. 5, 5.1 Added NetSec BR references</p> <p>27. 5.2.1 Removed duplicated entries</p> <p>28. 5.4.1 Added details for types of events recorded</p> <p>29. 5.4.1.1 Added details for Router and Firewall activities logs</p> <p>30. 5.4.1.2 Added details for types of events recorded for Timestamp Authorities</p> <p>31. 6.1.1.3 Updates for handling compromised and weak keys</p> <p>32. 6.1.2 Update to cover revocation</p> <p>33. 7.1, 7.1.1, 7.1.2, 7.1.2.1, 7.1.2.2, 7.1.2.2.1, 7.1.2.2, 7.1.2.2.1, 7.1.2.2.2, 7.1.2.2.3, 7.1.2.2.4, 7.1.2.2.5, 7.1.2.3, 7.1.2.3.1, 7.1.2.3.2, 7.1.2.3.3, 7.1.2.3.4, 7.1.2.3.5, 7.1.2.3.6, 7.1.2.3.7, 7.1.2.3.8, 7.1.2.4, 7.1.3.1, 7.1.3.1.1, 7.1.3.1.2, 7.1.3.2, 7.1.3.2.1, 7.1.3.2.2, 7.1.4, 7.1.4.1, 7.1.4.2, 7.1.4.2.1, 7.1.4.2.1.1, 7.1.4.2.1.2, 7.1.4.2.1.3, 7.1.4.2.1.4, 7.1.4.2.2, 7.1.4.2.3, 7.1.4.3, 7.1.4.3.1, 7.1.4.3.2, 7.1.4.3.3, 7.1.4.3.4, 7.1.4.3.5, 7.1.4.3.6, 7.1.4.3.7, 7.1.4.3.8, 7.1.4.3.9, 7.1.4.3.10, 7.1.4.3.11, 7.1.5, 7.1.6, 7.2, 7.2.1, 7.2.2, 7.2.2.1, Updates to the Certificate Profiles</p> <p>34. 8.4.1, 8.4.1, 8.4.2 Added CA Signing Service Assessment</p> <p>35. 8.8. Added reference to delegated parties</p> <p>36. 9.6.1 Updated CA Representations and Warranties</p> <p>37. 1.2.2, 1.6, 1.4.2, 3.1.1, 3.2, 3.2.2.10, 3.2.3.6, 6.2.1, 6.3.2, 7.1.2.3.3, 7.1.4.2.3, 7.1.4.3.7, 7.1.4.3.8, 7.2, 9.6.3.3, 9.8, Updates for EV/Non-EV Code Signing references</p> <p>Appendix B, added new ECC Roots and SubCA's</p>
4.9.2	December 04, 2024	<p>1. 1.2.2 Updated OIDs for CIV Certificates</p> <p>2. 1.6.1 Added some definitions</p> <p>3. 1.6.2 Added acronyms</p> <p>4. 3.2.2 Updated review for status of Applicant</p> <p>5. 3.2.2.4.7, 3.2.2.4.8, 3.2.2.4.18, 3.2.2.5.1, 5.4.1 Multi-Perspective Issuance Corroboration</p> <p>6. 3.2.2.7 Updated S/MIME Data Source Accuracy</p> <p>7. 3.2.2.8.1, 3.2.2.8.2 Updated CAA Records</p> <p>8. 4.2.1 Updated reference to EV TLS authentication</p> <p>9. 4.3.1.1. Add reference to Root CA issuance</p> <p>10. 4.3.1.2, 4.3.1.3, 6.6.1, 8.7 Added Linting requirements</p> <p>11. 4.9.9.1, 4.9.9.2, 4.9.10.1, 4.9.10.2, 6.2.7.1, 6.2.7.2, 6.2.7.3 Added sub-headers</p> <p>12. 6.1.1.1 updated CA Key Generation details</p> <p>13. 6.3.2 Updated validity period for Time-Stamping CA and CIV Card Authentication</p> <p>14. 7.1.4.3.3 Added details for S/MIME subject:commonName</p> <p>15. 7.1.4.3.5 Added details for DBA of organizationName in OV TLS certificates</p> <p>16. 8.4, 8.4.1, 8.4.2, 8.4.3 Updated version reference for WebTrust</p> <p>17. Appendix B: Removed and reference IdenTrust TrustID Certificate Hierarchy to the IdenTrust Downloads and Drivers webpage.</p>

### 1.2.1 Alphanumeric Identifier

The alphanumeric identifier (i.e., the title) for this CPS is the IdenTrust TrustID Certificate Practices Statement, v4.9.2 dated December 04, 2024, or "identrust\_TrustID\_cps\_v4.9.2\_20241204".

Root CAs governed by this CPS document are disclosed in the “IdenTrust TrustID Certificate Hierarchy” table of the [“IdenTrust Downloads and Drivers”](#) webpage.

### 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 TrustID CP and associated Policy documents is 2.16.840.1.113839.

Certificates issued pursuant to this CPS may contain one or more of the following OIDs:

TrustID Certificate Names, Types, and Policy OIDs			
Name	Type	IdenTrust Policy OID	CA/B Forum OID
Secure Email Software	Signing/Encryption S/MIME Mailbox-Validated	2.16.840.1.113839.0.6.11.1	2.23.140.1.5.1.2 (Multipurpose Profile) or 2.23.140.1.5.1.3 (Strict Profile)
Secure Email Hardware	Signing/Encryption S/MIME Mailbox-Validated	2.16.840.1.113839.0.6.11.2	2.23.140.1.5.1.2 (Multipurpose Profile) or 2.23.140.1.5.1.3 (Strict Profile)
Personal (Basic Individual) Software	Signing /Encryption/Identity S/MIME Individual-Validated	2.16.840.1.113839.0.6.1.1	2.23.140.1.5.4.2 (Multipurpose Profile) or 2.23.140.1.5.4.3 (Strict Profile)
Medium Assurance Individual Identity Software	Signing /Encryption/Identity S/MIME Individual-Validated	2.16.840.1.113839.0.6.1.2	2.23.140.1.5.4.2 (Multipurpose Profile) or 2.23.140.1.5.4.3 (Strict Profile)
Medium Assurance Individual Identity Hardware	Signing /Encryption/Identity AATL enabled S/MIME Individual-Validated	2.16.840.1.113839.0.6.12.1	2.23.140.1.5.4.2 (Multipurpose Profile) or 2.23.140.1.5.4.3 (Strict Profile)
Business	Signing/Encryption/Identity S/MIME Sponsor-Validated	2.16.840.1.113839.0.6.10.2	2.23.140.1.5.3.2 (Multipurpose Profile) or 2.23.140.1.5.3.3 (Strict Profile)
	Card Authentication S/MIME Sponsor-Validated	2.16.840.1.113839.0.6.10.100	
Business Software	Signing /Encryption/Identity S/MIME Individual-Validated	2.16.840.1.113839.0.6.2.1	2.23.140.1.5.3.2 (Multipurpose Profile) or 2.23.140.1.5.3.3 (Strict Profile)
Business Hardware	Signing /Encryption/Identity AATL enabled S/MIME Individual-Validated	2.16.840.1.113839.0.6.12.2	2.23.140.1.5.3.2 (Multipurpose Profile) or 2.23.140.1.5.3.3



TrustID Certificate Names, Types, and Policy OIDs			
Name	Type	IdenTrust Policy OID	CA/B Forum OID
			(Strict Profile)
FATCA Organization	Signing/Encryption S/MIME Organization-Validated	2.16.840.1.113839.0.6.8	2.23.140.1.5.2.2 (Multipurpose Profile) or 2.23.140.1.5.2.3 (Strict Profile)
Server Domain Validation	Server Authentication (DV)	2.16.840.1.113839.0.6.5	2.23.140.1.2.1
Server Organization Validation	Server Authentication (OV)	2.16.840.1.113839.0.6.3	2.23.140.1.2.2
Server Extended Validation	Server Authentication (EV)	2.16.840.1.113839.0.6.9	2.23.140.1.1
Non-EV Code Signing	Signing	2.16.840.1.113839.0.6.14.2	2.23.140.1.4.1
EV Code Signing	Signing	2.16.840.1.113839.0.6.14.1	2.23.140.1.3
Time-Stamping	Signing	2.16.840.1.113839.0.6.13.1 2.16.840.1.113839.0.6.13.3	2.23.140.1.4.2
CIV* Card Authentication Device	Signing/Encryption	2.16.840.1.101.3.2.1.3.19 2.16.840.1.113839.0.6.20.1	
CIV* Card Authentication Human	Signing	2.16.840.1.101.3.2.1.3.19 2.16.840.1.113839.0.6.12.25	
CIV* Card Authentication Basic Assurance	Signing/Encryption	2.16.840.1.101.3.2.1.3.19 2.16.840.1.113839.0.6.30.1	
Administrative CA	Signing/Encryption/Identity	2.16.840.1.113839.0.7 (arc)	
Administrators	Signing/Encryption/Identity	2.16.840.1.113839.0.7.1	
Registration Authorities	Signing/Encryption/Identity	2.16.840.1.113839.0.7.2	
Authorized Relying Parties	Signing/Encryption/Identity	2.16.840.1.113839.0.7.3	

\* These certificates are issued to enterprise customers adapting the CIV framework without having to cross-sign with the U.S. Federal Public Key Infrastructure (PKI) Bridge. CIV uses the same technology and data model as PIV-I credentials which are based on FIPS 201 and PIV-I specifications.

### 1.3 PKI PARTICIPANTS

This 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 TrustID CP and this CPS to fulfill any of the following roles: PMA, CA, RA, CMA, Repository, Subscriber, and Authorized Relying Party.

#### 1.3.1 Certification Authorities

A Certification Authority (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) 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 an Issuing CA is bound to act according to the terms of TrustID CP.

### 1.3.2 Registration Authorities

IdenTrust as Issuing CA is ultimately responsible for all TrustID Certificates it issues; however, under this 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 BR requirements that are applicable to the delegated function; and;
4. Comply with this CPS or the Delegated Third Party's Registration Practice Statement that IdenTrust has verified, and complies with the BR requirements. 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: If the Certificate request is for a Mailbox-Validated, Organization-Validated, or Sponsor-Validated profile, IdenTrust shall confirm that the Enterprise RA has authorization or control of the requested email domain(s) in accordance with [Section 3.2.2.4](#). If the Certificate request is for a Subscriber server Certificate, 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 Server Certificates the final cross-correlation and due diligence requirements of [Section 3.2.2.13 of the EV TLS BR](#) may be performed by a single person representing the Enterprise RA.

An Enterprise RA may also submit Certificate Requests using the Mailbox-Validated profile for users whose email domain(s) are not under the delegated organization’s authorization or control. In this case, IdenTrust confirms that the Email Address holder has control of the requested Email Address(es) in accordance with [Section 3.2.6.3](#).

For Subscriber server Certificates, IdenTrust does not delegate domain validation or IP Address validation to third parties.

### 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 may include unaffiliated Individuals (personal), Individuals who are affiliated (business), or Sponsoring Organizations applying for Code Signing, CIV Card Authentication, CIV Device or FATCA Organization Certificates.

### **1.3.3.1 Affiliated/Subscribing Organization**

Subscriber 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**

An Authorized Relying Party 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.

An Authorized Relying Party is required to act reasonably in determining whether to rely on a Certificate. By using or otherwise relying on a Certificate, the Relying Party agrees to be bound by the provisions of this CPS.

### **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 TrustID CP and this CPS with all the PKI Participants. The IdenTrust PMA also has charge of the future development and amendment of this CPS.

#### **1.3.5.2 Certificate Manufacturing Authority (CMA)**

IdenTrust is responsible for the manufacture of TrustID Certificates.

#### **1.3.5.3 Repositories**

IdenTrust will perform the role and functions of the Repository.

#### **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 acting, 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**

A Trusted Agent is an entity authorized to act as a representative of a Sponsoring Organization in verifying Applicant or PKI Sponsor information during the registration process. Trusted Agents do not have automated interfaces with the CA systems but will work manually with RAs and IdenTrust to have Applicants/PKI Sponsors approved.

### 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

TrustID Certificates are intended to support verification of Digital Signatures in applications where: (i) the identity of communicating parties needs to be authenticated; (ii) a message or file needs to be bound to the identity of its originator by a signature; and/or (iii) the integrity of the file or message has to be assured.

Digital Certificates are encrypted data that link a subscriber's identity to a Public Key, enabling secure electronic transactions and serving as a digital ID. They are commonly used for:

- Email signing and encryption
- Document Signing and encryption
- Client and Server authentication
- Time-stamp certificates provide cryptographic proof that data existed at a specific time
- Other purposes, if legally permissible and reliable

IdenTrust offers these types of Certificates

1. S/MIME
  - Mailbox-Validated (MV)
  - Individual-Validated (IV)
  - Sponsor-Validated (SV)
  - Organization-Validated (OV)
2. Server Certificates
  - Domain validated (DV)
  - Organization validated (OV)
  - Extended organization validated (EV)
3. Code Signing
  - Organization validated (Non-EV CS)
  - Extended organization validated (EV CS)
4. Time-Stamping
5. CIV Device Certificates
6. CIV Card Authentication and Administrative CA & CA
7. OCSP Signer

The Certificates listed above are governed by this CPS, the CP and Subscriber Agreements.

### 1.4.1 Appropriate Certificate Uses

Certificates issued pursuant to this CPS are created for specific uses. The uses for which such Certificates are created to reflect the TrustID CP requirements, industry guidelines (e.g., BRs), and technical standards (e.g., [RFC 5280](#)).

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

The tables below identify the allowed uses for each Certificate type issued under this Policy. The first table contains Certificates issued to Individuals and the second table focuses on Certificates issued to Sponsoring Organizations.

### 1.4.1.1 Certificates Issued to Individuals

TrustID Certificate Usage - Individuals					
Certificate Type	Description	Allowed Uses			
		Signing	Encryption	Client -Auth	Doc-Signing
Secure Email Software and Hardware	Certificate(s) issued to an Email Address only	Yes	Yes		
Personal Software – Basic Individual Software	Certificate(s) issued to an Individual not affiliated to a Sponsoring Organization	Yes	Yes	Yes	Yes
Medium Assurance Individual Identity Software	Certificate(s) issued to an Individual not affiliated to a Sponsoring Organization	Yes	Yes	Yes	Yes
Medium Assurance Individual Identity Hardware	Certificate(s) issued to an Individual not affiliated to a Sponsoring Organization – AATL enabled	Yes	Yes	Yes	Yes
Business Software	Certificate(s) issued to an Affiliated Individual	Yes	Yes	Yes	Yes
Business Hardware	Certificate(s) issued to an Affiliated Individual – AATL enabled	Yes	Yes	Yes	Yes
Administrative RA	Certificate(s) issued to an Affiliated Individual performing actions related to the LRA role in this CPS	Yes	Yes	Yes	

### 1.4.1.2 Certificates Issued to Sponsoring Organizations

TrustID Certificate Usage - Organizations						
Certificate	Description	Allowed Uses				
		Signing	Encryption	Client-Auth	Code Signing	Time-Stamping
FATCA Organization	Certificate issued for use by an Electronic Device supporting asymmetric encryption and signing of data submissions within the IRS FATCA program.	Yes	Yes	Yes		
Server (DV, OV, EV)	Certificate issued for use in an Electronic Device that supports server SSL/TLS Communications.	Yes	Yes	Yes		
Code Signing	Certificate issued for use in an Electronic Device signing code.	Yes			Yes	

TrustID Certificate Usage - Organizations						
Certificate	Description	Allowed Uses				
		Signing	Encryption	Client-Auth	Code Signing	Time-Stamping
Time-Stamping	Certificate issued for use in an Electronic Device time-stamping.	Yes				Yes
CIV Device Certificate	Certificate issued to an approved Cryptographic Module contained within an Electronic Device.	Yes	Yes	Yes		
CIV Card Authentication Certificate	Certificate issued to an approved Cryptographic Module.	Yes	Yes	Yes		
Authorized Relying Parties	Certificate issued for use in an Electronic Device that supports the signing of data submission by an automated Registration Authority.	Yes		Yes		

### 1.4.2 Prohibited Certificate Uses

Certificates issued under the provisions of this 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.

Code Signing Certificates are not intended to assert that the signed code is safe to install or free from malware, bugs, or vulnerabilities; they are intended to verify the identity of the Subscriber and that the signed code has not been modified from its original form.

## **1.5 POLICY ADMINISTRATION**

### **1.5.1 Organization Administering this CPS Document**

This CPS is administered by:

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

### **1.5.2 Contact Person**

Questions regarding the implementation and administration of this 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](mailto:Policy@IdenTrust.com)  
Phone: (888) 882-1104

Guidelines on reporting suspected Private Key Compromise, Certificate misuse, or any form of fraud, compromise, misuse, inappropriate conduct, or other Certificate-related matters for Subscribers, Relying Parties, Application Software Suppliers, and other third parties are provided in [Section 4.10.2.1](#) "Certificate Problem Reporting".

### **1.5.3 Person Determining CPS Suitability for the Policy**

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

### **1.5.4 CPS Approval Procedures**

The IdenTrust PMA is responsible for approving this CPS. Details on this procedure are provided in [Section 9.12](#).

#### **1.5.4.1 Copy of Policy**

A copy of this CPS is available via email from [support@Identrust.com](mailto:support@Identrust.com) or on the Internet at:

<https://secure.identrust.com/Certificates/policy/ts>

#### **1.5.4.2 Notification of Changes**

The PMA will notify all Issuing CAs authorized to issue Certificates under the TrustID CP of proposed changes, the final date for receipt of comments, and the proposed effective date of the change. The PMA may request that the Issuing CA notify RAs and Subscribers of the proposed changes. The PMA will also post a notice of the proposal on the PMA World Wide Web site.

#### **1.5.4.3 Mechanism to Handle Comments**

Written and signed comments on proposed changes must be directed to the PMA. Decisions with respect to the proposed changes are at the sole discretion of the PMA.



#### 1.5.4.4 Final Change Notice

The PMA will determine the period for the final change notice.

#### 1.5.4.5 Items Whose Change Requires a New Policy

If a Policy change is determined by the PMA to warrant the Issuance of a new Policy, the PMA may assign a new OID for the modified Policy.

### 1.6 DEFINITIONS AND ACRONYMS

#### 1.6.1 Definitions

Term	Definition
<b>Accept or Acceptance</b>	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: <ul style="list-style-type: none"><li>• Using the TrustID Certificate (after Issuance);</li><li>• Failing to notify IdenTrust of any problems with the TrustID Certificate within a reasonable time after receiving it; or</li><li>• Other manifestations of assent.</li></ul>
<b>Account Password</b>	Private data, which may consist of Activation Data, used by the Applicant/PKI Sponsor for authentication and delivered to the CA securely via a server-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 server-authenticated SSL/TLS-encrypted session.
<b>Activation Code</b>	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.
<b>Activation Data</b>	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).
<b>Affiliate</b>	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
<b>Affiliated Individual</b>	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).
<b>Applicant</b>	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.
<b>Applicant Representative</b>	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: <ol style="list-style-type: none"><li>1. who signs and submits, or approves a Certificate Request on behalf of the Applicant;</li><li>2. who signs and submits a Subscriber Agreement on behalf of the Applicant; and/or</li><li>3. who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.</li></ol>

<b>Term</b>	<b>Definition</b>
<b>Application Software Supplier</b>	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.
<b>Assumed Name</b>	Also known as “doing business as”, “DBA”, or “d/b/a” name in the US and “trading as” name in the UK.
<b>Attestation Letter</b>	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.
<b>Audit Period</b>	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 not the same as 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 <a href="#">Section 8.1</a> .
<b>Audit Report</b>	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 BR requirements.
<b>Authority Revocation List (or ARL)</b>	A list of revoked CA Certificates. An ARL is a CRL for CA Certificates.
<b>Authorization Domain Name</b>	The Domain Name used to obtain authorization for Certificate issuance for a given FQDN. The CA 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. The CA 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.
<b>Authorized Port</b>	One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).
<b>Authorized Relying Party</b>	An Individual or Organization that has entered into an Authorized Relying Party Agreement.
<b>Authorized Relying Party Agreement</b>	A contract between an Individual or an Organization and IdenTrust that allows the party to rely on TrustID Certificates in accordance with the TrustID CP and this CPS.
<b>Authorizing Official (or AO)</b>	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.
<b>Base Domain Name</b>	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.
<b>Business Certificate</b>	See Sponsor-Validated
<b>CA Certificate</b>	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.
<b>CA Key Pair</b>	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).
<b>CA Private Root Key</b>	The Private Key is used to sign CA Certificates.

<b>Term</b>	<b>Definition</b>
<b>CA Private Signing Key</b>	The Private Key that corresponds to IdenTrust's Public Key listed in its CA Certificate and used to sign TrustID Certificates.
<b>CA/B Forum</b>	The CA/Browser Forum is a collaborative consortium comprising certification authorities (CAs), providers of Internet browser software, and developers of various applications utilizing X.509 v.3 digital Certificates. These Certificates are employed for securing SSL/TLS connections, Code Signing, and S/MIME communications. The primary purpose of the CA/Browser Forum is to establish, update, and uphold the BRs that govern the issuance of these specific Certificate types by publicly trusted CAs.
<b>CAA</b>	From <a href="#">RFC 8659</a> : "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."
<b>CAA Resource Record Set</b>	Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended Certificate mis-issuance.
<b>Certificate</b>	<p>A computer-based record or electronic message that:</p> <ul style="list-style-type: none"> <li>• Identifies the Certification Authority issuing it</li> <li>• Names or identifies a Subscriber, Authorized Relying Party, or Electronic Device</li> <li>• Contains the Public Key of the Subscriber, Authorized Relying Party, or Electronic Device</li> <li>• Identifies the Certificate's Validity Period</li> <li>• Is Digitally Signed by a Certification Authority and</li> <li>• Has the meaning ascribed to it in accordance with applicable standards</li> </ul> <p>A Certificate includes not only its actual content but also all documents expressly referenced or incorporated in it.</p>
<b>Certificate Agreement</b>	See Subscriber Agreement.
<b>Certificate Chain</b>	A Certificate Chain is a series of Certificates connecting a Subscriber's Certificate to the Root Certificate. Successive and superior CA and Subordinate CA Certificates up to the Root Certificate connect superior Certificates (which may be self-signed) in a Certificate Chain. For Subscribers under this CPS, a self-signed Root Certificate is issued in compliance with this Policy.
<b>Certificate Data</b>	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.
<b>Certificate Holder</b>	See Subscriber
<b>Certificate Management Center (or CMC)</b>	An online interface available for Subscribers to manage their Certificate information.
<b>Certificate Data</b>	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.
<b>Certificate Manufacturing Authority (or CMA)</b>	An Organization that manufactures or creates TrustID Certificates for IdenTrust.
<b>Certificate Policy (or CP)</b>	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.

<b>Term</b>	<b>Definition</b>
<b>Certificate Problem Report</b>	Complaint of suspected Private Key compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to IdenTrust issued Certificates.
<b>Certificate Profile(s)</b>	The protocol used in <a href="#">Section 7</a> of this 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.
<b>Certificate Request</b>	Means a request to issue a Certificate, submitted to the CA by an authorized Individual.
<b>Certificate Revocation List (or CRL)</b>	A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.
<b>Certificate Subject</b>	See Individual-Validated
<b>Certificate Transparency (or CT)</b>	Open standard (see the <a href="#">RFC 6962</a> ) 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.
<b>Certification Authority (or CA)</b>	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.
<b>Certification Authority Authorization (or CAA)</b>	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.”
<b>Certification Practice Statement (or CPS)</b>	A statement of the practices that a CA employs in creating, issuing, managing, and revoking Certificates.
<b>Client-authenticated SSL/TLS-Encrypted Session</b>	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 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.
<b>Code Signing</b>	Term used to signify requirements that are applicable to TrustID Code Signing Certificates.
<b>Code Signing Certificate</b>	A digital Certificate issued by a CA that contains a Code Signing EKU. Non-EV and EV Code Signing Certificates focus only on assuring the identity of the Subscriber Organization and that the signed code has not been modified from its original form. These Certificates are not intended to provide any other assurances, representations, or warranties. Specifically, Non-EV and EV Code Signing Certificates do not warrant that code is free from vulnerabilities, malware, bugs, or other problems.
<b>Common Vulnerability Scoring System (or CVSS)</b>	A quantitative model used to measure the base level severity of a vulnerability (see <a href="https://nvd.nist.gov/home">https://nvd.nist.gov/home</a> ).
<b>Critical Vulnerability</b>	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 <a href="https://nvd.nist.gov/vuln-metrics/cvss">https://nvd.nist.gov/vuln-metrics/cvss</a> ), or as otherwise designated as a Critical Vulnerability by the CA or the CA/B Forum.
<b>Cross-Certified Subordinate CA Certificate</b>	A Certificate used to establish a trust relationship between 2 Root CAs.

<b>Term</b>	<b>Definition</b>
<b>Cryptographic Module</b>	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].
<b>CS BR</b>	The most current version of the CA/B Forum “Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates” published at: <a href="https://cabforum.org/baseline-requirements-code-signing/">https://cabforum.org/baseline-requirements-code-signing/</a>
<b>CSPRNG</b>	A pseudo-random number generator intended for use in a cryptographic system.
<b>Datacenter</b>	A building within which the IdenTrust CA system resides in a high-security area involving both physical and technological protection.
<b>Delegated Third Party</b>	A natural person or Legal Entity that is not the CA but is authorized by the CA, and whose activities are not within the scope of the appropriate CA audits, to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.
<b>Digital Signature / Digitally Sign</b>	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: <ul style="list-style-type: none"> <li>• Whether the transformation was created using the Private Key that corresponds to the Public Key; and</li> <li>• Whether the record has been altered since the transformation was made.</li> </ul>
<b>Distinguished Name (or DN)</b>	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)).
<b>Domain Contact</b>	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.
<b>Domain Label</b>	From <a href="#">RFC 8499</a> : “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.”
<b>Domain Name</b>	The label assigned to a node in the Domain Name system (see Fully Qualified Domain Name).
<b>Domain Name Registrant</b>	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.
<b>Domain Name Registrar</b>	A person or entity that registers Domain Names under the auspices of or by agreement with: <ul style="list-style-type: none"> <li>• The Internet Corporation for Assigned Names and Numbers (ICANN)</li> <li>• A national Domain Name authority/registry or</li> <li>• A Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).</li> </ul>
<b>Domain Namespace</b>	The set of all possible Domain Names that are subordinate to a single node in the Domain Name system.
<b>Electronic Device</b>	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.

<b>Term</b>	<b>Definition</b>
<b>Email Address(es)</b>	Same as Mailbox Address, 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."
<b>End Entity(ies)</b>	Subscribers and Authorized Relying Parties.
<b>Enrollment Workstation (or EWS)</b>	An Enrollment Workstation is the customer side computer application that interfaces with the CMS to accomplish Certificate registration.
<b>Enterprise RA</b>	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.
<b>EV TLS BR</b>	The most current version of the CA/B Forum "Baseline Requirements Guidelines for the Issuance and Management of Extended Validation Certificates" published at: <a href="https://cabforum.org/extended-validation/">https://cabforum.org/extended-validation/</a>
<b>Extended Validation Server Certificate (or EV Server)</b>	A Certificate that contains Subject information specified in the <a href="#">EV TLS BR</a> and that are validated in accordance with those guidelines.  The primary purposes of EV Server Certificates are to (1) identify the Legal Entity that controls a website or service site, and (2) enable encrypted communications with that site. The secondary purposes include significantly enhancing cybersecurity by helping establish the legitimacy of an organization claiming to operate a website, and providing a vehicle that can be used to assist in addressing problems related to distributing malware, phishing, identity theft, and diverse forms of online fraud.
<b>EV Code Signing Certificate ( EV Code Signing)</b>	Certificates that contain Subject information as specified in the most current <a href="#">CS BR</a> . and that are validated in accordance with those guidelines.  EV Code Signing Certificates include jurisdiction of incorporation details in the Subscriber Certificate.
<b>External CA</b>	An independent entity that is not affiliated to the Issuing CA that issues Certificates from a Subordinate CA Certificate. Such a Subordinate CA Certificate is issued and managed according to the Issuing CA Policy. The External CA will produce and publish a separate CP and CPS that they will be bound to adhere to its terms (each is publicly disclosed) and independently audited with publicly available reports. They are contractually bound to other obligations by the Issuing CA and bound to comply with Application Software Supplier programs.
<b>FATCA Foreign Financial Institution (or FFI) List Search and Download Tool</b>	An online application provided by the IRS to enable the creation and download of a partial or complete list of financial institutions registered, accepted, and issued a Global Intermediary Identification Number (GIIN) in accordance with FATCA regulations. The list is updated from time to time with additions and deletions and published at the beginning of the month. As of the release date, hereof such tool can be located at <a href="https://www.irs.gov/businesses/corporations/fatca-foreign-financial-institution-list-search-and-download-tool">https://www.irs.gov/businesses/corporations/fatca-foreign-financial-institution-list-search-and-download-tool</a>
<b>Fully Qualified Domain Name (or FQDN)</b>	A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name system.
<b>GET Method</b>	An OCSP request using the GET method is constructed as follows: GET {url}/{url-encoding of base-64 encoding of the DER encoding of the OCSP Request} where {url} may be derived from the value of the authority information access extension in the Certificate being checked for Revocation, or other local configuration of the OCSP client.
<b>Government Agency</b>	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



<b>Term</b>	<b>Definition</b>
	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.
<b>Government Entity</b>	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.).
<b>Identification Proofing</b>	To ascertain and confirm through appropriate inquiry and investigation the identity of an Individual, End Entity, or Sponsoring Organization.
<b>Individual(s)</b>	A Natural Person and not a juridical person or Legal Entity.
<b>Individual-Validated / Personal Certificate</b>	Refers to an S/MIME Certificate Subject that includes only Individual (Natural Person) attributes, rather than attributes linked to an Organization. In this CPS, these Certificate types: <ul style="list-style-type: none"> <li>• Personal Software</li> <li>• Medium Assurance Unaffiliated Hardware</li> </ul>
<b>Internal Name(s)</b>	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.
<b>Internet</b>	The Internet is a global system of interconnected computer networks that uses multiple protocols to communicate data.
<b>Internet Protocol (or IP)</b>	The primary protocol in the Internet Layer defined by the Request for Comment 1122 ( <a href="#">RFC 1122</a> ) - 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.
<b>IP Address or IP Addresses</b>	A 32-bit or 128-bit label assigned to a device that uses the Internet Protocol for communication.
<b>Issue Certificates / Issuance</b>	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.
<b>Issuing Certification Authority (or Issuing CA)</b>	An entity authorized by the PMA to issue and sign Certificates in accordance with the TrustID CP and this CPS. In both documents, the term "CA", and/or "Issuing CA", means issuance of IdenTrust CA TrustID Certificates.
<b>Jurisdiction of Incorporation</b>	The country and (where applicable) the state or 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.
<b>Key</b>	A general term used throughout this Policy to encompass any one of the defined Keys mentioned in these general definitions section.
<b>Key Compromise</b>	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.
<b>Key Escrow Database (or KED)</b>	A database that contains an escrowed copy of the encryption Certificate for each TrustID Certificate generated.
<b>Key Generation</b>	The process of creating a Key Pair.
<b>Key Generation Script</b>	A documented plan of procedures for the generation of a CA Key Pair.

<b>Term</b>	<b>Definition</b>
<b>Key Pair</b>	2 mathematically related Keys (a Private Key and its corresponding Public Key), having the properties that: (i) One Key can be used to encrypt a communication that can only be decrypted using the other Key; and (ii) even knowing one Key, it is computationally infeasible to discover the other Key.
<b>LDH Label</b>	From the <a href="#">RFC 5898</a> : “A string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string. Like all DNS labels, its total length must not exceed 63 octets.”
<b>Legal Entity</b>	An association, corporation, partnership, proprietorship, trust, Government Entity, or other entity with legal standing in a country’s legal system.
<b>Linting</b>	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 <a href="#">RFC 5280, Section 4.1.1.1</a> ) is checked for conformance with the profiles and requirements defined in the <a href="#">TLS BR</a> .
<b>Local Registration Agent (or LRA)</b>	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.
<b>Mailbox Address</b>	Also Email Address. The format of a Mailbox Address is defined as a “Mailbox” as specified in <a href="#">Section 4.1.2 of the RFC 5321</a> and amended by <a href="#">Section 3.2 of the RFC 6532</a> , with no additional padding or structure.
<b>Mailbox-Validated</b>	Refers to an S/MIME Certificate Subject that is limited to subject:emailAddress and/or subject:serialNumber attributes. In this CPS, these Certificate types: <ul style="list-style-type: none"> <li>• Secure Email Software</li> <li>• Secure Email Hardware</li> </ul>
<b>Multi-Perspective Issuance Corroboration</b>	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.
<b>Multipurpose Profile</b>	The S/MIME Multipurpose generation profiles are aligned with the more defined Strict Profiles, but with additional options for extKeyUsage and other extensions. This is intended to allow flexibility for crossover use cases between document signing and secure email.
<b>National Vulnerability Database (or NVD)</b>	A database that includes the Common Vulnerability Scoring System (CVSS) scores of security-related software flaws, misconfigurations, and vulnerabilities associated with systems (see <a href="https://nvd.nist.gov">https://nvd.nist.gov</a> ).
<b>Natural Person</b>	An Individual; a human being as distinguished from a Legal Entity.
<b>NetSec BR</b>	The most current version of the CA/B Forum “Network and Certificate System Security Requirements” published at: <a href="https://cabforum.org/network-security-requirements/">https://cabforum.org/network-security-requirements/</a>
<b>Network Perspective</b>	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.
<b>Non-EV Code Signing Certificate</b>	Certificates that contain Subject information as specified in the most current <a href="#">CS BR</a> for Non-EV Code Signing Certificates.



Term	Definition
	Non-EV Code Signing Certificates do not include jurisdiction of incorporation details in the Subscriber Certificate.
<b>Non-Reserved LDH Label</b>	From the <a href="#">RFC 5890</a> : “The set of valid LDH labels that do not have ‘-’ in the third and fourth positions.”
<b>Object Identifier (or OID)</b>	The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the PKI established by the TrustID CP and this CPS, they are used to uniquely identify Certificates issued under the TrustID CP and this CPS and the cryptographic algorithms supported.
<b>OCSP Responder</b>	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.
<b>Onion Domain Name</b>	A FQDN ending with the RFC 7686 “.onion” Special-Use Domain Name. For example, 2gzyxa5ihm7nsggfnu52rck2vv4rvmdlkiu3zzui5du4xycldn53wid.onion is an Onion Domain Name, whereas torproject.org is not an Onion Domain Name.
<b>Online Certificate Status Protocol (or OCSP)</b>	An online Certificate-checking protocol that enables Relying Party application software to determine the status of an identified Certificate (see also Online Status Check).
<b>Online Status Check</b>	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).
<b>Operational Period</b>	A Certificate’s actual term of validity, beginning with the start of the Validity Period and ending on the earlier of: <ul style="list-style-type: none"> <li>• The end of the Validity Period disclosed in the Certificate; or</li> <li>• The Revocation of the Certificate.</li> </ul>
<b>Organization(s)</b>	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).
<b>Organization-Validated</b>	Refers to an S/MIME Certificate Subject that includes only Organizational (Legal Entity) attributes, rather than attributes linked to an Individual. In this CPS, the TrustID FATCA Organization Certificate.
<b>OWASP Top Ten</b>	A list of application vulnerabilities published by the Open Web Application Security Project. See: <a href="https://owasp.org/www-project-top-ten/">https://owasp.org/www-project-top-ten/</a>
<b>Participants</b>	All PKI Service Providers and End Entities authorized to participate in the PKI defined by the CP and this CPS.
<b>Penetration Test</b>	A process that identifies and attempts to exploit openings and vulnerabilities on systems through the active use of known attack techniques, including the combination of different types of exploits, with a goal of breaking through layers of defenses and reporting on unpatched vulnerabilities and system weaknesses.
<b>Personal Certificate</b>	See Individual-Validated
<b>Personal Name</b>	Is the name of an Individual Subject typically presented as subject:givenName and/or subject:surname. However, the Personal Name may be in a format preferred by the Subject, the CA, or Enterprise RA as long as it remains a meaningful representation of the Subject’s verified name.
<b>Physical Identity Document</b>	A government-issued identity document issued in physical and human-readable form (such as a passport or national identity card).

<b>Term</b>	<b>Definition</b>
<b>PKI Service Providers</b>	The PMA, IdenTrust, Ras, CMAs, and Repositories participating in the PKI defined by the CP and this CPS.
<b>PKI Sponsor</b>	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: <ul style="list-style-type: none"> <li>• Signs and submits, or approves a request for a Certificate issued to an Electronic Device on behalf of the Organization, and/or</li> <li>• Signs and submits a Subscriber Agreement on behalf of the Organization, and/or</li> <li>• Acknowledges and agrees to the Certificate Terms of Use on behalf of the Organization when the Organization is an Affiliate of the CA (see <a href="#">Section 1.3.5.4</a>).</li> </ul>
<b>P-Label</b>	A XN-Label that contains valid output of the Punycode algorithm (as defined in the <a href="#">RFC 3492, Section 6.3</a> ) from the fifth and subsequent positions.
<b>PMA Charter</b>	The document adopted by the PMA that identifies the policies and procedures for administering the CP and this CPS.
<b>Policy</b>	The governing document that dictates the parties involved and requirements for these practices is listed in this Certification Practicing Statement.
<b>Policy Management Authority (PMA)</b>	The Organization responsible for setting, implementing, and administering Policy decisions regarding the TrustID CP and this CPS (also referred to in this CPS as Policy Authority).
<b>Precertificate</b>	A Precertificate is a signed data structure that can be submitted to a Certificate Transparency log, as defined by RFC 6962 and containing the critical poison extension (OID 1.3.6.1.4.1.11129.2.4.3).
<b>Primary Network Perspective</b>	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).
<b>Private Key</b>	The Key of a Key Pair kept secret by its holder, used to create Digital Signatures and to decrypt messages or files that were encrypted with the corresponding Public Key.
<b>Private Organization</b>	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.
<b>Pseudonym(s)</b>	A fictitious identity that a person assumes for a particular purpose. Unlike an anonymous identity, a pseudonym can be linked to the person's real identity.
<b>Public Key</b>	The Key of a Key Pair publicly disclosed by the holder of the corresponding Private Key and used by the recipient to validate Digital Signatures created with the corresponding Private Key and to encrypt messages or files to be decrypted with the corresponding Private Key.
<b>Public Key Cryptography</b>	A type of cryptography also known as asymmetric cryptography that uses a Key Pair to securely encrypt and decrypt messages.
<b>Public Key Infrastructure (or PKI)</b>	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based Public Key Cryptography system.
<b>Public Suffix</b>	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 <a href="#">Section 3.2.2.3.4</a> .
<b>Publicly-Trusted Certificate</b>	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.
<b>Qualified Auditor</b>	A Natural Person or Legal Entity that meets the requirements of <a href="#">Section 8.2</a> .

<b>Term</b>	<b>Definition</b>
<b>Random Value</b>	A value specified by a CA to the Domain Registrant that exhibits at least 112 bits of entropy.
<b>Reasonable Reliance</b>	<p>For purposes of the TrustID CP and this CPS, an Authorized Relying Party's decision to rely on a TrustID Certificate will be considered Reasonable Reliance if he, she, or it:</p> <ul style="list-style-type: none"> <li>• Has entered into an Authorized Relying Party Agreement and agreed to be bound by the terms and conditions of the TrustID CP and this CPS;</li> <li>• 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;</li> <li>• 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</li> </ul> <p>Used the TrustID Certificate for purposes appropriate under the TrustID CP, this 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.</p>
<b>Registration Agency</b>	<p>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</p> <ol style="list-style-type: none"> <li>i. a State Department of Corporations or a Secretary of State;</li> <li>ii. a licensing agency, such as a State Department of Insurance; or</li> <li>iii. 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.</li> </ol>
<b>Registration Authority (or RA)</b>	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.
<b>Registration Authority Agreement</b>	An agreement entered into between an entity and a CA authorizing the entity to act as an RA and detailing the specific duties and obligations of the RA, including but not limited to, the procedures for conducting appropriate Identity Proofing on potential End Entities.
<b>Registration Number</b>	The unique number assigned to a Private Organization by the incorporating agency in such entity's Jurisdiction of Incorporation.
<b>Registration Reference</b>	The unique number assigned to a Private Organization by the incorporating agency in such entity's Jurisdiction of Incorporation.
<b>Registration Scheme</b>	A scheme for assigning a Registration Reference meeting the requirements identified in <a href="#">Appendix A of the S/MIME BR</a> .
<b>Registry-Controlled Label</b>	A Public Suffix registered with a Domain Name Registrar.
<b>Reliable Data Source</b>	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.
<b>Reliable Method of Communication</b>	A method of communication, such as a postal/courier delivery address, telephone number, or Email Address, that was verified using a source other than the Applicant Representative.

<b>Term</b>	<b>Definition</b>
<b>Relying Party</b>	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.
<b>Remote Identity Proofing</b>	Remote Identity Proofing allows an authorized Individual to perform Identity Proofing via a video conferencing session, in lieu of conducting in-person Identity Proofing. <a href="#">NIST SP 800-63A Section 5.3.3</a> defines the parameters specific to Remote Identity Proofing and the methods in which the Identity Proofing event must occur. Based on the assurance level of the Certificate for which Remote Identity Proofing is being conducted, the session may be conducted in a supervised or an unsupervised session. See definitions for Supervised Remote Identity Proofing and Unsupervised Remote Identity Proofing for additional information regarding each Identity Proofing model. Refer to <a href="#">Section 3.2.3.2</a> for further definitions regarding Supervised versus Unsupervised Identity Proofing.
<b>Repository</b>	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.
<b>Request Token</b>	A value, derived in a method specified by the Issuing CA which binds this demonstration of control to the Certificate request.
<b>Required Website Content</b>	Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the Issuing CA.
<b>Reserved IP Address</b>	An Ipv4 or Ipv6 address that the IANA has marked as reserved: <a href="https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml">https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml</a> <a href="https://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml">https://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml</a>
<b>Revocation</b>	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).
<b>Root CA Certificate</b>	A Certificate at the beginning of a certification chain within the TrustID PKI hierarchy. This CA Certificate is established as part of the set-up and activation of IdenTrust. The Root CA Certificate contains the Public Key that corresponds to the CA Private Signing Key that IdenTrust uses to create or manage TrustID Certificates. Root 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 (see also Subordinate CA Certificate).
<b>Root Certificate</b>	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
<b>Root Key Generation Script</b>	A documented plan of procedures to be performed for the generation of the Root CA Key Pair
<b>S/MIME BR</b>	The most current version of the CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates published at: <a href="https://cabforum.org/smime-br/">https://cabforum.org/smime-br/</a>
<b>S/MIME Certificate</b>	Mailbox-Validated, Individual-Validated, Sponsor-Validated and Organization-Validated Certificates.
<b>SANS Top 25</b>	A list created with input from the SANS Institute and the Common Weakness Enumeration (CWE) that identifies the Top 25 most dangerous software errors that lead to exploitable vulnerabilities. See <a href="https://www.sans.org/top25-software-errors/">https://www.sans.org/top25-software-errors/</a>

<b>Term</b>	<b>Definition</b>
<b>Secure Email Software, Secure Email Hardware Certificates</b>	Also referred as Mailbox-Validated, a Certificate issued to an Email Address over which the Certificate Applicant demonstrates control to the RA by the Certificate Applicant responding to a unique challenge sent during the authentication process conducted before Issuance. A Secure Email Certificate can be used for the purposes of email signing, email encryption, and client authentication when installed on an approved hardware Cryptographic Module.
<b>Secure Room</b>	The room within the Datacenter 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.
<b>Security and Operations Manual</b>	A manual, handbook, or other publications in either hard copy or electronic form that outlines the security and general operations standards and rules for a particular PKI.
<b>Shared Secret</b>	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 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.
<b>Short-lived Subscriber Certificate</b>	For Certificates issued on or after 15 March 2024 and prior to 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 10 days (864,000 seconds). For Certificates issued on or after 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 7 days (604,800 seconds).
<b>Signing Authority</b>	An Organization that signs code on behalf of a Subscriber.
<b>Signing Service</b>	An organization that generates the Key Pair and securely manages the Private Key associated with a Code Signing Certificate, on behalf of a Subscriber.
<b>Split-Knowledge Technique</b>	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.
<b>Sponsoring Organization</b>	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.
<b>Sponsoring Organization Authorization Form</b>	The form used to provide information about an Affiliated Individual who will be authorized by an Organization to hold a TrustID Certificate.
<b>Sponsor-Validated / Business Certificate</b>	Refers to an S/MIME Certificate Subject which combines Individual (Natural Person) attributes in conjunction with a subject:organizationName (an associated Legal Entity) attribute. In this CPS, these Certificate types: <ul style="list-style-type: none"> <li>• Business</li> <li>• Business SHA-256</li> <li>• Business Hardware SHA-256</li> <li>• Medium Assurance Unaffiliated Hardware</li> </ul>
<b>Strict Profile</b>	The S/MIME Strict generation profiles are the long term target profile for S/MIME Certificates with extKeyUsage limited to id-kp-emailProtection, and stricter use of Subject DN attributes and other extensions.

<b>Term</b>	<b>Definition</b>
<b>Subject</b>	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.
<b>Subject Distinguished Name</b>	The specific field in a Certificate containing the unique name-identifier for the Subscriber.
<b>Subordinate CA</b>	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
<b>Subordinate CA Certificate</b>	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.
<b>Subscriber</b>	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.
<b>Subscriber Agreement</b>	An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
<b>Supervised Remote Identity Proofing</b>	<p>A real-time Identity Proofing event where the RA/Trusted Agent is not in the same physical location as the Applicant/Subscriber. The RA/Trusted Agent controls a device that is utilized by the Applicant/Subscriber in order to ensure the Remote Identity Proofing process employs physical, technical, and procedural measures to provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person Identity Proofing process.</p> <p>Supervised Remote Identity Proofing requires that a third person, in addition to the RA/TA and the Applicant, participate in the Identity Proofing event to attest to the Applicant's identity and act as a witness to the proceedings.</p> <p>Supervised Remote Identity Proofing is used for high assurance Certificate issuance.</p> <p>Refer to Remote Identity Proofing and Unsupervised Remote Identity Proofing for related information.</p> <p>Refer to <a href="#">Section 3.2.3.2</a> for further definitions regarding Supervised versus Unsupervised Identity Proofing.</p>
<b>Suspect Code</b>	Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, code that compromises user security and/or code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes.
<b>Technically Constrained Subordinate CA Certificate</b>	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.
<b>Terms of Use</b>	Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with this CPS when the Applicant/Subscriber is an Affiliate of the CA or is the CA.
<b>Timestamp Authority</b>	A service operated by the CA or a delegated third party for its own code signing certificate users that timestamps data using a certificate chained to a public root, thereby asserting that the data (or the data from which the data were derived via a secure hashing algorithm) existed at the specified time.
<b>Time-Stamping Certificate</b>	A Certificate used by a Time-Stamping Authority to time-stamp data, thereby asserting that the data existed at the specified time.



<b>Term</b>	<b>Definition</b>
<b>TLS BR</b>	The most current version of the CA/B Forum “ <i>Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates</i> ” published at: <a href="https://cabforum.org/working-groups/server/baseline-requirements/documents">https://cabforum.org/working-groups/server/baseline-requirements/documents</a> .
<b>Token</b>	A Cryptographic Module consisting of a hardware object (e.g., a “smart card”), often with memory and a microchip.
<b>Trusted Agent(s)</b>	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 <a href="#">Section 1.3.5.5</a> .
<b>Trusted Platform Module (or TPM)</b>	An international standard for a secure crypto-processor, which is a dedicated microprocessor designed to secure hardware by integrating cryptographic keys into devices.
<b>Trusted Role(s)</b>	A role involving functions that may introduce security problems if not carried out properly, whether accidentally or maliciously. The functions of Trusted Roles form the basis of trust for the entire PKI.
<b>TrustID Business, Business Software, Business Hardware Certificates</b>	TrustID Certificates considered as S/MIME Sponsor-Validated.
<b>TrustID Certificate</b>	A Certificate issued pursuant to the TrustID CP and this CPS.
<b>TrustID FATCA Organization Certificate</b>	TrustID Certificates considered as S/MIME Organization-Validated.
<b>TrustID Personal (Basic Individual) Software, Medium Assurance Individual Identity Software and Hardware Certificates</b>	TrustID Certificates considered as S/MIME Individual-Validated.
<b>Trustworthy System</b>	Computer hardware and software that: <ul style="list-style-type: none"> <li>• Are reasonably secure from intrusion and misuse;</li> <li>• Provide a reasonable level of availability; and</li> <li>• Are reasonably suited to perform their intended functions.</li> </ul>
<b>Unsupervised Remote Identity Proofing</b>	A real-time Identity Proofing event where the RA/Trusted Agent is not in the same physical location as the Applicant/Subscriber. The RA/Trusted Agent controls a device that is utilized by the Applicant/Subscriber in order to ensure the Remote Identity Proofing process employs physical, technical, and procedural measures to provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person Identity Proofing process. For Unsupervised Remote Identity Proofing, only the RA/Trusted Agent and the Applicant are required to participate in the session. Unsupervised Remote Identity Proofing may be used for Basic and Medium Assurance Certificate issuance. Refer to Remote Identity Proofing and Supervised Remote Identity Proofing for related information. Refer to <a href="#">Section 3.2.3.2.1</a> for additional details.
<b>Valid Certificate</b>	Certificate that passes the validation procedures specified in this CPS which are in line with the <a href="#">RFC 5280</a> .

Term	Definition
<b>Validation Specialist</b>	Someone who performs the information verification duties specified by the CA/B Forum BRs.
<b>Validity Period</b>	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 <a href="#">Section 4.1.2.5 of the he RFC 5280</a> : “The period of time from notBefore through notAfter, inclusive.”
<b>Vulnerability Scan</b>	A process that uses manual or automated tools to probe internal and external systems to check and report on the status of operating systems, services, and devices exposed to the network and the presence of vulnerabilities listed in the NVD, OWASP Top Ten, or SANS Top 25.
<b>WHOIS</b>	Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in the <a href="#">RFC 3912</a> , the Registry Data Access Protocol defined in the <a href="#">RFC 7482</a> , or an HTTPS website.
<b>Wildcard Certificate</b>	A Certificate containing an asterisk (*) in the left-most position of any of the Fully Qualified Domain Names contained in the Certificate.

### 1.6.2 Acronyms

Acronym	Definition
<b>AATL</b>	Adobe® Approved Trust List
<b>AO</b>	Authorizing Official
<b>ARL</b>	Authority Revocation List
<b>BR</b>	The CA/B forum Baseline Requirements
<b>CA</b>	Certification Authority
<b>CAA</b>	Certification Authority Authorization
<b>CIV</b>	Commercial Identity Verification
<b>CMA</b>	Certificate Manufacturing Authority
<b>CMC</b>	Certificate Management Center
<b>CMS</b>	Card Management System
<b>CN</b>	Common Name
<b>CP</b>	Certificate Policy
<b>CPS</b>	Certification Practice Statement
<b>CRL</b>	Certificate Revocation List
<b>CSA</b>	Certificate Status Authority
<b>DBA</b>	Doing Business As
<b>DN</b>	Distinguished Name
<b>DNS</b>	Domain Name System
<b>doS/DdoS</b>	Denial of Service/Distributed Denial of Service
<b>DSA</b>	Digital Signature Algorithm
<b>ECDSA</b>	Elliptic Curve Digital Signature Algorithm
<b>EKU</b>	Extended Key Usage
<b>EV</b>	Extended Validation



<b>Acronym</b>	<b>Definition</b>
<b>EWS</b>	Enrollment Workstation
<b>FATCA</b>	Foreign Account Tax Compliance Act
<b>FIPS</b>	Federal Information Processing Standard (U.S. Government)
<b>FQDN</b>	Fully Qualified Domain Name
<b>gTLD</b>	General Top-Level Domain
<b>ICANN</b>	Internet Corporation for Assigned Names and Numbers
<b>IRS</b>	Internal Revenue Service of the United States of America
<b>ISO</b>	International Standards Organization
<b>ITU</b>	International Telecommunications Union
<b>MRSP</b>	Mozilla Root Store Policy
<b>KED</b>	Key Escrow Database
<b>LRA</b>	Local Registration Agent
<b>NIST</b>	National Institute of Standards and Technology (U.S. Government)
<b>OCC</b>	Office of the Comptroller of the Currency
<b>OCSP</b>	Online Certificate Status Protocol
<b>OID</b>	Object Identifier
<b>PED</b>	PIN Entry Device
<b>PIN</b>	Personal Identification Number (e.g. a password)
<b>PIV</b>	Personal Identity Verification
<b>PIV-I</b>	Personal Identity Verification – Interoperable
<b>PKI</b>	Public Key Infrastructure
<b>PKIX</b>	IETF Working Group on Public Key Infrastructure
<b>PMA</b>	The IdenTrust Policy Management Authority
<b>PPP</b>	Policy Practices and Procedures
<b>QGIS</b>	Qualified Government Information Source
<b>QGTIS</b>	Qualified Government Tax Information Source
<b>RA</b>	Registration Authority
<b>RFPS</b>	Registration Practices Statements
<b>RSA</b>	Rivest-Shamir-Adleman cryptosystem
<b>SAN</b>	Subject Alternative Name
<b>S/MIME</b>	Secure /MIME (Secure/Multipurpose Internet Mail Extensions)
<b>SSP</b>	System Security Plan
<b>TLS</b>	Transport Layer Security
<b>TTL</b>	Time to Live
<b>URI</b>	Uniform Resource Identifier
<b>URL</b>	Uniform Resource Locator

Acronym	Definition
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

No stipulation.

### 1.6.4 Conventions

No stipulation.

## 2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

IdenTrust develops, implements, enforces and at least once annually, update its TrustID CP and CPS policy documents to ensure compliance with the latest approved version of the CA/B Forum BR as published at <https://cabforum.org> and/or in each browser's root store CA Policy as published on each root store website.

Incremental version numbering and date change log are present both on the title page of each document and in the Table of [Section 1.2](#) as evidence of annual review, even when no other changes are made to the document.

### 2.1 REPOSITORIES

IdenTrust 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://identrust.com>. The information is documented in this section and the Certificate Profiles [Section 7](#). See the next section for publication of Certificate revocation information.

TrustID Certificates issued by IdenTrust contain pointers to locations where Certificate-related information is published including CRLs, as specified by the TrustID CP (see [Section 2.3](#) for the frequency of publication of IdenTrust's Repository).

CRLs for Subordinate CA and Root CA Certificates are available at: <http://validation.identrust.com/crl/>.

Additionally, online Certificate status information is available through IdenTrust's TrustID validation services through OCSP. The validation services can be found at: <https://commercial.ocsp.identrust.com>.

### 2.2 PUBLICATION OF CERTIFICATION INFORMATION

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

- Copy of the TrustID CP;
- This CPS; and
- Other information related to IdenTrust (e.g., 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 CPS and the CP documents are structured in accordance with the [RFC 3647](#) and include all material required by the [RFC 3647](#).

This CPS and the CP conforms to the current version of the CA/B Forum BR published at <http://www.cabforum.org>. In the event of any inconsistency between this CP and CPS, the CA/B Forum BR, the CA/B Forum BR take precedence over this CPS and CP.

The following webpage is available for testing SSL/TLS Subscriber Certificates - valid, revoked, and expired - chaining up to the IdenTrust publicly trusted root: <https://testssl.identrust.com/>

#### 2.2.1 Interoperability

IdenTrust TrustID CA's adhere to the following requirements:

1. Operate a PKI that has undergone a successful compliance audit pursuant to Section 8 of the TrustID CP;
2. Issue Certificates interoperable with the profiles described in the TrustID CP, and make Certificate status information available in compliance with the TrustID CP; and
3. Provide CA Certificate and Certificate status information to the Authorized Relying Parties.

## **2.3 TIME OR FREQUENCY OF PUBLICATION**

All the information required by the TrustID CP to be published in the Repository is published as PDF immediately after such information is available to IdenTrust. TrustID Certificates are published immediately once they are accepted by the Subscriber. Information relating to the status of a TrustID Certificate is published in accordance with the TrustID CP.

When changes to the CP are implemented by the PMA, IdenTrust will codify these new practices into this CPS and publish it upon approval by the IdenTrust PMA. The published CP and CPS documents are tracked by incrementing the version number and adding a dated changelog entry, even if no other changes are made to the document.

The PMA also reviews and updates this CPS on an annual basis or more frequently when required, to include the most recent CA/B Forum BRs, and/or browser's root store Policy.

## **2.4 ACCESS CONTROLS ON REPOSITORIES**

IdenTrust does not impose any read access controls on the TrustID CP, IdenTrust's Root CA Certificate for its signing Key, this CPS, and annual WebTrust audits as well as Certificates and status information. IdenTrust does, however, impose access controls to ensure the authentication of Subscribers with respect to their Certificate(s) and the status of such Certificate(s) and personal registration information, which is separately managed from the public Certificate and status Repository. Access is restricted in accordance with [Section 9.4](#).

## 3 IDENTIFICATION AND AUTHENTICATION

### 3.1 NAMING

#### 3.1.1 Types of Names

IdenTrust only generates and signs Certificates that contain a non-null Subject Distinguished Name complying with the X.500 standard, and the CA/B Forum BR for naming. In such instance, when the Subject naming information is present only in the subjectAltName extension, then the Subject Distinguished Name must be an empty sequence and the subjectAltName extension must be marked as critical.

Names used in Certificates are X.501 Distinguished Names (DNs). Where DN's are required, Subscribers are assigned the appropriate DN's 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.

TrustID Certificates Identity Authentication Requirements	
TrustID Certificate Type	Identification Requirements
Secure Email	Identity shall be established by: Demonstration that the Applicant of the Certificate had control of the Applicant-provided Email Address at the time of email verification, based on <a href="#">Section 3.2.6.3</a> .
Personal / Individual	Identity shall be established by: Verification of the identity of the unaffiliated Applicant based on <a href="#">Section 3.2.3</a>
Business; Administrative CA for Administrators and Registration Authorities;	Identity shall be established by: Verification of the identity of the affiliated Applicant based on <a href="#">Section 3.2.3</a> Verification of the Organization based on <a href="#">Section 3.2.2.2</a>
FATCA Organization	Identity shall be established by: Verification of the Organization based on <a href="#">Section 3.2.2</a> .
Server Domain Validation (DV)	Identity for Domain Validation (DV) server Certificates are all be established by validating authorization and/or ownership by Domain Name Registrant and verification of country based on the applicable requirements set forth in the <a href="#">TLS BR</a> . When the Subject Distinguished Name is present, it must contain a single IP address or an FQDN that is one of the values contained in the Certificate subjectAltName extension.
Server Organization Validation (OV)	Identity for Organization Validation (OV) server Certificates is established by validating authorization and/or ownership by Domain Name Registrant and verification of the Subject Identity Information (i.e., identity, DBA/Tradename), the authenticity of the Certificate Request, verification of Individual authorized Applicant, as well as validation of the organization as a Legal Entity, and the locality/city, state and country of the organization as set forth in the <a href="#">TLS BR</a> .
Server Extended Validation (EV)	Identity for EV Server Certificates is established by performing the validations described above for OV server Certificates, as well as validation of the legal existence of the organization including attributes such as business category, jurisdiction, registration id, etc., as set forth in <a href="#">Section 3.2.2 of the EV TLS BR</a> .
Code Signing	Identity shall be established by: Verification of the Applicant's Organization in accordance with <a href="#">Section 3.2.2.1 of the CS BR</a> .

TrustID Certificates Identity Authentication Requirements	
TrustID Certificate Type	Identification Requirements
EV Code Signing	Identity shall be established by: Verification of the Applicant's Organization in accordance with <a href="#">Section 3.2.2.2 of the CS BR.</a>
Time-Stamping	Identity shall be established by: Verification of the Applicant's Organization per <a href="#">Section 3.2.2.1 of the CS BR.</a>
CIV Device	Identity shall be established by: Demonstration that the applicant of the certificate associated RA or the CA has assigned a unique name for identifying the Electronic Device containing a Cryptomodule. If an Organization name is included in this Certificate type, identity shall be established by performing name verification in accordance with <a href="#">Section 3.2.2.</a>
CIV Card Authentication	Identity shall be established by: Demonstration that the associated RA or the CA has assigned a unique name for identifying the Cryptographic Module.
Administrative CA for Authorized Relying Parties	Identity shall be established by: Verification of the identity of the Relying Party based on <a href="#">Section 3.2.3.10.</a>

When applications are transmitted electronically, via email or a website, the transmissions are secured via SSL/TLS or similar protocol, otherwise, applications may be submitted by postal mail or in person.

### 3.1.2 Need for Names to Be Meaningful

The contents of each Certificate contain a Subject extension, and within that extension there are common name, Organization name, Organization unit, Country, and Locality fields. Each of these fields has an association with the authenticated name of the End Entity. In the case of Individuals, the authenticated common name is a combination of first name, middle initial, and last name.

A Certificate issued for an Electronic Device includes the authenticated name of the Electronic Device including the dNSName containing the FQDN or IP Address legitimate owned or controlled by the Applicant and, if applicable, the name of the responsible Individual or Organization.

The entire Domain Namespace in wildcard Certificates must be rightfully controlled by the Subscriber Organization.

A Certificate issued as TrustID CIV Card Authentication Certificate or TrustID CIV Device Certificate will not contain an FQDN as the dNSName, or common name.

TrustID Certificate Type	Naming Requirements
Secure Email	The DN must include a validated Email Address provided in the emailAddress field. There is no common name included in the DN for this type of Certificate.
Personal	The DN must include an authenticated common name must be a combination of first name, surname, and optional initials.
Business; Administrative CA for Administrators and Registration Authorities;	In addition to the authenticated common name (as described above), the DN must also include the authenticated legal Subscribing Organization name in organizationName. Optionally, the organizationUnitName may be used to name the Subscribing Organization unit/department that is associated with the Subscriber, if provided by the Subscriber.

TrustID Certificate Type	Naming Requirements
Administrative CA for Authorized Relying Parties; TrustID FATCA Organization	
Server Domain Validation (DV)	Where the Subject Distinguished Name is empty, then the FQDN or a single IP address must be named in the subjectAltName and must be marked as critical. If the Subject Distinguished Name is present, then it will contain a single IP address or FQDN that is one of the values contained in the Certificate's subjectAltName extension.
Server Organization Validation (OV)	Where the Subject Distinguished Name is empty, then the FQDN must be named in the subjectAltName and must be marked as critical. The Subject Distinguished Name must be as set forth in <a href="#">Section 7.1.4.3.5</a> . If the Subject Distinguished Name is present, then it will contain a single IP address or FQDN that is one of the values contained in the Certificate's subjectAltName extension.
Server Extended Validation (EV)	If present, the Subject Distinguished Name must contain a single Domain Name(s) owned or controlled by the Subject and to be associated with the Subject's server. Such server may be owned and operated by the Subject or another entity (e.g., a hosting service). The Subject Distinguished Name fields are also subject to the requirements of <a href="#">Section 7.1.4.2 of the EV TLS BR</a> . Wildcard Certificates are not allowed for EV Server Certificates except unless the FQDN portion of the Wildcard Domain Name is an Onion Domain Name verified in accordance with <a href="#">Appendix B of the TLS BR</a> . If the Subject Distinguished Name is present, then it will contain a single IP address or FQDN that is one of the values contained in the Certificate's subjectAltName extension.
Code Signing	The Subject Distinguished Name must conform to the Certificate profile as outlined in <a href="#">Section 7.1.4.3.7</a> Non-EV Code Signing and <a href="#">Section 7.1.4.3.8</a> EV Code Signing.
Time-Stamping Authority	Time-Stamping Authority Certificates are issued to IdenTrust and used in conjunction with the Time-stamping Authority Server service. The Subject Distinguished Name must conform to the Certificate profile as outlined in <a href="#">Section 7.1.4.3.9</a> Time-Stamping of the TrustID CPS.
CIV Device	The DN for device must include a unique name populated in the common name that identifies the Electronic Device that will contain the associated Cryptographic Module.
CIV Card Authentication	TrustID CIV Card Authentication Certificates must include a unique name for identifying the associated Cryptographic Module.

### 3.1.3 Anonymity or Pseudonymity of Subscribers

For human Subscribers, IdenTrust TrustID Certificates do not contain anonymous or Pseudonym identities.

Server Domain Validation (DV) Certificates, Device Certificates, and Secure Email Certificates do not name a Subscriber; rather these types of Certificates have subject fields identifying only Domain Names, device identification or Email Addresses, respectively (not people or organizations). For these types of Certificates, relying parties may consider the Certificate Subscriber to be anonymous.

All Certificates must meet the requirements for name uniqueness as defined in [Section 3.1.5](#) of this 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. Email names in the SAN extension are interpreted using the [RFC 5322](#), (formerly the [RFC 822](#)), specifying the

format of Internet email messages. Email Addresses and FQDNs can be resolved through Domain Name services (DNS). Sections 4.1.2.4 and 4.2.1.7 of the [RFC 5280](#) describe how character sets and strings are to be interpreted in Issuer and Subject fields, and Subject Alternative Name (SAN) extension. The [RFC 2253](#) explains how an X.500 distinguished name in ASN.1 is translated into a UTF-8 human-readable string representation, and the [RFC 2616](#) explains how to interpret Uniform Resource Identifiers (URIs) for HTTP references.

#### **3.1.4.1 Non ASCII Character Substitution**

IdenTrust may include an ASCII character name that is not a direct conversion of the Applicant's registered name provided that it is verified in a Reliable Data Source or suitable Attestation Letter.

#### **3.1.4.2 Geographic Names**

IdenTrust may use geographic endonyms and exonyms in the subject:localityName and subject:stateOrProvinceName attributes, (e.g., Munich, Monaco di Bavaria, or Мюнхен for München). IdenTrust avoids the use of archaic geographic names, (e.g., prefer Mumbai over Bombay).

#### **3.1.5 Uniqueness of Names**

Name uniqueness within the IdenTrust TrustID space is enforced by IdenTrust's CA. IdenTrust and RAs enforce name uniqueness within the X.500 namespace for which they have been authorized. When other name forms are used, they too are allocated such that name uniqueness across the TrustID system is ensured.

IdenTrust uses the following name forms and allocates names within the Subscriber community to guarantee name uniqueness among current and past Subscribers for all Certificates:

- Name uniqueness is enforced through the use of an additional naming attribute that is part of the Subscriber's Subject DN. This attribute is 2.5.4.5, which is the OID for the subject:SerialNumber.
- The subject:SerialNumber value, along with the common name of the Subscriber, guarantees the uniqueness of the Certificate in the Repository.
- For server Certificates the uniqueness of the Subject DN is ensured by the inclusion of the FQDN after verification of its registration with the Domain Registrar. The uniqueness of a Domain Name is controlled by Internet Corporation for Assigned Names and Numbers (ICANN).
- For Time-Stamping Certificates, the uniqueness of the Subject DN is ensured by the inclusion of the Signing Authority name as verified per [Section 3.2](#) along with a unique serial number.
- As other methods and standard practices of guaranteeing name uniqueness emerge, to increase application interoperability of Certificates, IdenTrust may implement these as well.

##### **3.1.5.1 Human / Personal Certificates**

For human Certificates issued by the Issuing CA, the Subject Name identified in a TrustID Certificate shall be unambiguous and must conform to X.500 standards for name uniqueness. If necessary, additional numbers or letters may be appended to the real name to ensure the name's uniqueness within the domain of TrustID Certificates issued by the Issuing CA. Each name shall be unique for a single Subscriber. A CA may issue more than one Certificate with the same unique name to the same Subscriber. In addition, the name must contain the Subscriber identity and organization affiliation (if applicable) that is meaningful to humans;

##### **3.1.5.2 Secure Email (S/MIME) Certificates**

Subscribers are not named in Secure Email (S/MIME) Certificates. The validated Email Address is populated in the DN emailAddress field.



Name uniqueness is established by providing a Global Unique Identifier (GUID) that is generated by the Issuing CA.

### **3.1.5.3 CIV Card Authentication and CIV Device Certificates**

The device name and serial number are used to ensure the uniqueness of the name.

### **3.1.5.4 Server Certificates**

By nature, a Fully Qualified Domain Name (FQDN) is unique. The FQDN is included in either the DN common name or the subjectAltName. However, this does not prevent devices from sharing a Fully Qualified Domain Name (FQDN) as the common name.

Wildcard forms are allowed, subject to the restrictions imposed by Application Software Suppliers programs.

### **3.1.5.5 Code Signing Certificates**

For Code Signing Certificates, the uniqueness of the Subject DN is ensured by the inclusion of the Organization's name or DBA as verified per [Section 3.2](#) along with a unique serial number.

### **3.1.5.6 Time-Stamping Certificates**

For Time-Stamping Certificates, the uniqueness of the Subject DN is ensured by requiring a unique hash and time or unique serial number assigned to the time-stamped event.

## **3.1.6 Recognition, Authentication, and Role of Trademarks**

Applicants are prohibited from using names or marks that infringe upon the intellectual property rights of others. An 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. A Certificate will not be revoked merely because there is another rightful owner of a name or mark when the Subject Name is sufficient for identification within the PKI and are non-infringing or otherwise not deceptive. Without incurring any liability to an Applicant PKI Sponsor or Subscriber, IdenTrust may reject any application or revoke a Certificate because of a name or trademark dispute.

IdenTrust is not required to subsequently issue a new TrustID Certificate to the rightful owner of any name if IdenTrust has already issued to that owner a TrustID Certificate containing a Subject Name that is sufficient for identification within the PKI.

Any Participant aggrieved by a decision may proceed under the Dispute Resolution Procedures outlined in Section 9.13 of the TrustID CP. If it is determined that the intellectual property rights of a third party have been infringed because a Subscriber provided incorrect information to receive the infringing name or mark in its Certificate, that Subscriber hereby agrees to indemnify and hold IdenTrust harmless for any losses or damages arising out of the use of such name or mark.

### **3.1.6.1 Name Claim Dispute Resolution Procedure**

IdenTrust reserves the right for its PMA to make all decisions regarding End Entity names in TrustID Certificates. If necessary, a party requesting a TrustID Certificate may be required to demonstrate its right to use a particular name. IdenTrust PMA will investigate and correct, if necessary, any name collisions brought to its attention.

## 3.2 INITIAL IDENTITY VALIDATION

IdenTrust 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. RAs may designate one or more employees or agents, to be referred to as LRAs, and Trusted Agents may be nominated by Sponsoring Organizations and appointed by IdenTrust or an RA to perform Identity Proofing in accordance with [Section 3](#) including [Section 3.2.1](#) proving possession of the Applicant/PKI Sponsor generated Private Key, the verification of information provided by the Applicant/PKI Sponsor based on [Section 3.2.4](#), and all requirements as follows below:

TrustID Certificates Initial Identity Validation Requirements	
Certificate Type	Identification Requirements
Secure Email	Demonstration of the Applicant’s control of the Email Address at the time of Email Address verification, based on <a href="#">Section 3.2.6.3</a> .
Personal	Verification of the identity of the unaffiliated Applicant based on <a href="#">Section 3.2.3</a> and the performance of an Electronic Identification based on <a href="#">Section 3.2.3.4</a> or the performance of in-person or Unsupervised Remote Identity Proofing based on <a href="#">Section 3.2.3.2</a> ; and Verification of Email Address based on <a href="#">Section 3.2.6.3</a> .
Business	Verification of the affiliated Applicant based on <a href="#">Section 3.2.3</a> and performance of in-person or Unsupervised Remote Identity Proofing based on <a href="#">Section 3.2.3.2</a> ; Verification of the Organization based on <a href="#">Section 3.2.2</a> ; Verification of Individual-Organization affiliation based on <a href="#">Section 3.2.2.1</a> ; Verification of Email Address based on <a href="#">Section 3.2.6.3</a> ; and Verification of a Certificate request based on <a href="#">Section 3.2.6.4</a> .
FATCA Organization	Verification of the Organization based on <a href="#">Section 3.2.2</a> ; Verification of Email Address based on <a href="#">Section 3.2.6.3</a> ; and Verification of a Certificate request based on <a href="#">Section 3.2.6.4</a> .
Server *	Verification of the Organization based on <a href="#">Section 3.2.2</a> ; Verification of the PKI Sponsor’s Organization affiliation based on <a href="#">Section 3.2.2.3</a> ; Verification of a Certificate request based on <a href="#">Section 3.2.6.4</a> ; Authentication of a Device identity based on <a href="#">Section 3.2.2.6</a> ; Verification against high-risk and denied request lists based on <a href="#">Section 4.2.2.2</a> ; Verification of the authorization by Domain Name Registrant based on <a href="#">Section 3.2.2.5</a> . Verification of DBA/Tradename based on <a href="#">Section 3.2.2.3.1</a> ; Verification of country code based on <a href="#">Section 3.2.2.3.2</a> ; Verification of control over entire namespace delimited by the FQDN of wildcard Certificate on <a href="#">Section 3.2.2.3.4</a> ; Verification of Email Address based on <a href="#">Section 3.2.6.3**</a> ; and Verification of IP address based on <a href="#">Section 3.2.2.5</a> . In addition to these applicable requirements, adherence to the applicable requirements listed in the <a href="#">TLS BR</a> .
EV Server*	In addition to the applicable verification requirements for the server Certificate listed above, adherence to the requirements listed in <a href="#">Section 3.2.2 of the EV TLS BR</a> and the Subscriber Agreement on <a href="#">this webpage</a> listed in the “Agreements” Section as “TrustID

TrustID Certificates Initial Identity Validation Requirements	
Certificate Type	Identification Requirements
	IdenTrust SSL/TLS Organization Identity Extended Validated (EV) Subscriber Agreement <sup>1</sup> , which includes defined roles.
Code Signing and Time-Stamping*	A TrustID Code Signing Certificate, or TrustID Time-Stamping Certificate identifies an Organization as the Subject of a Certificate, and such Organization is attributable for the purposes of accountability and responsibility for signatures created by the Organization to be used to verify the integrity of its code. When issuing a TrustID Code Signing Certificate, or a TrustID Time-Stamping Certificate, the Issuing CA shall conform with the applicable provisions set forth in <a href="#">Section 3.2 of the CS BR</a> and verification of the Email Address based on <a href="#">Section 3.2.6.3</a>
CIV Device Certificate	Demonstration that the Applicant of the Certificate, associated RA, or the CA has assigned a unique name for identifying the Electronic Device containing a Cryptographic Module.
CIV Card Authentication Certificate	Demonstration that the associated RA or the CA has assigned a unique name for identifying the Cryptographic Module.
Administrative RA Certificates	The Subscriber's identity must be established by the Authorized Official (AO). The AO is an elected representative of the Organization requesting an Administrative RA Certificate. This Individual must be bound by the Organization's agreement between the Organization and the Issuing CA. An Organization may have more than one AO but must provide a list including each AO to the Issuing CA for verification purposes.
Authorized Relying Parties	Identification and authentication of Authorized Relying Parties may be performed by the Issuing CA and RAs as a consequence of the enrollment process by which an Authorized Relying Party enters into an Authorized Relying Party Agreement with the Issuing CA.

\*All documents and data provided for verifying the server Certificate must not be used by the RA if the document or data was obtained no more than 825 days prior to issuing the Certificate or in the case of EV Server Certificates and EV Code Signing Certificates, the age of all data used to support renewals will not exceed the period specified in [Section 3.2.2.14.3 of the EV TLS BR](#).

For validation of Domain Names and IP Addresses any reused data, document, or completed validation are obtained no more than 398 days prior to issuing the Certificate.

\*\*This check is only performed when necessary for server Certificates. It will be performed when the profile of the requested server Certificate specifies an Email Address, which requires verification.

### 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 4.4](#). 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.

Private Keys are generated by the Applicant/PKI Sponsor: 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. The IdenTrust PMA has determined the use of Private Keys for Certificates to create a Digital Signature only in a PKCS#10 for the purpose of establishing proof of possession is an acceptable use of such Private Key.

In the case where Key Generation is performed by IdenTrust or an RA either (1) directly on the Subscriber's hardware or software Cryptographic Module, or (2) in a Key generator that benignly transfers the Key to the party's Cryptographic Module, then proof of possession is not required. If the End Entity is not in possession of the Token when the Key is generated, then the Token will be delivered immediately to the End Entity via a trustworthy and accountable method.

### **3.2.1.1 Binding Identity and Public Key**

IdenTrust ensures that the Applicant's identity information and Public Key are adequately bound. This association is established by the use of an Account Password, exchanged between the Applicant and the IdenTrust RA via a secure referral process.

### **3.2.2 Authentication of Organization 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;
- Unique identifier and type of identifier for the Legal Entity;\*
- A Legal Entity Identifier (LEI) data reference;\*
- Full business address;
- Telephone number;
- Proof of good standing in the jurisdiction where the Applicant is incorporated or otherwise organized; and
- The unique organization identifier shall be included in the Certificate subject:organizationIdentifier as specified in the Certificate Profile.

\* for S/MIME Sponsor-Validated and Organization-Validated Certificates.

IdenTrust or RA may use the same documentation listed above to verify both the Applicant's identity and address, and that the status of the Applicant is not designated by labels such as "ceased", "inactive", "invalid", "not current" or the equivalent. When an LEI data reference is used, IdenTrust or the RA shall verify that the RegistrationStatus is ISSUED and the EntityStatus is ACTIVE. IdenTrust only allows the use of an LEI when the ValidationSources entry is FULLY\_CORROBORATED.

Applicants may request an Assumed Name to be included in the Certificate. IdenTrust or RA shall verify that:

1. The Applicant has registered its use of the Assumed Name with the appropriate government agency for such filings in the jurisdiction of its incorporation or registration; and
2. The Assumed Name filing continues to be valid.

IdenTrust may rely on an Attestation Letter that indicates the Assumed Name under which the Applicant conducts business, the government agency with which the Assumed Name is registered, and that such filing continues to be valid.

The sponsoring Organization information is verified by cross-checking it with trusted information in a database of user-supplied business information, from a third party vendor of such business information, or from the Organization's financial institution references. IdenTrust LRA and/or the RA will evaluate the data source's accuracy and reliability. IdenTrust and the RA will not use a data source to verify Sponsoring Organization if the data source is deemed not reasonably accurate or reliable as per requirements listed in [Section 3.2.4](#).

Disconnected phone service and other insufficient, false, or suspicious information provided by the Sponsoring Organization warrants further investigation. If requested follow-up information is not forthcoming, or if an Applicant or PKI Sponsor refuses to produce any such requested information, the Certificate application will not be approved. The LRA may rely on information previously obtained concerning the Sponsoring Organization for the Identity Proofing and the RA and IdenTrust will keep a record of the type and details of information used for verifying identity.

### **3.2.2.1 Authentication of the Individual-Organization Affiliation**

IdenTrust will 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 Business and 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 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.

In the case of Sponsor-Validated Certificates approved by an Enterprise RA, records maintained by the Enterprise RA shall be accepted as evidence of Individual identity.

IdenTrust issues Personal Certificates to Individuals having no organizational affiliation, or who are acting in a personal capacity and not a professional capacity; in this case, the authentication of the Application-Organization affiliation is not required and the practices explained in this section are not executed.

When processing EV Server Certificates, additional checks are performed based on [Section 3.2.2.11 of the EV TLS BR](#).

When processing EV Code Signing Certificates, additional checks are performed based on [Section 3.2.2.10 of the CS BR](#).

### **3.2.2.2 Authentication of Subscribing Organization Identity**

Before approving the inclusion of Sponsoring Organization information in a Certificate, the LRA will verify 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.

Additional checks will be in place based on requirements listed in [Section 3.2.2.4 of the EV TLS B.R.](#)

### **3.2.2.3 Authentication of the PKI Sponsor-Organization Affiliation**

IdenTrust issues Certificates to Electronic Devices owned or controlled by a Sponsoring Organization. A PKI Sponsor represents the Subscribing Organization during the application, retrieval, and management processes for a Certificate issued to an Electronic Device, and the PKI Sponsor’s affiliation to the Sponsoring Organization is verified before Issuance of the Certificate.

For Certificates issued to a Sponsoring Organization and requested by a PKI Sponsor, LRAs and Trusted Agents will not approve Issuance of a Certificate without obtaining verification of the existence of affiliation between the Sponsoring Organization and the PKI Sponsor. 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.

For PKI Sponsors requesting a TrustID Server Organization Validation or TrustID EV Server Certificates, IdenTrust or the RA obtains approval of the Issuance by the Sponsoring Organization that owns the Domain Name using the procedures explained in [Section 3.2.2.4](#). The approval enables the Sponsoring Organization to manage its internal PKI and infrastructure.

PKI Sponsors have control over the Private Key of a Certificate, and Digital Signatures can be created with such Certificate; however, whether a Digital Signature can be viewed as the Sponsoring Organization’s signature



depends on whether the PKI Sponsor as an Individual has the authority to use the Certificate 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.

IdenTrust or the RA records confirmations performed in this section in an auditable log.

### **3.2.2.3.1 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 system. If the information is obtained through a phone call, the LRA must document 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.

### **3.2.2.3.2 Verification of Country Code**

The LRA will verify 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](http://www.identrust.uk) as opposed to [www.identrust.com](http://www.identrust.com)), this confirmation will be sought from the Domain Name level to which the ccTLD applies. This means that the LRA cannot obtain verification from [www.identrust.com](http://www.identrust.com) if the PKI Sponsor is applying for a Domain Name from [www.identrust.uk](http://www.identrust.uk).

PKI Sponsors requesting a Certificate that will contain the countryName field and the other Sponsoring Organization will be verified by the LRA 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.

### **3.2.2.3.3 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.

#### **3.2.2.3.4 Verification of Control Over Entire Namespace Delimited by FQDN of a Wildcard Certificate**

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 Registry-Controlled Label 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/>. As a further example, the FQDN "\*.highland.k12.ut.us" may be accepted pending the verifications described in [Section 3.2.2.3.3](#).

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 [Section 3.2.2.3.3](#) will be completed first and the Subscribing Organization will provide written assertions about the rightful control over the entire Domain Namespace.

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

Before issuing a server 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 BRs version number used.

Additional checks and verification will be made for EV Server Certificate applications based on the requirements in [Section 3.2.2 of the EV TLS BR](#).

Code Signing Certificates are excluded from this validation as they do not include Domain Names.

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

This domain validation method is not used by IdenTrust.

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

The LRA confirms the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value is sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact.

Each email, fax, SMS, or postal mail may confirm control of multiple Authorization Domain Names.

The LRA may send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email, fax, SMS, or postal mail.

The Random Value shall be unique in each email, fax, SMS, or postal mail.

The LRA may send the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and 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.

**Note:** Once the FQDN has been validated using this method, the LRA 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.

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

This domain validation method is not used by IdenTrust.

#### **3.2.2.4.4 Constructed Email to Domain Contact**

The LRA confirms the Applicant's control over the FQDN by

- (i) 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
- (ii) including a Random Value in the email, and
- (iii) 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, the LRA 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.

#### **3.2.2.4.5 Domain Authorization Document**

This domain validation method is not used by IdenTrust.

#### **3.2.2.4.6 Agreed-Upon Change to Website**

This domain validation method is not used by IdenTrust.

#### **3.2.2.4.7 DNS Change**

The LRA confirms the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either 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, the LRA shall provide a Random Value unique to the Certificate request and shall not use the Random Value after i. 30 days or ii. 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 of the TLS BR](#) or [Section 3.2.2.14.3 of the EV TLS BR](#)).

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

**Note:** Once the FQDN has been validated using this method, the LRA 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**

The LRA confirms the Applicant’s control over the FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with [Section 3.2.2.5](#).

When using this method, the LRA implements Multi-Perspective Issuance Corroboration as specified in [Section 3.2.2.9 of the TLS BR](#). To count as corroborating, a Network Perspective must observe the same IP address as the Primary Network Perspective.

**Note:** Once the FQDN has been validated using this method, the LRA does not issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the LRA performs a separate validation for that FQDN using an authorized method. This method is not suitable for validating Wildcard Domain Names.

#### **3.2.2.4.9 Test Certificate**

This domain validation method is not used by IdenTrust.

#### **3.2.2.4.10 TLS Using a Random Value**

This domain validation method is not used by IdenTrust.

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

This domain validation method is not used by IdenTrust.

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

This domain validation method is not used by IdenTrust.

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

This domain validation method is not used by IdenTrust.

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

This domain validation method is not used by IdenTrust.

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

This domain validation method is not used by IdenTrust.

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

This domain validation method is not used by IdenTrust.

#### **3.2.2.4.17 Phone Contact with DNS CAA Phone Contact**

This domain validation method is not used by IdenTrust.

#### **3.2.2.4.18 Agreed-Upon Change to Website v2**

The LRA 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. The LRA 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.
  - a) Redirects must be the result of a 301, 302, or 307 HTTP status code response, as defined in the [RFC 7231, Section 6.4](#), or a 308 HTTP status code response, as defined in the [RFC 7538, Section 3](#). Redirects must be to the final value of the Location HTTP response header, as defined in the [RFC 7231, Section 7.1.2](#).
- 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:

1. IdenTrust must provide a Random Value unique to the Certificate request.
2. 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, the LRA using this method implements Multi-Perspective Issuance Corroboration as specified in [Section 3.2.2.9 of the TLS BR](#). 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:** The LRA must not issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the LRA performs a separate validation for that FQDN using an authorized method. This method is not suitable for validating Wildcard Domain Names.

#### **3.2.2.4.19 Agreed-Upon Change to Website - ACME**

This domain validation method is not used by IdenTrust.

#### **3.2.2.4.20 TLS Using ALPN**

This domain validation method is not used by IdenTrust.

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

IdenTrust as 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](#) for server Certificates, 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**

The LRA confirming 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
  - a. 30 days or
  - b. 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](#) for server Certificates.

The LRA using this method must implement Multi-Perspective Issuance Corroboration as specified in [Section 3.2.2.9 of the TLS BR](#). 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**

The LRA 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.

The LRA 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.

The LRA 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.

### **3.2.2.5.3 Reverse Address Lookup**

This IP Address validation method is not used by IdenTrust.

### **3.2.2.5.4 Any other Method**

This IP Address validation method is not used by IdenTrust.

### **3.2.2.5.5 Phone Contact with IP Address Contact**

This IP Address validation method is not used by IdenTrust.

### **3.2.2.5.6 ACME "http-01" method for IP Addresses**

This IP Address validation method is not used by IdenTrust.

### 3.2.2.5.7 ACME “http-01” method for IP Addresses

This IP Address validation method is not used by IdenTrust.

### 3.2.2.6 Wildcard Domain Validation

Before issuing a Wildcard Certificate, IdenTrust establishes and follows a documented procedure that determines if the FQDN portion of any Wildcard Domain Name in the Certificate is “registry-controlled” or is a “public suffix” (e.g. “\*.com”, “\*.co.uk”, per [RFC 6454 Section 8.2](#)).

If the FQDN portion of any Wildcard Domain Name is “registry-controlled” or is a “public suffix”, IdenTrust refuses issuance unless the Applicant proves its rightful control of the entire Domain Namespace. (e.g. do not issue “\*.co.uk” or “\*.local” but may issue “\*.example.com” to Example Co.).

See [Section 3.2.2.3.3](#) Verification of gTLD Domains

### 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.

For S/MIME certificates, Enterprise RA records are Reliable Data Source for individual subject attributes included in Sponsor-Validated Certificates issued to the Enterprise RA’s Organization.

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. CAA Records

#### 3.2.2.7.1 Server Certificates

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 the TLS BR](#)) or IP address(es) (see [Section 3.2.2.5 of the TLS BR](#)) 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 of the TLS BR](#).) 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:.

### **3.2.2.7.2 S/MIME Certificates**

Prior to issuing a Certificate that includes a Mailbox Address, IdenTrust should retrieve and process CAA records in accordance with [Section 4 of RFC 9495: Certification Authority Authorization \(CAA\) Processing for Email Addresses](#).

Starting on March 15, 2025, prior to issuing a Certificate that includes a Mailbox Address, IdenTrust shall retrieve and process CAA records in accordance with [Section 4 of RFC 9495: Certification Authority Authorization \(CAA\) Processing for Email Addresses](#).

When processing CAA records, IdenTrust shall process the issuemail property tag as specified in RFC 9495. Additional property tags may be supported but shall not conflict with or supersede the authorizations to issue S/MIME Certificates as specified in the issuemail property tag.

If IdenTrust issues a Certificate following a CAA check, it will do so within the TTL of the CAA record, or 8 hours, whichever is greater. This stipulation does not prevent IdenTrust from checking CAA records at any other time.

If the Certificate includes more than one Mailbox Address, then IdenTrust shall perform the above procedure for each Mailbox Address.

CAA checking is optional for Certificates issued by a Technically Constrained Subordinate CA Certificate as set out in [Section 7.1.5 of the S/MIME BR](#), where the lack of CAA checking is an explicit contractual provision in the contract with the Technically Constrained Subordinate CA Applicant.

IdenTrust shall not issue a Certificate unless IdenTrust determines that Certificate Request is consistent with the applicable CAA RRset. IdenTrust shall log all actions taken, if any, consistent with its CAA processing practice.

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

- the failure is outside of the CA’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.

### **3.2.2.8 Authentication of CIV Device Identity**

Certificates for Electronic Devices are issued to an application or server. IdenTrust issues Certificates of different server types such as SSL/TLS, VPN, and OCSP Responders based on the completion of required Identity Proofing for each Certificate type set forth in [Section 3.2](#). Servers and applications are identified using a Fully Qualified Domain Name.

A TrustID Certificate request identifying an Electronic Device as the Subject of a Certificate may only be made by a PKI Sponsor of the Sponsoring Organization for whom the Electronic Device's signature is attributable for the purposes of accountability and responsibility. The Certificate will be issued by IdenTrust once the application can be fully verified by the Identity Proofing process specified by this CPS. By following these procedures of Identity Proofing, IdenTrust seeks to reduce the likelihood that the information contained in the Certificate Profile is misleading.

### **3.2.2.9 Code Signing Certificates**

Likewise, checks and verifications will be made for Non-EV Code Signing and EV Code Signing Certificate applications based on the requirements of [Section 3.2.2 of the CS BR](#).

The Subject Distinguished Name must conform to the Certificate profile as outlined in [Section 7.1.4.3.7](#) Non-EV Code Signing, [Section 7.1.4.3.8](#) EV Code Signing and [Section 7.1.4.3.9](#) Time-Stamping.

### **3.2.2.10 CIV Card Authentication Certificate and CIV Device Certificates**

For TrustID CIV Card Authentication Certificates and TrustID CIV Device Certificates, the Certificate will be issued by IdenTrust once either the PKI Sponsor or an RA or IdenTrust itself assigns a unique identifier to the corresponding Cryptographic Module. For TrustID CIV Device Certificate, the assigned unique identifier may identify an Electronic Device.

### **3.2.2.11 Authentication of TrustID Administrative RA Certificates for Devices and Individuals**

For TrustID Administrative RA Certificates for Electronic Devices and Individuals, identity is established by the Authorized Official (AO). The AO is an elected representative of the Organization requesting an Administrative RA Certificate. This Individual is bound by the Organization's agreement between the Organization and IdenTrust. An Organization may have more than one AO but must provide a list including each AO to IdenTrust for verification purposes.

An authorization form must be sent with the application signed by the AO. Certificate authorization forms are verified by IdenTrust. Information provided on the online application and the authorization form is checked by an LRA to ensure that the AO is listed with IdenTrust. This verification will occur before the Certificate is issued.

These types of Certificates are not issued to Enterprise RAs. Enterprise RAs are issued an IdenTrust TrustID Business Certificate after successful I&A as listed in [Section 3.2](#). To perform the duties of an Enterprise RA, a TrustID Business Certificate must be obtained and an Enterprise RA addendum signed.

## **3.2.3 Authentication of Individual Identity**

The Issuance of a TrustID Certificate is based upon IdenTrust, or RA Enterprise authenticating the identity of the Applicant as explained in this and the following sections. The authentication process requires the collection and



verification of the Applicant’s information. Both information collection and verification may be performed either in-person, via Remote Identity Proofing, or through automated processes<sup>1</sup>.

The number and types of identification documents (IDs), the process documentation, and the authentication requirements for Issuance of a Certificate shall depend upon the type of Certificate as set forth in the table below:

TrustID Certificates Individual Identity Authentication Requirements	
TrustID Certificate Type	Description
Personal Basic Individual Software Medium Assurance Individual Identity Software and Hardware	Identity is established by: Verification and validation of identity information provided by the Applicant, including out-of-band confirmation <sup>2</sup> , performed in accordance with <a href="#">Section 3.2.6.2</a> ; Contemporaneous in-person or Remote Identity Proofing consists of a review of at least two acceptable forms of ID, one of which shall be a government-issued photo-ID (see <a href="#">Section 3.2.3.1</a> ), performed in accordance with performance of <a href="#">Section 3.2.3.2</a> .
Business Software Business Hardware Business Card Authentication	The Sponsoring Organization confirms the Affiliated Individual's affiliation with the Sponsoring Organization. For non-Enterprise Subscribers, the CA or RA may verify the authority or affiliation of an Individual to represent an Organization to be included in the subject:organizationName of the Certificate using an Attestation Letter provided by the Organization and verified in accordance with <a href="#">Section 3.2.6.5</a> . In the case of Sponsor-Validated Certificates approved by an Enterprise RA, The RA shall validate all identity attributes of an Individual to be included in the Certificate. The RA may rely upon existing internal records to validate Individual Identity. The Enterprise RA shall maintain records to satisfy the requirements of <a href="#">Section 1.3.2.1</a> .

The order in which the authentication steps are followed and how they are performed, in-person or automatically, are driven by the Certificate type and specific implementations.

The information that is collected includes:

- Applicant name as appears in the Certificate’s CN attribute;
- Method of application (e.g., online, in-person, remote);
- For each data element accepted for verification, including electronic forms:
  - Name of the document presented for Identity Proofing;
  - Issuing authority;
  - Date of Issuance;
  - Date of expiration;
  - All fields verified;
  - Source of verification (i.e., which sources are used for cross-checks);
  - Method of verification (e.g., online, in-person, remote); and,
  - Date of verification.
- Identity of the person performing the verification, including names of contractors, subcontractors or entities providing identification services, if any;
- Any associated error messages and codes; and

<sup>1</sup> Effective September 1, 2023, the process of electronic individual Identity verification has been discontinued.

<sup>2</sup> Issued before September 1, 2023

- Date/time of process completion.

If the Applicant fails identity verification by the LRA, IdenTrust or the RA will not approve the application.

To ensure that the Applicant's identity information, its validation, and the Public Key are properly bound, IdenTrust maintains a Subscriber account that is protected by an Account Password provided by the Applicant/PKI Sponsor/Subscriber. This Account Password is gathered online over a secure session, during data collection or Key Pair Generation, and is maintained encrypted to prevent unauthorized use by Individuals other than the Applicant/PKI Sponsor/Subscriber.

IdenTrust issues TrustID Certificates only to Individual Applicants or to Devices represented by the PKI Sponsors. Specifically, in the case of human Subscribers, IdenTrust does not issue Certificates that contain a Public Key whose associated Private Key is shared.

### **3.2.3.1 Acceptable Forms of Identification Documents**

All Individuals seeking the Issuance of a TrustID Certificate who apply in person or in an in-person Remote Identity Proofing event must present satisfactory proof of identity using documents which discernible show the Applicant's face.

1. The following are considered by the TrustID Policy to be acceptable "Government-issued photo IDs" in its original form for in-person and Remote Identity Proofing (all photo IDs must be currently-valid (e.g., unexpired) at the time of presentment by the Applicant for Identity Proofing)
  - A government-issued driver's license or non-driver's license identification card;
  - A passport;
  - A military ID;
  - An alien registration card or naturalization Certificate (with photograph);
  - A national health card (with photograph); and
  - Any other currently valid photo ID issued by a governmental agency.
2. The following are considered by the TrustID CP and this CPS to be other "Acceptable Forms of ID":
  - A current college photo identification card;
  - A currently-valid major credit card;
  - An employer identification card (with photograph);
  - A social security or national health card (without a photograph);
  - An original or certified copy of a birth Certificate;
  - An original or certified copy of a court order with name and date of birth;
  - A utility bill invoiced within the last 60 days that contains a matching name and address;
  - A monthly or quarterly statement from a financial institution (e.g., brokerage, mortgage, depository institution) issued within the last 60 days that contains a matching name and address;
  - An insurance Policy containing name and date of birth;
  - A voter registration card;
  - A concealed handgun license;
  - A pilot's license;
  - A marriage license;
  - A high school or college diploma;
  - A vehicle title;
  - A library card; and
  - Third party affidavits of identity based on personal acquaintance with the Applicant/PKI Sponsor.

### 3.2.3.2 In-Person Identification

Identity Proofing is a component of the overall Certificate application process and may be done either in-person or remotely. The process also includes submission of an online secure application, verification of the information provided in that application, and completion of a telephone number-address-name match. When in-person identity verification is performed, the Applicant/PKI Sponsor meets with an Individual authorized to collect the appropriate Physical Identity Documents in its original form to verify the Applicant's/PKI Sponsor's identity. See conditions for remote Identity Proofing provided later in this section.

In-person identification is performed by, and in the presence of:

- CA authorized representative (i.e., LRA),
- RA authorized representative (i.e., LRA),
- An authorized representative of an Individual's Sponsoring Organization (i.e., Trusted Agent),
- A licensed notary or
- Person or Entity certified by a governmental agency as being authorized to confirm identities (e.g., a driver license bureau, a county clerk, etc.).
- Enterprise RA

Credentials required are one Federal or National/State Government ID and an additional acceptable form of ID, one of which shall be a photo ID (e.g., driver license). All IDs used in the Identity Proofing process must be from the approved list in [Section 3.2.3.1](#) and valid at the time that the Identity Proofing event is conducted.

The process of documentation and authentication includes the following:

- Identity of the licensed notary, Trusted Agent or LRA performing the identification;
- A signed declaration by the licensed notary, Trusted Agent, or LRA that he or she verified the identity of the Applicant/Subscriber as required by this section;
- A unique identifying number from the ID of the licensed notary, Trusted Agent or LRA and from the ID of the Applicant;
- The date of the verification;
- A declaration of identity signed by the Applicant using a handwritten signature; performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

IdenTrust or the RA verifies all of the following identification information supplied by the Applicant: first name, middle initial, and last name, current address (number and street, city, zip code), and home or cellular telephone number.

If the evidence has an explicit validity period, IdenTrust or the RA verifies that the time of the identity validation is within this validity period. In context this can include the date of expiry of an identity document.

IdenTrust or the RA may reuse existing evidence to validate Individual identity subject to the age restrictions in [Section 4.2.1](#).

Information is recorded in a paper form and, when authentication is not performed by an LRA, paper forms are securely submitted to an LRA by the Applicant, the Trusted Agent, or the licensed notary. Packages secured in a tamper-evident manner by the certified entity (e.g. sealed in an overnight delivery package commonly used by domestic and international couriers) satisfy this requirement provided that the information is collected and delivered to the LRA in a manner that is adequately protected against fraud and forgery (e.g., colored ink or embossed seal on identity certification by notary or government agency and delivery to the LRA via official postal delivery (i.e., US Postal Service first class mail) or UPS, FedEx, DHL, Airborne Express, TNT, Emery, etc., in a sealed, tamper-evident envelope).

All information submitted by the Applicant for Identity Proofing identification must be reviewed and crosschecked to determine that it is (i) internally consistent, and (ii) consistent with the information contained in the application for the Certificate. Identity established in this manner shall be communicated to the CA by a signed communication (in writing or digitally) indicating that the Applicant was properly identified.

In addition to the paper submission explained above, the Applicant or Individual who performs the verification will submit part of the information over a secure website directly to IdenTrust or the RA. The complete paper forms need to be reviewed by the LRA before the final approval. The Individual performing verification can electronically submit one or multiple applications.

The telephone number-address-name match is performed using original documents that, by themselves or in combination, prove the connection between the Applicant's name, address, and home or cellular telephone number (e.g., original telephone bill, driver's license, utility bills, etc.).

When license notaries are unable to perform the telephone-address-name match, an LRA from IdenTrust or the RA performs it. The LRA uses original documentation (e.g., original telephone bill, utility bill), notarized copies (e.g., driver's license), or third party databases to perform the match.

All the requested information from the Identity Proofing event is recorded in a paper-form of the documents used for verification are collected and submitted by the LRA, or submitted to him or her, for final application verification, approval, and recording in the system. If supporting documentation is required for verification, a copy of documentation may accompany the original forms.

After an application has been approved using the automated, in-person, or Remote Identity Proofing processes, an out-of-band notification is sent to the previously verified physical mail address via US Postal Service first class mail.

### **3.2.3.2.1 Remote Identity Proofing**

According to NIST publication SP 800-63-3A there are 2 scenarios for conducting Remote Identity Proofing—Supervised Remote Identity Proofing and Unsupervised Remote Identity Proofing. The need to conduct Supervised Remote, Unsupervised Remote, or in-person Identity Proofing is determined by the Assurance level of the Certificate for which the Applicant has requested.

Human Certificates issued under the TrustID CP and CPS are classified by NIST as either Basic or Medium assurance Certificates.

Basic Assurance Certificates issued before September 1, 2023, are eligible for automated<sup>3</sup>, in-person, or Unsupervised Remote Identity Proofing.

Medium Assurance Certificates are eligible for in-person or Unsupervised Remote Identity Proofing

Where Remote Identity Proofing is permitted, the following practices must be followed:

The Remote Identity Proofing session must be conducted by an IdenTrust LRA or an Individual or group of Individuals who have been authorized by IdenTrust to conduct Remote Identity Proofing, such as a Trusted Agent.

1. The remote Identity Proofing session must be conducted using preauthorized technology, which must include high resolution video and audio-conferencing capabilities.
2. All agents who are authorized to conduct a Remote Identity Proofing session must have completed a formal training session that addresses at least the following topics:
3. Scheduling a Remote Identity Proofing session.

---

<sup>3</sup> Effective September 1, 2023, the process of electronic individual Identity verification has been discontinued

4. Conducting a Remote Identity Proofing session.
5. Validating required identity documents.
6. Spotting potentially fraudulent actions.
7. The agent conducting the remote session must monitor the entire Identity Proofing session, from which the Applicant or the agent must not depart at any time from the view of the camera.
8. The agent will require all actions taken by the Applicant during the Identity Proofing session to be clearly visible to the agent via the remote conferencing video feed.
9. If digital verification of any provided evidence is required, the agent must perform this verification via integrated scanners and sensors.
10. All remote sessions will be initiated by an IdenTrust LRA and will be prescheduled (not impromptu). Sessions initiated by an Applicant are prohibited.
11. The use of remote kiosks or publicly located workstations for the express purpose of conducting Remote Identity Proofing is prohibited under this CPS.

Once the remote identity session has been complete, the Applicant must submit, via email, scanned copies of identity credentials and all application forms completed during the session and/or required for application approval.

### **3.2.3.3 Attestation of Identity by an Employer or Other Person**

Identity may be established by an Attestation Letter signed (in writing or digitally) by an authorized representative (e.g., a supervisor, administrative officer, information security officer, authorizing official, Certificate coordinator, etc.) of the Applicant's employer that has been identified and authenticated in accordance with [Section 3.2.2.2](#), or by a person or entity certified by a government agency as being authorized to confirm identities, provided that the attestation is checked to ensure legitimacy.

For non-Enterprise Subscribers, IdenTrust or RA verify the authority or affiliation of an Individual to represent an Organization to be included in the subject:organizationName of the Certificate using an Attestation Letter provided by the Organization and verified in accordance with [Section 3.2.6.5](#).

In the case of Sponsor-Validated Certificates approved by an Enterprise RA, The RA will validate all identity attributes of an Individual to be included in the Certificate. The RA may rely upon existing internal records to validate Individual Identity.

The Enterprise RA will maintain records to satisfy the requirements of [Section 1.3.2.1](#)

#### **3.2.3.3.1 Disclosure of Verification Sources**

For Organization-Validated and Sponsor-Validated Certificates, IdenTrust verifies the unique organization identifier used in the Certificate from a register that is maintained or authorized by the relevant government agency.

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.

In the case of a LEI data reference, the CA or RA shall verify the associated data record with the [Global Legal Entity Identifier Foundation](#).

For validation of Organizations that apply for EV Server, EV Code Signing, Organization-Validated or Sponsor-Validated Certificates, 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:

<https://www.identrust.com/support/documents/TrustID>.

The “Organization Verification Sources” document is located in the “Product Datasheets” Section.

For S/MIME Certificates, IdenTrust documents and publishes the methods it uses to collect Individual identity attributes at this location: <https://www.identrust.com/support/documents/trustid> under General Questions: [TrustID | Identity Verification Requirements](#).

### **3.2.3.4 Electronic Identification**

When the authentication is performed through an automated/online<sup>4</sup> process, the Applicant submits the information directly to IdenTrust or the RA over a secure session online. Automated authentications are not based on human interaction but are based on the high correlation of an identity-proofing algorithm, and they are completed automatically. No paper forms are necessary in this case.

To meet the requirements for completing the identity-proofing algorithm an Applicant must provide at least one of these forms of “antecedent in-person based information” identification:

1. Currently valid credit card number;
2. Alien Registration number;
3. Passport number; and
4. Currently a valid state-issued driver’s license number or state-issued identification card number.

In addition to the requirements above, the Applicant must also provide 2 or more “non-antecedent pieces of information” as listed below:

1. Social Security number;
2. Date of birth;
3. Place of birth;
4. Current employer name, address (number and street, city, zip code), and telephone number.

IdenTrust and the RAs have designed identity-proofing algorithms that use the Applicant’s data and correlate them with information collected from independent data sources for consistency. If a high correlation is found, the application is approved, and no additional human intervention is needed. If no or lower correlation is found instead, an application is placed on an exception process and additional information is requested from the Applicant (e.g., telephone or utility bill, notarized documentation, etc.). An LRA reviews the additional documentation and approves or disapproves the application.

The information used for the verification algorithm may change from time to time to take advantage of technology and data quality enhancements.

### **3.2.3.5 Know Your Customer Identity Proofing**

Know Your Customer (KYC) Identity Proofing is a standard process that may be used by financial institutions to establish the identity of an Applicant. KYC processes may be used as an alternative method to standard Identity Proofing processes as stated in this CPS, providing that the following requirements are met:

If (i) the RA has previously established the identity of an Individual, and (ii) the RA and the Individual have an ongoing, trusted business relationship (e.g., commercial, banking, or employment) sufficient to satisfy the RA of the Individual’s identity, then the RA may rely on such prior identification and ongoing relationship to satisfy the Identity Proofing requirements of this Policy and to process the request for a TrustID Certificate. In addition, the RA may perform the out-of-band confirmation with respect to such Individual by (i) in-person delivery, based on the RA’s personal knowledge of the Individual (e.g., in an employment relationship) or reasonable identification

---

<sup>4</sup> Effective September 1, 2023, the process of electronic individual Identity verification has been discontinued.

at the time of delivery, or (ii) use of a Shared Secret between the RA and the Individual, previously established in connection with the prior identification and ongoing relationship described above.

The RA will ensure that it has collected or reviewed and kept records of the type and details of information regarding the Individual's identity that meets the minimum requirements of its "Know Your Customer" Policy, or other similar procedures, which may include verification of all of the following identification information supplied by the Applicant: (i) first name, middle initial, and last name; (ii) street address; and (iii) home or work telephone number.

The RA should determine whether it has a record of the Applicant's persistent street address and verification of a telephone number by calling the Applicant's residence or place of employment. Disconnected phone service, no record of employment, or other insufficient, false, or suspicious information provided by the Individual warrant further investigation. If requested follow-up information is not forthcoming, or if an Applicant refuses to produce any requested information, the Certificate application should not be approved.

Such Know Your Customer procedures shall not conflict with other stipulations of this Policy.

### **3.2.3.6 Code Signing and Time-Stamping Certificates**

A TrustID Non-EV Code Signing or EV Code Signing Certificate or TrustID Time-Stamping Certificate identifies an Organization as the Subject of a Certificate, and such Organization is attributable for the purposes of accountability and responsibility for signatures created by the Organization to be used to verify the integrity of its code. When issuing either TrustID Non-EV Code Signing or EV Code Signing Certificate or TrustID Time-Stamping Certificate, IdenTrust as Issuing CA conforms with the provisions of the current version of the [CS BR](#). In the event of any conflict between the provisions of this CPS and the provisions of the above referenced document, then the provisions of the above referenced document, as applicable, shall govern. A TrustID Non-EV Code Signing or EV Code Signing Certificate or TrustID Time-Stamping Certificate identifying an Organization as the Subject of the Certificate can only be issued by an Issuing CA that can ensure accomplishment of the Identity Proofing required by this section.

### **3.2.3.7 Secure Email Certificate**

For Secure Email Certificates, at the time of Email Address verification during authentication before Issuance of the Certificate, the Applicant must demonstrate to the RA the Applicant's control of the Email Address the Applicant provided for inclusion in the Certificate during the registration process.

For Certificates supporting the S/MIME protocol, Email Address validation is always handled by IdenTrust as Issuing CA using the validation methods described in [Section 3.2.6.3](#).

### **3.2.3.8 TrustID CIV Card Authentication Certificate**

For TrustID CIV Card Authentication Certificate either an RA or a CA will assign a unique name-identifier to the relevant Cryptographic Module and such unique name-identifier is at a minimum to be contained in the Subject Name of the TrustID CIV Card Authentication Certificate issued to the Cryptographic Module.

### **3.2.3.9 TrustID CIV Device Certificate**

For a TrustID CIV Device Certificate, the RA or Applicant authenticates an Electronic Device and assigns it a unique name-identifier. Such unique name-identifier is to be contained in the Subject Name of the TrustID CIV Device Certificate issued to the Electronic Device containing the Cryptographic Module storing the corresponding Key Pair.

### 3.2.3.10 Authorized Relying Parties

IdenTrust may perform Identity Proofing of Authorized Relying Parties, including but not limited to performing such Identity Proofing as part of any enrollment process by which an Authorized Relying Party enters into an Authorized Relying Party Agreement with IdenTrust.

### 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 specified in the TrustID Certificate Profile, 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.

For server Certificates, during the Domain Name validation procedure for any method described in [Section 3.2.2.4](#), the Domain Contact will be asked if they would like to provide a list of Individuals authorized to apply for a Certificate for that Domain Name and/or any additional FQDNs verified under their control. Individuals that apply for FQDNs provided by the Domain Contact that are not named on such a list will not be authorized to request a Certificate for that Domain Name. The Domain Contact will be eligible to update this list based on any business needs upon contacting or being contacted and verified by the LRA.

For S/MIME and Code Signing Certificates, IdenTrust uses a Reliable Method of Communication to verify the authority and approval of an Applicant Representative to perform one or more of the following:

- To act as an Enterprise RA;
- To request issuance or revocation of Certificates; or
- To assign responsibilities to others to act in these roles.

IdenTrust may use the sources listed in [Section 3.2.2.1](#)

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.

### 3.2.6 Criteria for Interoperation

To ensure PKI interoperability, IdenTrust:

- Operates a PKI that has undergone a successful compliance audit pursuant to [Section 8](#);
- Issue Certificates compliant with the profiles described in [Section 7](#), and make Certificate status information available in compliance with this CPS; and
- Provide CA Certificate and Certificate status information to the Authorized Relying Parties.
- 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<sup>5</sup> described in [Section 3.2](#): Initial Identity Validation may consist of either (i) 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; (ii) information provided through third party vendors of such information; or (iii) 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 (i) delivery of a Shared Secret to a confirmed and trusted data point (e.g., street address, telephone number, or Email Address), (ii) 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](#), (iii) 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, (iv) 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 (v) another equivalent process.

Any documents received for the manual verification process will be inspected by the LRA 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 S/MIME 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](#) or [S/MIME 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

---

<sup>5</sup> Effective September 1, 2023, the process of electronic individual Identity verification has been discontinued.

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 must be entered within 24 hours of issuance. 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. The [TLS BR](#) validation methods are not used for Email Address validation.

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.

#### **3.2.6.4 Verification of the Certificate Request**

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

If an LRA determines a verification of an Applicant for a TrustID Personal Certificate should be completed, he or she will be contacted via a Reliable Method of Communication, such the phone number provided during the application process and ask for verification of the request from the Applicant. The Applicant may be contacted

To verify the authenticity of a FATCA Organization Certificate request, the LRA must follow the guidance in [Section 3.2.6.3](#) and may also confirm the Base Domain Name of the Applicant's Email Address using one of the validation methods listed in [Section 3.2.2.4](#).

If a server 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.

Additional checks and verification will be made for EV Server Certificate applications based on [Section 3.2.2.1.1 of the EV TLS B.R.](#)

Likewise, checks and verifications will be made for Code Signing Certificate applications based on the requirements within the [CS BR](#).

### 3.2.6.5 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. Enterprise RA records are a Reliable Data Source for Individual Subject attributes included in Sponsor-Validated Certificates issued to the Enterprise RA's Organization.

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.

#### 3.2.6.5.1 Verification and Validation of Personal and Business Certificate Information Sources

Registration information provided by the Applicant must include at least his or her name, address, telephone number, Email Address, and the serial numbers from 2 acceptable forms of ID, one of which shall be a Government-issued photo ID as described and required in [Section 3.2.3](#), [Section 3.2.3.1](#), [Section 3.2.3.2](#) dependent on the type of application and Certificate that is requested as listed in [Section 3.2](#).

#### 3.2.6.5.2 Verification and Validation of Server Certificate Information Sources

In addition to the verification of information, by comparison to trusted information as described above, for server Certificates 2 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 4.2.2.3](#); 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 server Certificate requests will be verified against this list.
- Additional checks are performed for EV Server Certificates based on [Section 3.2.2.11 of the EV TLS BR](#).
- Additional checks are performed for EV Code Signing Certificates based on [Section 3.2.2.10 of the CS BR](#).

Should a third party vendor be utilized to confirm the information provided manually or electronically for server Certificates, 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.

### 3.2.6.5.3 Verification and Validation of FATCA Organization Certificate Sources

Registration information provided by the PKI Sponsor must include information about herself/himself, the Sponsoring Organization, and an email. This information is validated in accordance with [Section 3.2](#). Other information is optional and may include:

- The Global Intermediary Identification Number (GIIN) provided by the Internal Revenue Service of the United States of America (“IRS”) to Organizations registered within the FATCA program, and
- A Domain Name.

For verification of the GIIN, IdenTrust will use records provided by the IRS through the FATCA Foreign Financial Institution (FFI) List Search and Download Tool. With respect to verification of the GIIN, IdenTrust may use the information available through the tool only to resolve exceptions during an application. The absence from the list will not result in a declined Certificate application automatically. When a GIIN provided does not correspond to the Sponsoring Organization in the application and is used as part of an exception verification process, such application will be declined.

Verification of a Domain Name will follow the procedures outlined in [Section 3.2.2.4](#).

## 3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

### 3.3.1 Identification and Authentication for Routine Re-key

For human Subscribers, as long as an End Entity’s TrustID Certificate has not expired, been revoked, or suspended, the Subscriber can request Issuance of a new TrustID Certificate with a new Key Pair within 3 months before the end of the TrustID Certificate's Validity Period and the RA or IdenTrust will rely on the information on file that was initially verified. If any information has changed in the Certificate (e.g., last name, Sponsoring Organization, any additional FQDNs listed under the SAN extension, etc.) the identity must be re-established through the initial identity-proofing process specified for the required Certificate in [Section 3.2](#). PKI Sponsors may also opt to remove or edit FQDNs during re-key.

For End Entity server 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](#).

#### 3.3.1.1 Certificate Renewal

Certificate renewals are currently available for CSAs. Subscribers, External CAs, and Issuing CAs cannot renew their Certificates and therefore will not be asked to go through the Identity Proofing processes listed in [Section 3.2](#) to renew their respective Certificate(s). For further information on the process, see [Section 4.6](#).

#### 3.3.1.2 Certificate Update

For all update requests, identity must be re-established through the initial identity-proofing process specified in [Section 3.2](#) for the corresponding Certificate type. For further information on the process, see [Section 4.8](#).

### 3.3.2 Identification and Authentication for Re-Key after Revocation

Suspended, 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 or suspension request in any other manner is authenticated in accordance with [Section 4.9](#). Revocation or suspension requests authenticated on the basis of the TrustID Certificate's associated Key Pair is always accepted as valid. Other Revocation or suspension request authentication mechanisms may be used as well, including a request in writing signed by the Subscriber, and sent via U.S. Postal Service first class mail, or UPS, FedEx, DHL, Airborne Express, TNT, Emery, etc., in a sealed, tamper-evident envelope. These authentication mechanisms balance the need to prevent unauthorized Revocation or suspension requests against the need to quickly revoke or suspend Certificates. These mechanisms are explained in [Section 4.9](#).

## 4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

### 4.1 CERTIFICATE APPLICATION

This CPS identifies the required information and procedures that constitute assurance and support trust in the IdenTrust PKI. To this end, the Policy endorses the following procedures for satisfying the security requirements of the IdenTrust PKI. The following steps are required when applying for a TrustID Certificate: (i) submission of a Certificate Request; (ii) sign a Subscriber Agreement and/or Terms of Use; (iii) establish the identity of Subject (per [Section 3](#)); (iv) obtain a Key Pair for each TrustID Certificate required; (v) prove to the IdenTrust CA that the Public Key forms a functioning Key Pair with the Private Key held by the End Entity; and (vi) provide a point of contact for verification of any roles or authorizations requested.

The Certificate Request and Subscriber Agreement prescribed by IdenTrust complies with [Section 9.6.3 of the TLS BR](#). When appropriate, IdenTrust obtains any additional documentation it determines necessary to fulfill these Requirements.

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.

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.

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.

#### 4.1.1 Who Can Submit a Certificate Application

IdenTrust maintains access to all previously revoked Certificates and Certificate applications whether approved or rejected, based on the record archival procedure described in [Section 5.5.2](#); IdenTrust uses this information to identify subsequent suspicious Certificate requests.

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

##### 4.1.1.1 Personal Certificates

- An Individual who agrees to the terms of the Subscriber Agreement.
- An Individual who is already a Subscriber of this type of Certificate.

##### 4.1.1.2 Business Certificates, Organization Certificates

- An Individual who is affiliated with a Sponsoring Organization, through employment, contractual, or agency relationship, agrees to the terms of the Subscriber Agreement.
- An Individual who is already a Subscriber of this type of Certificate.
- The Sponsoring Organization through an authorized representative (e.g., Trusted Agent).

##### 4.1.1.3 Server, Code Signing and Electronic Device Certificates

- 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.

- Additional checks and requirements for the Applicant for EV Server Certificates Subjects are made in accordance with [Section 4.1.1 of the EV TLS BR](#).
- Likewise, checks and verifications will be made for EV Code Signing Certificate applications based on the requirements within the [CS BR Section 4.1.1](#).

#### 4.1.1.4 FATCA Organization Certificates

- An Individual, acting in the role of PKI Sponsor, who is affiliated with a Sponsoring Organization, through employment, contractual, or agency relationship, and agrees to the terms of the Subscriber Agreement.
- The Sponsoring Organization through an authorized representative (e.g., Trusted Agent).

#### 4.1.1.5 RA Systems Certificates

1. An employee of the RA who has been appointed as an RA Administrator by one of the Organization's Authorizing Officials identified in the Registration Authority Agreement or a Certificate of incumbency.

### 4.1.2 Enrollment Process and Responsibilities

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

1. A Certificate Request; and
2. An executed Subscriber Agreement and/or Terms of Use.

The Certificate Request and Subscriber Agreement or Terms of Use comply with [Section 9.6.3 of the CA/B Forum TLS BR](#). When applicable, IdenTrust obtain any additional documentation necessary to fulfill the Certificate Request.

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.

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.

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 designed enrollment processes that facilitate the submission of registration information from the Applicant/PKI Sponsor to IdenTrust. Options include but are not limited to: Direct submission over a TrustID dedicated website; Trusted-Agent-mediated submission in bulk, Enterprise RA-mediated submission in bulk to IdenTrust, and submission through an RA that is securely forwarded to IdenTrust.

#### 4.1.2.1 Information Collection

All Certificate requests contain a request from, or on behalf of, the Applicant or PKI Sponsor for the Issuance of a Certificate. Additionally, a certification is required by, or on behalf of, the Applicant that all of the information contained within the Certificate request is correct.



An RA may enter into an agreement with IdenTrust to host its registration process and interface with IdenTrust's Certificate manufacturing architecture via IdenTrust's secure registration messaging protocol for the creation, delivery, and management of Certificates. The RA will be contractually bound to adhere to the applicable provisions of the TrustID CP and this CPS and to provide registration services in strict accordance with the practices set forth in [Section 3](#) and [Section 4](#).

During the application phase of registration, Applicant/PKI Sponsor information is collected in one of the following ways:

- Individual Applicants or PKI Sponsors can provide registration information via an online Certificate application process over a server-authenticated SSL/TLS secured website hosted by IdenTrust or the RA;
- Individual Applicants or PKI Sponsors can provide registration information to a Trusted Agent, who will forward the information to IdenTrust or the RA via the bulk loading process described in [Section 4.1.2.1.1](#); or
- PKI Sponsors can provide registration information to an Enterprise RA, who will collect the appropriate information necessary for a server Certificate and enter the information into an IdenTrust provided administrative interface to approve the application on behalf of IdenTrust.

#### **4.1.2.1.1 Information Collection via Bulk Loading**

A Sponsoring Organization may enter into an agreement with IdenTrust or an RA to process affiliated Certificates in bulk (e.g., Business, etc.). This process is different when performed by Trusted Agents or by Enterprise RAs.

##### **4.1.2.1.1.1 Bulk-Loading by Trusted Agents**

The Sponsoring Organization in conjunction with IdenTrust or the RA appoints Trusted Agent(s) to assist with the processing of requests for the Issuance of Certificates. Trusted Agents undergo Identity Proofing in accordance with [Section 3.2.2](#), [Section 3.2.3](#), and [Section 3.2.3.1](#). Trusted Agents must enter into an agreement and have or obtain a TrustID Certificate to perform and communicate Subscriber Identity Proofing in accordance with the processes described in this CPS. The Trusted Agent performs in-person or Remote Identity Proofing of Applicants/PKI Sponsors and collects the information required by [Section 3.2.2](#) and [Section 3.2.3](#). The Trusted Agent gathers Certificate application information, including name, address, phone number, Email Address, and Organization name into a bulk Certificate Issuance request, which is Digitally Signed by the Trusted Agent and securely delivered to the RAs or IdenTrust for processing.

Printed records, signed declarations, and other pertinent records are maintained by the RA or IdenTrust. The Trusted Agent collects, seals, and delivers the records and declarations to IdenTrust or the RA for safekeeping. Authentication by a Trusted Agent does not relieve IdenTrust or its RAs of responsibility to verify identifying information by checking official records.

##### **4.1.2.1.1.2 Bulk Loading by Enterprise RAs**

The Sponsoring Organization in conjunction with IdenTrust appoints Enterprise RAs to assist with the processing of requests for the Issuance of server Certificates. An Enterprise RA, who is current with requirements of the agreement and Identity Proofing in this Policy gathers and enters the Certificate application information including each PKI Sponsor's name, job title, phone number, Email Address, and requested FQDN(s) name into a bulk Certificate Issuance request and securely approved in the administrative interface on behalf of IdenTrust.

The Enterprise RA collects and maintains the records in the RA administrative interface provided by IdenTrust. The Enterprise RA and the Sponsoring Organization that has elected that Enterprise RA are contractually responsible for the materials and information submitted to the administrative interface for approval.



## 4.1.2.2 Data Collected during Enrollment Process

All Applicants and PKI Sponsors must provide the following based on Certificate type:

### 4.1.2.2.1 Data Collection by Certificate Type

#### 4.1.2.2.1.1 Personal Certificates

- Applicant name;
- Applicant's Email Address;
- Applicant's phone number;
- An Account Password;
- Payment information such as credit card details, purchase order number, or voucher number;
- Photo ID number and type as required by [Section 3.2.3.1](#); and
- Point of contact for confirmation of information provided.

#### 4.1.2.2.1.2 Business Certificates, Business/Organization Certificates

- Applicant's name;
- Applicant's job title;
- Sponsoring Organization information, including name, entity type (for-profit corporation, non-profit, government, partnership, LLC, sole proprietorship, etc.), address (including country), and the name of the jurisdiction under whose law the entity has been organized (i.e., state of incorporation e.g., Delaware);
- Applicant's Email Address;
- Applicant's phone number;
- An Account Password; and
- Payment information such as credit card details, purchase order number, or voucher number.

#### 4.1.2.2.1.3 SSL/TLS Electronic Device Certificates

- PKI Sponsor's name;
- PKI Sponsor's Email Address;
- PKI Sponsor's phone number;
- PKI Sponsor's job title;
- Sponsoring Organization information, including name, entity type (for-profit corporation, non-profit, government, partnership, LLC, sole proprietorship, etc.), address (including country), and the name of the jurisdiction under whose law the entity has been organized (i.e., state of incorporation e.g., Delaware);
- Registered server name;
- Domain Name(s);
- RSA PKCS#10 Certificate signing request (CSR);
- Additional requirements as specified in [Section 4.1.1 of the EV TLS BR](#).

#### 4.1.2.2.1.4 FATCA Organization Certificate

- PKI Sponsor's name;
- PKI Sponsor's job title;
- Sponsoring Organization information, including name, entity type (for-profit corporation, non-profit, government, partnership, LLC, sole proprietorship, etc.), address (including country), and the name of the jurisdiction under whose law the entity has been organized (i.e., state of incorporation e.g., Delaware);

- Organization’s Email Address;
- Organization’s phone number;
- IRS Global Intermediary Identification Number (GIIN) (if available);
- Organization’s Domain Name (if available);
- An Account Password; and
- Payment information such as credit card details, purchase order number, or voucher number.

#### **4.1.2.2.1.5 RA Systems Certificates**

- Applicant’s name;
- Applicant’s Email Address;
- Applicant’s job title;
- Applicant’s phone number;
- An Account Password;
- Payment information such as credit card details, purchase order number, or voucher number; and
- Name of AO.

#### **4.1.2.2.2 Account Password**

An Account Password selected by the Applicant/PKI Sponsor and consisting of at least eight (8) characters, which will be utilized for user authentication along with Activation Data provided in an out-of-band method (for use during Certificate retrieval). As part of the online application process only, the Applicant/PKI Sponsor is required to create three questions and secret answers, which together serve as a mechanism to reset their Account Password in case they forget it before they can download their Certificate. This process is activated by the Subscriber providing his or her Activation Code, and by clicking on an Account Password reset uniform resource locator (URL). This process sends a one-time-code and specified URL to the Email Address on file for the Subscriber. After receiving the email, the Subscriber must enter both the Activation Code and the one-time code at the specified URL to gain access to the three questions that were selected during registration. The three questions were selected by the Applicant/PKI Sponsor from a list of ten randomly selected questions that were randomly generated from a pool of password-reset questions. If the answers are correct, the Subscriber is allowed to change the Account Password, which is immediately hashed and stored in the CA system for further use.

#### **4.1.2.2.3 Applicant/PKI Sponsor Education and Disclosure**

At the time of application for an IdenTrust-issued TrustID Certificate, Applicants/PKI Sponsors are advised of the advantages and potential risks associated with using TrustID Certificates and Subscribers are provided with information regarding the use of Private Keys and Digital Signatures or encrypted messages created with such Keys, and other Subscribers’ obligations described in [Section 9.4](#). IdenTrust and RAs use two main mechanisms to educate and disclose the information: The IdenTrust website, which enables access to the TrustID CP and this CPS; and the Subscriber Agreement that is provided during the enrollment process.

#### **4.1.2.2.4 Establishment of Identity**

For Certificates that do not require submission of registration forms, identity is deemed to have been established on the day the RA System successfully completes automated identity verification, or if an in-person or Remote Identity Proofing process was utilized, the date the Identity Proofing information is received and entered into the system by the LRA.

For Certificates where submission of forms is required, identity is deemed to have been established only after the Identity Proofing documentation is reviewed by the LRA, approved by the LRA, and entered by the LRA into

the RA System. The date of identity establishment is deemed the date the Identity Proofing paperwork is entered into the RA System as approved by the LRA.

Upon completion of the registration process, all identity-related data for the Applicant and establishment thereof has been recorded in the RA System database.

The following sections discuss in more detail the collection and verification of identity data, and Certificate Issuance processes.

## **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 the CP and this CPS.

Information in the Certificate application is verified as accurate before Certificates are issued as specified in [Section 3.2](#).

IdenTrust and RAs include checking of CAA records to process validation of FQDNs in server Certificate applications. As part of the Issuance process, the IdenTrust CA check for CAA records and follow the processing instruction found on property tags for each dNSName in the subjectAltName extension of the Certificate to be issued, as specified in the [RFC 8659](#). Issuwild property tags are ignored unless the request is for a wildcard Certificate. See [Section 3.2.2.3.4](#).

To prevent resource exhaustion attacks, IdenTrust limits the length of CNAME chains that are accepted and processes CNAME chains that contain 8 or fewer CNAME records.

Action taken on CAA records are logged and when issued, it is done following the instructions in [Section 4.2.3](#).

### **4.2.1 Performing Identification and Authentication Functions**

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](#).

For server Certificates, 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

[For EV Server Certificates, IdenTrust follows the identification and authentication functions as described in Section 4.2.1 of the EV TLS BR.](#)

For server Certificates, 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 397 days before issuing the Certificate. For EV Server and EV Code Signing Certificates, the age of all data used to support renewals shall not exceed more than thirteen months as specified in [Section 3.2.2.14.3 of the EV TLS BR](#).

For S/MIME Certificates, Applicant information shall include, but not be limited to, at least one Email Address to be included in the Certificate's subjectAltName extension.

IdenTrust may reuse completed validations and/or supporting evidence performed in accordance with [Section 3.2](#) within the following limits:

1. **Validation of Email Address Authorization or Control:** Completed validation of the control of a mail server in accordance with [Section 3.2.6.3](#) shall be obtained no more than 397 days prior to issuing the Certificate.

In the event of changes to the [TLS BR](#) methods specified in [Section 3.2.2.1](#), a CA may continue to reuse completed validations and/or supporting evidence for the period stated in this section.

Completed validation of control of an Email Address in accordance with [Section 3.2.6.3](#) shall be obtained no more than 30 days prior to issuing the Certificate.

2. **Authentication of Organization Identity:** Completed validation of organization identity in accordance with [Section 3.2.2](#) shall be obtained no more than 825 days prior to issuing the Certificate.

Validation of authority in accordance with [Section 3.2.5](#) shall be obtained no more than 825 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.

3. **Authentication of Individual Identity:** Completed validation of Individual identity in accordance with [Section 3.2.3](#) shall be obtained no more than 825 days prior to issuing the Certificate.

A prior validation shall not be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.

#### 4.2.2 Approval or Rejection of Certificate Applications

For non-server Certificates and Code Signing Certificate applications, IdenTrust and RAs appoint Individuals within the Organization who act in the role of an LRA and are responsible to approve Certificate applications.

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.

An RA or IdenTrust terminates an Applicant/PKI Sponsor registration process if:

- The Applicant/PKI Sponsor's identity or Organization affiliation cannot be established in accordance with Identity Proofing requirements;
- Not all forms necessary to establish Identity Proofing are submitted on a timely basis;
- For server and S/MIME Certificates:
  - , the PKI Sponsor is unable to establish or provide verifiable evidence to IdenTrust or the RA that they are authorized to request the Certificate for the FQDN from the Domain Administrator or a CAA record is found but "identrust.com" or "www.identrust.com" are not listed as one of the trusted CA Domain Names; and/or
  - The RA or IdenTrust is unable to verify or process the Applicant/PKI Sponsor's payment information (where payment information is required).

Upon application rejection, the RA or IdenTrust provides information to the Certificate Applicant/PKI Sponsor:

- Indicating a failure of the Identity Proofing process; and
- Informing the Applicant/PKI Sponsor of the process necessary to resume the processing of the application.

Upon application rejection, the RA or IdenTrust records applicable transaction data including the following:

- 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;

- Name of the document presented for Identity Proofing including the name of its issuing authority, the date of Issuance, and the date of expiration (not required for server Certificates);
- All fields verified;
- Source of verification (i.e., which databases used for cross-checks);
- Method of verification (e.g., online, in-person, remote);
- Date/time of verification;
- Names of entities providing identification services, including contractors, subcontractors, if any;
- Fields that failed verification;
- Status of current registration process (suspended or ended);
- All Identity Proofing data;
- All associated error messages and codes; and
- Date/time of process completion.

#### 4.2.2.1 Server Certificates

IdenTrust does not issue server Certificates containing Internal Names or Reserved IP Address.

For server Certificate requests in addition to the majority of the list above (noted when not applicable), the rejection transaction record will include:

- The FQDN(s) requested;
- Whether or not “identrust.com” or “[www.identrust.com](http://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](http://www.identrust.com)” were listed as one the trusted CA Domain Names in the CAA record; and
- Date/time of process completion.

#### 4.2.2.2 Verification against High Risk and Denied Request Lists

To ensure that requests for TrustID server, EV Server Certificates and Code Signing 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.

- Additional requirements as specified in [Section 4.2.1 of the TLS BR](#);
- Additional requirements as specified in [Section 3.2.2.12 of the EV TLS BR](#); and
- Additional requirements for Applicants as outlined in [Section 3.2.8 of the CS BR](#).

#### **4.2.2.3 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 server 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.google.com](http://www.google.com), [www.identrust.com](http://www.identrust.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.

#### **4.2.2.4 Denied Request Procedure**

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

#### **4.2.3 Time to Process Certificate Applications**

There is no stipulation for the period between the receipt of an application for a human sponsored Certificate and its Issuance. However, the Issuing CA should respond promptly to all such applications.

For server and S/MIME 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.

#### **4.2.4 Final Cross-Correlation and Due Diligence**

Enterprise RAs may perform the cross-correlation and due diligence for EV Server Certificates following the requirements of [Section 3.2.2.13 of the EV TLS BR](#).

For Code Signing certificates, the CA LRA, the cross-correlation and due diligence is done following the requirements of [Section 3.2.9 of the CS BR](#).

### **4.3 CERTIFICATE ISSUANCE**

The Certificate Issuance process described in this section ensures that this CPS complies with the TrustID CP, including the following requirements:

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 requires at least 2 Individuals with Trusted Roles, one of whom deliberately issues a direct command in order for the Root CA to perform a Certificate signing operation.
6. IdenTrust has published the Subscriber's Certificates to IdenTrust's Repository.

#### **4.3.1 CA Actions During Certificate Issuance**

CA and RA actions are included in this section.

Issuance of a TrustID Certificate occurs once an application for that Certificate has:

1. Been approved by an LRA or Enterprise RA;
2. Activation materials have been delivered in one of the following methods:
  - a. IdenTrust or the RA delivers the unique Activation Code generated by IdenTrust or the RA to the Subscriber in a letter with a retrieval kit or over a verified channel such as email (out-of-band) or telephone call (out-of-band), including instructions for retrieval;
  - b. The RA receives the requested Certificate(s) via a secure channel between the RA and IdenTrust and inserts such Certificate(s) into an approved hardware device and provides to the Subscriber; or
  - c. The Enterprise RA delivers the unique Activation Code over a verified channel such as email (in-band), telephone call (out-of-band), or mail (out-of-band).
3. The Subscriber initiates a web-based retrieval process or accepts the hardware device that has been provided by the RA.
4. The operation of the systems handling Certificate issuance process is managed by 2 Individuals with trusted roles.

##### **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 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 by RFC 6962, Section 3.2.

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 non-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 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.
3. Upon authentication of the Applicant/Subscriber to the Retrieval URI and verification of 'approved' status of the Applicant/Subscriber's Certificate application, the system initiates Key Generation for Signing Keys (invoked locally on the Applicant/Subscriber's machine using either an ActiveX control and MS, or a browser add-on, or equivalent). The resulting public Signing Key is encapsulated in a Certificate request in the form prescribed by RSA PKCS#10.
4. The PKCS#10 Certificate request for the Signing Certificate is submitted to the IdenTrust CA for Certificate generation. The information in the Subscriber database previously verified during the Identity Proofing process, as approved by the LRA for Certificate Issuance, overrides the Subject DN information submitted in the PKCS#10. However, the binding between the Public Key within the PKCS#10 Certificate request and the Private Key is maintained—the signature on the PKCS#10 Certificate request is verified by the CA to ensure that it was signed with the corresponding Private Key before building the Certificate.
5. Encryption Key Pair and Encryption Certificate generation occur using the same verified information contained in the Subscriber database. The Encryption Key and Certificate are generated by the CA system and they are downloaded to the Cryptographic Module using an RSA PKCS#12 format protected by a strong password. This process happens in the background, and it is transparent to the Applicant/Subscriber using the same retrieval option mentioned in step 3 above.
6. IdenTrust delivers the Applicant/Subscriber's Certificates to the Certificate store (in either a browser or a hardware Cryptographic Module) using a format adhering to RSA PKCS #7 for the Signing Certificate and PKCS #12 for the Encryption Key Pair and Certificate.
7. In addition, IdenTrust delivers the Root CA Certificate and the TrustID Certificate in RSA PKCS #7 format with instructions to download them into the Subscriber's Certificate store. On supported platforms, the installation of both the Root and Certificates is automated via a web interface.
8. Installation of the Subscriber's Signing Certificate and Root CA Certificate is confirmed by initiating a client-authenticated SSL/TLS session between the IdenTrust or RA Retrieval URL, and the Subscriber's client platform. The Subscriber is instructed to select his or her Signing Certificate for authentication. The



process of mutual authentication ensures that the Certificate has been installed successfully and that cryptographic integrity exists between the Subscriber's Signing, the Intermediate, and the Root CA Certificates.

9. Upon successful installation of the Subscriber's Certificates, both Signing and Encryption Certificates will be published in IdenTrust's Repository.

#### **4.3.1.5 Issuance Via Secure Website**

For the Issuance of a Certificate for servers, the PKI Sponsor needs to follow only steps 1 and 2 above. (Note that 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 that this CPS complies with the TrustID CP.

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 the requirements of the TrustID CP;
2. IdenTrust has complied with all requirements in the TrustID CP 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 the TrustID CP.

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 4.9.1.1.2](#).

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.

#### **4.3.1.6 Issuance via Secure Interface between the RA and CA**

An alternate acceptable process is managed by the CMS and the EWS directly as described below. The process of Key and Certificate generation; the biometric data collection (if required), signature, and insertion in the smart card are performed by the LRA in the presence of the Applicant.

This method is available only applicable to RAs who are using an EWS for credential Issuance on a smart card hardware device. After the Issuance of a Certificate has been approved by the LRA, a TA or a different LRA provides the smart card to the Applicant which contains the requested Certificates and signed biometric data as part of an assisted card personalization.

1. In this scenario, the smart card is sent to the RA in advance. At the time of smart card personalization, the EWS interacts with and authenticates the smart card through the use of a factory-set key used for initial card communication. The factory-set Key is replaced with a diversified Key by the CMS as part of the personalization process.
2. In the event cards are loaded and personalized using a batch process, each card is locked until the applicable Applicant is available for card activation. The LRA identifies the Applicant by confirming identity credentials. Upon successful activation, the card PIN is changed by the Applicant and the card is activated.
3. After the LRA approves Certificate Issuance, the Applicant appears in-person before the TA or LRA different than the Certificate approving LRA, who authenticates the Applicant based on previously collected personal data.
4. The smart card is placed in the personalization station where the facial image is printed on it. Subsequently, the station connects to the CMS and all the Certificates and signed biometrics (if collected) are securely inserted into the smart card.
5. The TA or LRA, different than the Certificate approving LRA instructs the Applicant to change the PIN in the smart card and through the personalization workstation authorizes the CMS to set to an Applicant-selected PIN and activate the smart card.
6. The Subscriber formally acknowledges receipt of the smart card with all Certificates and signs the Subscriber Agreement that contains a declaration of identity.

#### **4.3.2 Notification to Subscriber by the CA of Issuance of Certificate**

Upon successful completion of the Subscriber Identity Proofing process explained in [Section 3.2.3](#), and before Certificate Issuance explained in [Section 4.4](#); IdenTrust, Enterprise RA, or the RA notifies the Applicant/PKI Sponsor about the approval of the Certificate. Notification letters are sent to the Applicant/PKI Sponsor's verified physical address containing enough information to guide the Applicant/PKI Sponsor through the Issuance process. Information may include a Uniform Resource Locator (URL), an Activation Code (i.e., a mutually shared secret), and basic instructions. Alternatively, the Activation Code may be delivered to a verified phone number or verified Email Address that is associated with the Applicant/PKI Sponsor while the retrieval URL may be delivered out-of-band via email. Within the context of a Sponsoring Organization with elected Enterprise RAs for server Certificates, the Activation Code may be sent through an in-band process to the verified Email Address of the approved PKI Sponsor and Subscriber.

If Certificates are delivered to the Subscriber during an in-person session, notification is not required.

## **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 Section 4.4 of the TrustID CP and this CPS 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 2.2.1](#), 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**

Through a combination of online processes, including registration and retrieval; and printed or online forms, including the Subscriber Agreement, each Applicant/PKI Sponsor for a TrustID Certificate:

- Provides complete and accurate responses to all requests for information made by IdenTrust (or a Trusted Agent or RA) during the Applicant/PKI Sponsor registration, Certificate application, and Identity Proofing processes;
- Generates a Key Pair using a reasonably trustworthy system, and take reasonable precautions to prevent any compromise, modification, loss, disclosure, or unauthorized use of the Private Key;
- Upon Issuance of a TrustID Certificate naming the Applicant/PKI Sponsor as the Subscriber, reviews the TrustID Certificate to ensure that all Subscriber information included in it is accurate, and to expressly indicate Acceptance or rejection of the TrustID Certificate;
- Promises to protect a Private Keys at all times, in accordance with the applicable Subscriber Agreement, this CPS, the TrustID CP, and any other obligations to which the Subscriber may otherwise have committed;
- Uses the TrustID Certificate and the corresponding Private Key exclusively for purposes authorized by the TrustID CP and only in a manner consistent with the TrustID CP;
- Instructs IdenTrust (or an RA, Trusted Agent, or employer) to revoke or request a Revocation of the TrustID Certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the

- Private Key, or, in the case of a business representative, whenever the Subscriber is no longer affiliated with the Sponsoring Organization; and
- Responds as required to notices issued by IdenTrust or its authorized agents.

Subscribers who receive Certificates from IdenTrust assert that they will comply with these requirements as well as those in the TrustID CP 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 9.6.1.2](#).

Key Usage is discussed below 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 the TrustID CP or this 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 the TrustID CP or this 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**

This process will consist of issuing a new Certificate with a new Validity Period and serial number while retaining all other information in the original Certificate, including the Public Key. Certificate renewals are currently available for CSAs. Subscribers, Issuing CAs, and External CAs cannot renew their Certificates. A Certificate may be renewed if the Key Pair has not reached the end of its validity, the Private Key has not been compromised, the End Entity name and attributes are correct and the affiliation between the Affiliated Individual and his or her Sponsoring Organization still exists. The old Certificate need not be revoked but will not be renewed further.

After Certificate renewal, the old Certificate is not revoked by IdenTrust may or may not revoke it. In any case, the system automatically prevents the Certificate to be renewed again, re-keyed or modified.

#### **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. Thus, IdenTrust may choose to implement a 3-year re-key period with an initial issuance and 2 annual renewals before re-key is required. The old Certificate need not be revoked, but must not be further re-keyed, renewed, or updated.

#### **4.6.2 Who May Request Renewal**

Only the End Entity may request Certificate renewal.

##### **4.6.2.1 Treatment of a Request for Certification of a New Key**

If out of band processes are in place to authenticate an End Entity (such as a Shared Secret or bio-metric means of identity verification), it is not necessary for an Issuing CA or RA to subject the request to a complete re-certification, even if the Private Key has been compromised.

#### **4.6.3 Processing Certificate Renewal Requests**

Renewal of the TrustID Certificate of an Affiliated Individual will require that the affiliation between the Affiliated Individual and his or her Sponsoring Organization still exists.

#### **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](#) and [Section 3.3.1](#)).

#### **4.7.3 Processing Certificate Re-Keying Requests**

For human Subscribers, 3 months before the expiration period, the IdenTrust or the RA's system may automatically notify the Subscriber that he or she must Re-key and re-establish identity by presenting his or her valid TrustID Certificate.

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.

#### 4.7.3.1 Subscribers and LRAs

During a re-key, the Subscriber must present a current valid IdenTrust-issued TrustID Certificate. This establishes a Client-authenticated SSL/TLS-Encrypted Session using the IdenTrust Certificate Management Center (CMC) user interface. The CMC user interface validates the authenticity of the Certificate presented by verifying:

- It was issued by IdenTrust
- Comparing the status of the Certificate in the relational database to confirm it is not revoked
- The Certificate is still valid (not expired)

This database is also used to issue the CRLs and provides a real-time check of the Certificate status to verify its validity (See definition of “Client-authenticated SSL/TLS-Encrypted Session” in [Section 1.6.1](#)).

IdenTrust offers re-key services through subscription renewal rekey. Beginning ninety (90) days before the expiration of a human Certificate and 30 days for server Certificates, emails are sent to the Subscriber directing them to a CMC user interface where the current valid IdenTrust-issued TrustID Certificate is used to authenticate the Subscriber through a Client-authenticated SSL/TLS-Encrypted Session.

- If the Subscriber successfully uses their Certificate to enter the CMC user interface, the Subscriber will complete the re-key through an automated online process. The Subscriber is eligible for immediate retrieval of the rekeyed Certificate after meeting the following criteria: The maximum Validity Period for Key Pair Usage as defined in [Section 6.3.2](#) and the Key usage period has not been exceeded.
- The Subscriber confirms that no information in the Certificate has changed.
- The Subscriber reviews and accepts the terms of the Subscriber Agreement.
- The Subscriber provides payment for the new Certificate.

If the Subscriber changes any information during this process, the re-key application will be referred to an RA operator for manual review. If it is determined that the Subscriber has had any information changed or any data contained in the Certificate changed, the RA will notify the Subscriber that they are not eligible for re-key and will need to apply for a new Certificate and must appear in-person or remotely for Identity Proofing.

If the modified information is not information that is included in the Certificate, (such as a telephone number), the RA operator will approve the re-key request and send a notification via courier or U.S. mail including the retrieval instructions for the re-keyed Certificate.

If the Subscriber cannot present their Certificate or changes specific information, related to verification (personal information, Organization affiliation, etc.) he or she is not eligible for re-key and must apply for a new Certificate and appear for in-person or Remote Identity Proofing.

Refer to [Section 4.7.1](#) Circumstances for Certificate Re-Key for guidance regarding re-key for non-Subscriber and LRA Certificates.

For server Certificates, the PKI Sponsor/ Subscriber will follow the same steps to check the content for the server Certificate is still accurate and valid. If the PKI Sponsor indicates that any of the contents of the server Certificate have changed during the re-key (e.g., the FQDN(s) and Organization information), the RA will request verification information in accordance with the verification processes set forth in [Section 3.2](#) before the re-key process can be completed. Additional steps processing steps must be executed as required for EV Server Certificates, or EV Code Signing Certificates, in accordance with the [CS BR](#).

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 4.3.3](#).

### **4.8 CERTIFICATE MODIFICATION**

Certificate modification consists of creating new Certificates with Subject information that may differ from the old Certificate. IdenTrust provides 2 types of Certificate modification with the type of modification being dependent on the type of Certificate. The first type of modification, replacement, is available for all Certificate types. For this type of modification, all original information is kept. The second type of modification is available for server Certificates only and allows the PKI Sponsor to add, remove and modify the FQDN(s) within the Certificate. For both types of Certificate modification, the new Certificate has a new associated Key but retains the same expiration date.

When other information in the Certificate's Subject field changes (e.g., the last name, Sponsoring Organization's name), Certificate modification is not used. Instead, a new application for a Certificate is required.

Root CA Certificate and Subordinate CA Certificate modification consists of creating a new Certificate where information can be changed including different fields such as Subject, Certificate policies, CRL distribution point, and authority information access. The associated Public Key and original expiration date are maintained.

After a server Certificate modification, the old Certificate is not revoked by IdenTrust, or the RA and the Subscriber may or may not revoke it. In any case, the system automatically prevents the Certificate from being modified again, re-keyed, or renewed.

#### **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.

IdenTrust may request a modification of its Root and Subordinate CA Certificates.

## **4.8.3 Processing Certificate Modification Requests**

Upon receiving an authenticated request to replace a damaged or lost Certificate from a Subscriber (i.e., Personal or business) or an authorized official of a business entity for a business representative Subscriber, IdenTrust replaces the 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 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**

##### **4.9.1.1.1 Reasons for Revoking Non-Server Subscriber Certificates**

IdenTrust shall revoke a Certificate within 24 hours if one or more of the following occurs:



1. The Subscriber requests in writing that IdenTrust revoke the Certificate;
2. The Subscriber notifies IdenTrust that the original Certificate Request was not authorized and does not retroactively grant authorization;
3. IdenTrust obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
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\(5\)](#);
5. 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 to generate the Private Key was flawed;
6. IdenTrust obtains evidence that the validation of domain authorization or mailbox control for any Mailbox Address in the Certificate should not be relied upon.
7. IdenTrust has reasonable assurance that a Certificate was used to sign Suspect Code.

IdenTrust should revoke a Certificate within 24 hours and shall revoke a Certificate within 5 days if one or more of the following occurs:

8. The Certificate no longer complies with the requirements of [Section 6.1.5](#) and [Section 6.1.6](#);
9. IdenTrust obtains evidence that the Certificate was misused;
10. IdenTrust is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
11. IdenTrust is made aware of any circumstance indicating that use of an email address or Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g., a court or arbitrator has revoked the right to use an email address or Domain Name, a relevant licensing or services agreement between the Subscriber has terminated, or the account holder has failed to maintain the active status of the email address or Domain Name);
12. IdenTrust is made aware that the Certificate was not issued in accordance with the CA/B Forum BRs or with IdenTrust's CP and/or CPS;
13. IdenTrust is made aware of a material change in the information contained in the Certificate;
14. IdenTrust determines or is made aware that any of the information appearing in the Certificate is inaccurate or misleading;
15. IdenTrust or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
16. IdenTrust's right to issue Certificates under these Requirements expires or is revoked or terminated, unless IdenTrust has made arrangements to continue maintaining the CRL/OCSP Repository;
17. Revocation is required by IdenTrust's CP and/or CPS; or
18. 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.

IdenTrust may delay revocation of a Code Signing Certificate based on a request from Application Software Suppliers where immediate revocation has a potentially large negative impact to the ecosystem.

**Note:** Nothing herein prohibits IdenTrust from revoking a Code Signing Certificate prior to these time frames.

#### **4.9.1.1.2 Reasons for Revoking Subscriber Server Certificates**

With the exception of Short-lived Subscriber Certificates, IdenTrust will revoke a Subscriber server Certificate 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 server Certificate within 24 hours and must revoke a Subscriber server 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 BRs (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 BRs 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 BRs 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 BRs 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.
- 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. Other third parties may submit Certificate Problem Reports informing the Issuing CA of reasonable cause to revoke the Certificate. See [Section 4.9.1.1.2](#).

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

#### **4.9.3 Procedure for Revocation Request**

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 system.

If the Private Key is not available, Revocation can be accomplished by contacting an LRA, Enterprise RA, or a Trusted Agent and undergoing an Identity Proofing process based on the procedures outlined in [Section 3.2.3](#). In this case, a request for Certificate suspension can be submitted while a complete Identity Proofing process is performed. The Certificate remains suspended until further verification is completed and the request resolves into a Revocation or unsuspension if not a subscriber server Certificate.

The Subscriber or PKI Sponsor should first attempt to contact the LRA, Enterprise RA, or Trusted Agent who was involved during the Issuance of the Certificate or the Trusted Agent of their Sponsoring Organization. LRAs and Enterprise RAs can revoke the Certificate upon completion of positive Identity Proofing.

Trusted agents must complete another process to complete the Revocation. After positive Identity Proofing has been performed and when a Trusted Agent intermediates a Revocation request, the LRA will authenticate

Trusted Agent's signed Revocation request emails by verifying (i) the Trusted Agent has a Valid Certificate of commensurate of the Certificate to be revoked (i.e., a Trusted Agent may submit a request to revoke a TrustID Business Certificate when he or she has a TrustID Business Certificate) (ii) the authority to request actions on behalf to the Sponsoring Organization. The authority to request is validated based on lists put together by LRAs based on the paperwork that nominates the Trusted Agent. The list contains identifiers that uniquely identify the Trusted Agent (i.e., Name, Certificate's thumbprint/fingerprint / serial number).

Additionally, Certificates for an Electronic Device can be revoked by additional methods. The PKI Sponsor can revoke the Certificate once they authenticate and request a Revocation on a secure online web page using a server-authenticated SSL/TLS Encrypted Session and the account number and Account Password used by the PKI Sponsor during initial registration. If the PKI Sponsor no longer has the account number or cannot remember the Account Password, then identifying information of the PKI Sponsor obtained during registration can be used to authenticate the PKI Sponsor's request (e.g., the Sponsor can be called at the phone number previously established during registration.) In addition, a Digitally Signed request from the PKI Sponsor that enables the LRA or Enterprise RA to link the PKI Sponsor to the Certificate, using the electronic records in the RA or CA system, is considered valid.

See [Section 1.5.2](#) 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](#) - CRL and CRL Entry Extensions.

The Subscriber or PKI Sponsor is required to present an acceptable form(s) of photo identification (See [Section 3.2.3.1](#)), which the LRA, Enterprise RA, or Trusted Agent reviews to identify and authenticate the Subscriber or PKI Sponsor making the Revocation request. Trusted Agents notify LRAs immediately upon validating the Revocation request and request that the LRA revoke the Certificate.

If the Cryptographic Module cannot be obtained from the Subscriber, then the Subscriber's Certificate(s) will be immediately revoked, expressing the reason code as "Key compromise." Promptly after Revocation, IdenTrust updates the Certificate status in the Repository and updates the CRL. Alternatively, a Sponsoring Organization may opt for not collecting any Cryptographic Module due to logistical difficulties (e.g., Subscriber is terminated under unfriendly conditions, Subscriber in a remote location, etc.) and instead always request Revocation of the Certificates as if the Cryptographic Module was not obtained from the Subscriber. In these cases, the Revocation request will always result in a "Key compromise" code.

#### **4.9.3.1 Procedure for Revocation Request of Subscriber Certificate by Subscriber**

Before revoking a Certificate, IdenTrust verifies the identity and authority of the entity requesting Revocation and will proceed with the Revocation within 24 hours if one or more of the following events take place:

The Subscriber requests written Revocation.

The Subscriber notifies IdenTrust that the original Certificate request was not authorized.

IdenTrust obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate was compromised.

IdenTrust obtains evidence that the validation of domain authorization or control for any FQDN or IP Address in the Certificate should not be relied upon.

#### **4.9.3.2 Procedure for Revocation by a PKI Sponsor or Sponsoring Organization**

A PKI Sponsor or Sponsoring Organization is responsible for promptly requesting Revocation of a TrustID Certificate:

- When any of the identifying information, affiliation, name components, or attributes contained in the Certificate become invalid;
- When the Private Key or the media holding the Private Key, associated with the TrustID Certificate is, or is suspected of having been, compromised and no longer complies with the TrustID CP;
- If IdenTrust obtains evidence that the Certificate was misused;
- When the Individual named as a business representative or no longer represents or is no longer affiliated with the Sponsoring Organization;
- The Subscriber or other authorized party, as defined in an applicable agreement (e.g., bulk submission agreement), asks for his/her Certificate to be revoked;
- For Server and FATCA Organization Certificates, the Sponsoring Organization notifies the CA that the original Certificate request was not authorized and does not retroactively grant authorizations; or
- IdenTrust is made aware that a wildcard Certificate has been used to authenticate a fraudulently misleading Subordinate CA FQDN.

Failure to request Revocation under these circumstances is at the Subscriber's risk.

When a Revocation has occurred, IdenTrust reflects this change in the CRL as explained in [Section 4.7](#) and [Section 4.8](#). The Certificate information (i.e., serial number) remains in the CRL until after the Certificate expiration date.

#### **4.9.3.3 Procedure for Revocation of Server and Non- Server Certificates by IdenTrust**

As outlined in [Section 4.9.1](#)

##### **4.9.3.3.1 Procedure for Revocation of Procedure for Revocation of CA, CSA Certificate**

IdenTrust will revoke a CA or CSA Certificate it has issued if the Private Key corresponding to the Public Key in the Certificate has been or is suspected to have been compromised. In any event, before taking such action, the highest level IdenTrust Operations Manager available will convene a meeting of management representatives (including representatives of the affected RAs and IdenTrust PMA) to assess the situation and make an appropriate decision concerning a course of action.

##### **4.9.3.4 Procedure for Revocation of Subscriber's Certificate by Other Participants**

When a request for Revocation does not originate from the Subscriber or PKI Sponsor, it must be made in-person by an authorized person who meets the requirements of [Section 4.9.2](#), and it must be accompanied by adequate proof of identity and authority. LRAs, Enterprise RAs, and Trusted Agents are provided with instructional material on methods to authenticate Revocation requests made by third parties. Trusted Agents cannot process the Revocation of the Certificate, but he or she will obtain the verification of the request and send that information via phone or email to the LRA to process the Revocation.

The LRAs, Trusted Agents, or Enterprise RAs, validate the credentials of the requesting party and determine if the Revocation request meets the requirements of [Section 4.9.1](#). It is the responsibility of the LRA, Enterprise RA, or Trusted Agent to investigate the alleged reason for Revocation and to determine whether Revocation is appropriate. If the Cryptographic Module cannot be obtained from the Subscriber, then the Subscriber's Certificate(s) will be immediately revoked, expressing the reason code as "Key compromise." If Revocation is appropriate, the LRA, Enterprise RA, or Trusted Agent document information concerning the identification of the requestor, the Certificate, and the reason for the request. After verification, an LRA or Enterprise RA can execute the Revocation. Trusted Agents cannot process the Revocation. If a Trusted Agent receives a Revocation request, they will verify the request and forward the Revocation request via signed email and mail the documentation supporting the request to the LRA for archival. The request will be reviewed, verified, and executed by an LRA upon checking the credentials of the signed email and the contents of the message.

Requests of Revocation of all other Certificates is done either with a Digitally Signed Revocation request using the Private Key corresponding to the Certificate being revoked or by the authenticated request of an authorized representative of the RA who is identified and authenticated in accordance with [Section 3.2.2](#) and [Section 3.2.3](#).

#### **4.9.3.5 Procedure for Revocation by Non-Authorized Requestors**

Any Certificate Revocation requests from other, non-authorized requestors must be submitted to IdenTrust. If IdenTrust determines that Revocation is appropriate, it will be revoked as specified below.

#### **4.9.3.6 Execution of Revocation by LRAs and Enterprise RAs**

Account restrictions exist in the CA and RA Systems that prevent an LRA or Enterprise RA from requesting or approving the Revocation of Certificates of Subscribers who are not within their Organization, domain, Subscriber community, etc. The LRA's or Enterprise RAs Certificate is compared against the Access Control List (ACL) and, if authorized for that domain or namespace, the LRA or Enterprise RA executes the Revocation.

The LRA or Enterprise RA will revoke the Certificate through a Client-authenticated SSL/TLS-encrypted Session with the CA System. Alternatively, the LRA or Enterprise RA can revoke the Certificate through an RA System that submits the Revocation to the CA via a Server-authenticated SSL/TLS-encrypted session using a Digitally Signed data structure. IdenTrust will change the Certificate status in the Repository from valid to Revoked. Revocation occurs when the serial number and other identifying information for the Certificate being published in a CRL. In any event, all Certificate Revocation requests should be promptly communicated to IdenTrust.

It is the LRA or Enterprise RA's responsibility to send the Subscriber an email notice with a brief explanation of the reasons for Revocation and to archive such notice. IdenTrust and RA system can be configured to automatically send Revocation notification emails to Subscribers.

#### **4.9.3.7 General Guidance for All Situations not Specifically Addressed**

Persons authenticating Revocation requests must balance the risk of an unauthorized request and the potential harm caused by revoking the Certificate against the harm caused by not revoking the Certificate.

Trusted Agents, Enterprise RAs, and LRAs are trained to expedite authentication and authorization checks on Revocation requests and to affect them on the CA as soon as possible.

Refer to [Section 4.10.2.1](#) "Certificate Problem Reporting" for details on submitting revocation request or reporting Certificate issues to IdenTrust.

#### **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 or Suspect Code 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 4.9.1.1.2](#). 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.

For Code Signing Certificates, the 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.

#### **4.9.6 Revocation Checking Requirements for Relying Parties**

The use of revoked Certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new Revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a Certificate whose Revocation status cannot be guaranteed. Therefore, before relying on a TrustID Certificate an Authorized Relying Party must conduct a validation request in accordance with the method and procedures established by the Issuing CA pursuant to [Section 4.10](#). If it is temporarily infeasible to obtain Revocation information, then the Relying Party must either reject use of the Certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a Certificate whose authenticity cannot be guaranteed to the standards of the TrustID CP and this CPS.

IdenTrust shall have no liability if a Relying Party does not obtain an OCSP response indicating that the Certificate is valid or fails to check the most recent CRL for Certificate Revocation.

#### **4.9.7 CRL Issuance Frequency**

IdenTrust CRLs are available via this publicly-accessible HTTP URL: <http://crl.dentrust.com>.

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.

IdenTrust CAs issuing Subscriber Certificates:

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.

IdenTrust CAs issuing CA Certificates:

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.

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

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

#### 4.9.8 Maximum Latency for CRLs

IdenTrust publishes a CRL within commercially reasonable time after authenticating a Revocation request. Each CRL is published no later than the time specified in the nextUpdate field of the previously issued CRL for the same scope.

#### 4.9.9 Online Revocation/Status Checking Availability

##### 4.9.9.1 Non-Server Certificates

The IdenTrust Certificate Status Authority (CSA) supports OCSP and provides online Certificate status information in Digitally Signed OCSP responses in accordance with the [RFC 6960](#) for Certificates issued by Root CAs and Subordinate CAs that are indicated in OCSP Requests submitted by Relying Parties.

When provided, OCSP responses shall conform to the [RFC 6960](#) and/or the [RFC 5019](#). OCSP responses are either:

1. Be signed by the IdenTrust that issued the Certificates whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose Certificate is signed by the IdenTrust CA that issued the Certificate whose revocation status is being checked.

##### 4.9.9.2 In the latter case, the OCSP signing Certificate contains the ocspsigning EKU (1.3.6.1.5.5.7.3.9) and an extension of type id-pkix-ocsp-nocheck, as defined by the [RFC 6960](#). Server Certificates

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

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, 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 the [RFC 6960](#) and/or the [RFC 5019](#). IdenTrust may process the Nonce extension (1.3.6.1.5.5.7.48.1.2) in accordance with the [RFC 8954](#).

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

- Effective 2025-01-15, 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 the [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 in [Section 7.1.2.8 of the TLS BR](#).

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. If the OCSP responder is for a CA that is not Technically Constrained in line with [Section 7.1.2.3 of the TLS BR](#) or [Section 7.1.2.5 of the TLS BR](#), the responder must not respond with a “good” status for request.

#### **4.9.10 Online Revocation Checking Requirements**

The use of revoked Certificates could have damaging or catastrophic consequences. The matter of how often new Revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a Certificate whose Revocation status cannot be guaranteed.

##### **4.9.10.1 Non-Server Certificates**

IdenTrust supports an OCSP capability using the HTTP GET method as described [RFC 6960](#) and/or [RFC 5019](#).

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds

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.

#### **4.9.10.2 Server certificates**

No stipulation.

#### **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](#) and [Section 4.8.9](#) in cases of (i) IdenTrust mis-issued the Certificate, (ii) the Certificate was used to sign Suspect Code, or (iii) 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**

IdenTrust allows Certificate suspension as a mechanism to minimize risk and illegitimate use. The LRA verifying a Certificate suspension request may suspend a Certificate when the risk of Certificate use by not suspending may outweigh the risk of preventing legitimate Certificate use (i.e., denial of service) by suspending it. This risk evaluation is at the discretion of the LRA (for Human Certificates) based on the situation and information available at the time.

Suspension is not available for any server or Code Signing 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**

The only persons permitted to request Revocation or suspension of a TrustID Certificate issued pursuant to this CPS are the Subscriber, the PKI Sponsor on behalf of the Sponsoring Organization, the Issuing CA, the RA, an Enterprise RA, or Trusted Agent who performed the Identity Proofing process.

#### **4.9.15 Procedure for Suspension Request**

A suspension may be requested at any time for any reason. To effect a suspension, minimal identity validation may be required depending upon the circumstances (source of the request, circumstances for the request, etc.) and when completed, IdenTrust changes the Certificate status in the Repository from valid to suspended (i.e.,

reason code CertificateHold). Should a Revocation be requested during or after the suspension takes effect, the verification of the Revocation request should be completed using the procedures outlined in [Section 4.9.3](#).

#### **4.9.15.1 Suspension of Subscriber Certificate by Subscriber or PKI Sponsor**

A Subscriber or PKI Sponsor, who is unable to submit a signed or in-person-authenticated suspension request, can submit a request for suspension through an unsigned email or phone call to a Trusted Agent or LRA. If the Trusted Agent is the first contact, they will contact the LRA by phone or by email to complete the suspension after verification. This type of request will trigger a suspension process at the discretion of the LRA based on the information available at the time of the request.

The minimum necessary identity validation is accomplished if the request is:

- submitted from the Subscriber's email in the Certificate to be suspended or in the case of the PKI Sponsor, from email on record; or
- received through a phone call, and the LRA can positively obtain any 3 pieces of information from the caller that identify the Subscriber or PKI Sponsor in the system (e.g., identification number such as social security number or driver's license, address, date of birth (DOB,) employer, job title, etc.).

There are only 2 outcomes when a Certificate has been suspended: Revocation or unsuspension. After the Certificate is suspended and Certificate use is restricted, the Trusted Agent or LRA will use the processes described in [Section 4.9.3](#) to execute a Revocation if it is requested by the Subscriber or if circumstances require.

The Subscriber may ask for an unsuspension at any time by sending a written statement with a wet signature that has been notarized.

#### **4.9.15.2 Suspension of Subscriber Certificate by Other Participants**

Participants, who are different than the Subscriber or PKI Sponsor, may request a suspension at any time. The request can be submitted by sending an unsigned email request, calling the Trusted Agent or LRA, or submitting instructions through the Certificate Problem section available on the IdenTrust Support webpage.

To process the suspension identity validation will be required if the request comes from the Organization associated with the Subscriber. The LRA may accept a request from an email (signed or unsigned) with a Domain belonging to the Sponsoring Organization in the Certificate to be suspended. When the request is received through a phone call, the Participant is guided to submit the request via an email compliant with the conditions above.

If the Trusted Agent is the initial recipient of the request, he or she will submit a suspension request in a signed email to the LRA who has access to the system. If the LRA is the initial recipient, the suspension can be executed at the discretion of IdenTrust.

There are only 2 outcomes when a Certificate has been suspended: Revocation or unsuspension. After the Certificate is suspended and Certificate use is restricted, the Trusted Agent or LRA will use the processes described in [Section 4.9.3](#) to request (Trusted Agent) or execute a Revocation (LRA) if it is requested by the Subscriber/associated Sponsoring Organization or if circumstances require.

The Trusted Agent or a member of Sponsoring Organization (specifically a company officer or human resources management) may ask for an unsuspension at any time by sending a written statement with a wet-signature that has been notarized and verified by an LRA as associated with the Subscriber's account.

#### **4.9.16 Limits on Suspension Period**

No stipulation.

## 4.10 CERTIFICATE STATUS SERVICES

IdenTrust uses OCSP and CRLs to distribute Certificate status information. Specifics on how to obtain status information via CRL or OCSP are found in [Section 7.2](#) and [Section 7.3](#).

At the time of execution of a status change, the LRA or Enterprise RAs use administrative interfaces that clearly link the Subscriber's identity information with the Certificate whose status is being modified. The LRA or Enterprise RA is given the opportunity to cancel any changes before effecting the final approval. However, after the change is approved but before it is published, no review or changes are possible.

### 4.10.1 Operational Characteristics

IdenTrust validates the status of the TrustID Certificate indicated in a Certificate validation request message in accordance with the [RFC 6960](#).

Revocation entries on the CRL or OCSP Response will not be removed until after the expiry date of a revoked Certificate, except for Code Signing and Time-Stamping Certificates which remain on the CRL or OCSP for at least 10 years after revoked or expired; See details in [Section 7.2](#).

### 4.10.2 Service Availability

IdenTrust operates and maintains CRL and OCSP capability with resources sufficient to provide a response time of ten (10) seconds or less. IdenTrust Root CA Certificates, CRLs, and online TrustID Certificate status information are available for retrieval 24 hours a day, seven7 days a week, with a minimum of 99% availability overall per year, and scheduled downtime does not exceed 0.5% annually, excluding network outages. CRLs are also available at: <http://validation.identrust.com/crl/>. The specific location depends on the Issuance of the Certificate signing the CRL.

Additionally, online Certificate status information is available through IdenTrust's TrustID validation services through OCSP. The validation services can be found at <https://commercial.ocsp.identrust.com>.

#### 4.10.2.1 Certificate Problem Reporting

IdenTrust provides Subscribers, Relying Parties, Application Software Suppliers, and other third parties with contact information for reporting suspected Private Key compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to the TrustID Certificates. The contact details are available online at the IdenTrust website in the "OUR HELPFUL SUPPORT TEAM" webpage at: <https://www.identrust.com/support/support-team>.

This page lists a telephone number to contact Customer Support Representatives during business hours and an email contact to ensure reporting will be received 24/7. In this page, use the link at the bottom to [Report Certificate Security Compromise Issues](#).

Once a report is received either by email or telephone call, a Customer Support Representative will file a ticket for the report including the details provided by the contact. The Customer Support Representative will provide the following information for the report when possible:

1. Account number;
2. Name and contact information of the Individual/Organization reporting the Certificate;
3. Subscriber, Organization, domain, and/or PKI Sponsor name;
4. Nature of the issue (illegal activity, Private Key compromise, etc.); and
5. When the issue was discovered.

Once that ticket is filed, the Customer Support Representative will forward that contact with the details and ticket number to the appropriate level of management or the Security Office via email. Upon creating a record of the contact, the following considerations are assessed to determine the appropriate action:

1. The nature of the alleged problem;
2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
3. The entity making the complaint (for example, a complaint from a law enforcement official that a website is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that he/she didn't receive the good they ordered); and
4. Relevant legislation.

Upon review, IdenTrust security, or an appropriate level of management, will determine whether Revocation, suspension, or other action is warranted. If it is determined that Revocation or suspension is necessary, The Security Office or management will send an official request to a Customer Support Representative or an LRA to execute the specified action accordingly. When deemed necessary based on the content of the report and the findings by Security and management, IdenTrust will forward the complaint to law enforcement.

All email contact associated with the case must be saved and documented by the Customer Support agent.

To respond to high-priority Certificate Problem Reports IdenTrust maintains the Certificate Problem Reports support page 24/7 whether by telephone contact during office hours or email contact during the evening, weekend, or holiday hours.

#### **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.

For server Certificates, 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**

If a Key Pair is used for signature and confidentiality purposes, recovery of the Private Key is prohibited. If an encryption Certificate is issued and retrieved separately from the signing Certificate, IdenTrust does offer selective services to recover the Private Key of the Encryption Certificate only. IdenTrust does not provide the mechanisms (hardware, software, or procedural) that permit recovery of the Private Key of TrustID Certificates. The Encryption service may or may not be available for TrustID Certificates. The following steps provide the stipulations for Key recovery.

#### **4.12.1.1 Circumstances for Private Key Recovery**

There are no circumstances for Private Key Recovery for TrustID Certificates because the Private Key is not held in escrow.

#### **4.12.1.2 Key Recovery Roles: Who can Request Private Key Recovery**

When and if the Key Recovery feature is enabled for TrustID, a request for Key recovery may be made by the Subscriber using his or her signature Private Key for purposes of authentication (automated self-recovery) or by any Individual who can demonstrate a reasonable authority and lawful need to obtain a recovered Key (a Requestor).

### **4.12.2 Session Key Encapsulation and Recovery Policy and Practices**

#### **4.12.2.1 Automated Self-Recovery**

When and if the Key Recovery feature is enabled for TrustID, the Subscriber is authenticated to the Key escrow system using a valid, approved CA Certificate. The identity of the Subscriber for the escrowed Key to be recovered is authenticated during automated self-recovery when the Subscriber attempts to access IdenTrust's Certificate Management Center (CMC) or a similar facility for hosted registration processes. Subscribers are asked to present their digital Certificate or apply their Digital Signature and authenticate themselves to the CMC or similar facility. The encryption key cannot be recovered unless the corresponding Digital Signature Certificate is presented which is an equivalent to the Certificate whose companion Private Key is being recovered (e.g., a TrustID Business Certificate cannot be recovered with a TrustID Personal Certificate). Once the Subscriber has authenticated himself/herself to the CMC or hosted facility, the Subscriber's PKCS#12 and the Account Password are extracted from the Key Escrow Database (KED) and made available to the Subscriber during a secure, online session. The Subscriber is then required to install the Key in a cryptographic container meeting the same security level for the Certificate, as specified in the Subscriber Agreement and the Certificate Policy for the corresponding product.

#### **4.12.2.2 Session Key Encapsulation and Recovery Policy and Practices**

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

## 5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The [NetSec BR](#) is incorporated by reference as if fully set forth herein.

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.

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.

The Certificate Management Process must 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.

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.

IdenTrust and its associated Trusted Agents, RAs, CSAs, and Repositories maintain security controls to assure adequate security for all information processed, transmitted, or stored for the TrustID Program. This includes appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or Tokens) used in connection with providing CA services.

Adequate security means protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. Systems and applications used by Relying Parties operate securely and provide appropriate protection for confidentiality, integrity, and availability.



Adequate security includes physical security and environmental controls (system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention), network security and firewall management (port restrictions and IP Address filtering), user management (separate Trusted Role assignments, education, awareness, and training), and logical access controls (activity logging, and inactivity time-outs to provide Individual accountability).

No party may use any software, program, routine, query, device, or manual process in an attempt to bypass security measures (including attempting to probe, scan or test vulnerabilities to breach security) unless that party has a legitimate business need to do so and such activities have been authorized by the Head of Operations or another Risk Management Committee member, provided that no Risk Management Committee member shall authorize themselves or a person, directly or indirectly, under their management; interfere with the proper operation of IdenTrust's CA systems; or impose a disproportionately large load on (i.e., overload or crash) the infrastructure supporting IdenTrust's systems (e.g., DoS/DdoS attacks, viruses, etc.).

IdenTrust's CA, CSA, and RA equipment, including production and backup Cryptographic Modules, is located in IdenTrust's primary facility located in Utah. Backup equipment for TrustID Certificates, excluding Cryptographic Modules, are also located at the disaster recovery facility in Colorado.

IdenTrust has 3 facilities dedicated to hosting CMA equipment:

- Primary Data Center in Utah
- Operations Center in Utah
- Disaster Recovery Data Center in Colorado

For each system, Trusted Role employees assure that there is adequate security within the system, including ways to prevent, detect, and recover from security problems. The CA, CSA, and RA operations for TrustID Certificates are serviced by trusted IdenTrust personnel. All IdenTrust personnel with Trusted Roles meet the requirements of the TrustID CP for Trusted Roles.

The IdenTrust security program includes an annual risk assessment conducted by Security Officers and other Trusted Role employees as directed by the Risk Management Committee. This program includes identifying foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate management processes. It also assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate management processes. In addition, it assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that IdenTrust has in place to counter such threats.

## 5.1 PHYSICAL SECURITY CONTROLS

IdenTrust and all associated Trusted Agents, RAs, CMAs, and Repositories, provide appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or Tokens) used in connection with providing IdenTrust CA services. Access to such hardware and software is limited to those personnel performing in a Trusted Role as described in [Section 5.2.1](#).

IdenTrust implements a physical and environmental security program that addresses access controls, water exposure, fire safety, failure of supporting utilities, media storage, waste disposal, offsite backup capabilities, structural collapse, interception of data, and control of mobile and portable systems.

IdenTrust CA secure environment is protected by the security controls described below, as outlined in [Section 4.5.1 of the RFC-3647](#) which are designed, built and maintained in accordance with risk assessments conducted by IdenTrust:



### **5.1.1 Site Location and Construction**

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

IdenTrust's CA system is housed in an unmarked secure Datacenter, 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.

#### **5.1.1.1 Primary Facility**

The building that houses the Datacenter has been designed for environmental safety and security. It is constructed to Class-4 seismic standards, exceeding the Class-3 earthquake zone in which it is located. To prevent water damage, the IdenTrust systems are located on the second floor of the building, which is sited in an area where flooding is virtually nonexistent. The building itself contains subfloor curbing to prevent any water or moisture from affecting computer equipment or cabling. The building is also designed so that no water lines or plumbing fixtures exist directly above or below the Datacenter areas.

For further protection, subfloor sensors alert the building staff if water or high moisture is detected. For fire protection, the building has a full complement of VESDA sensors that automatically alert both building staff and fire authorities if smoke is detected. The Datacenter areas are also equipped with Inergen inert-gas fire suppression systems. To protect against excessive temperatures, the building has an overcapacity heating/cooling tower, with redundant HVAC systems for backup.

Telecommunications are obtained from multiple providers using separate access points to the building.

The building has environmental sensors that signal a network operations center that is staffed during business working hours.

The facility is located less than one-half mile from a major power generation plant and substation, with power coming directly from the substation into the site over nonpublic lands. Additionally, the facility maintains its UPS and backup generator, which are maintained and tested routinely.

#### **5.1.1.2 Disaster Recovery Facility**

IdenTrust's disaster recovery Datacenter is located in the intermountain region of the United States of America. This area in which it is located is not prone to such environmental hazards as tornadoes, earthquakes, hurricanes, forest fires, etc. The Datacenter is housed in an unmarked concrete unmarked building; the site is not identified as housing IdenTrust equipment in any way. The Datacenter is located on a raised level, at least 24 inches above the normal first-floor level, in an area with no windows.

Multiple layers of security surround the CA, CSA, CMS, and RA equipment in the disaster recovery center, including at least the following:

1. Trees, berms, and other natural barriers protecting the building itself, with bollards protecting the entrance;
2. Restricted access to the building, requiring preapproval and electronic badges;
3. Restricted access to the general Datacenter room, requiring preapproval and multiple factors of authentication including biometrics;

4. Restricted access to the IdenTrust secure cage, requiring preapproval and 2-person, dual-factor access including biometrics. Locked cabinets within the secure cage, which house the equipment itself.

The IdenTrust secure area is a cage with chain-link fencing forming the walls and ceiling, and with additional barriers to prevent access from under the floor. The area is surveilled 24x7x365 by both building cameras and IdenTrust's camera system, which can be monitored in real time, searched for past events, or logged, if necessary, by the IdenTrust Security Office. No cameras are placed in such a way that on-screen data could be captured.

## **5.1.2 Physical Access**

IdenTrust provides physical access controls designed to provide protection against unauthorized access to its TrustID system resources.

### **5.1.2.1 Physical Access for CA, CSA, and RA Server-Side Equipment in the Primary Facility**

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 with staff onsite during normal business hours. Dedicated facility staff are responsible for monitoring the facility outside of normal business hours and are available to respond to any issues that may arise.

The staff members from the hosting facility perform frequent checks of the facility. Additionally, IdenTrust's Security Office performs checks and reviews of the physical security integrity of the facility to ensure that alarms, access points, biometric readers to access the Secure Room, safes containing Cryptographic Modules and activation materials, video cameras, storage containers, access logging equipment, and other items, are functioning correctly. A record of these reviews is kept that describes the types of checks performed, the time, and the person who performed them. Records are kept for no less than one year and reviewed with external auditors annually as part of the WebTrust for CA audit described in [Section 8](#).

Programmable electronic badges are required for employee entrance to the grounds and to the external foyer of the building. Entrance into the public and Datacenter areas of the building requires preapproval and registration, and 2-factor authentication, including programmable electronic badges; these programmable electronic badges permit entry only into those Datacenter areas authorized by the appropriate building tenants.

Both Datacenter and IdenTrust employees are prohibited from permitting unknown or unauthorized persons to pass through doors, gates, and other entrances to restricted areas when accessing the facilities. Authorization for any persons, including vendors, repair persons, or visitors, to enter the IdenTrust portion of the facility must be obtained in advance from the Security Office or Operations Management.

Visitors are allowed within the fence only with authorization from the guard in the control center after properly identifying themselves, their purposes, and the persons they will visit. Also, visitors are only allowed to access IdenTrust offices after their visits' purposes and their identities have been verified, they have presented government-issued photo identification for entry into an electronic visitor log, and at least one IdenTrust employee escorts them. Visitors are not allowed in nonpublic areas of the building without escorts.

The Secure Room is physically secured with 2-person dual-factor authentication including biometrics, using an access system under exclusive IdenTrust control. The room is also equipped with a 24x7x365 camera system that is monitored and reviewed by the Security Office. Only previously authorized IdenTrust Trusted Role employees are granted access to the Secure Room. Such authorization is granted by the Head of Operations, or when so designated, by the Security Office.

The Secure Room is required to be under 2-of-M person control at all times when Individuals are present in the room. By Policy, M is kept to the lowest number of Trusted Role employees, which still allows for enough personnel to cover the needs of IdenTrust's diverse customer base. 2-person control is enforced through strict Policy provisions, as well as the access system described previously. At no time is any Individual left alone in the

Secure Room. 2 approved Trusted Role employees accompany any additional personnel or contractors at all times.

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.

In addition to the electronic entry and exit logs generated by the biometrics access-control system, each entry into, and exit from, the Secure Room is logged with the Individuals' names, entry and exit times, date, and reason for access. Before signing out and departing the Secure Room, IdenTrust personnel accessing the Secure Room are required by Policy to check that all physical protection is in place, that all sensitive materials are securely stored, and that the alarms are properly armed.

CA, CSA, and RA equipment are located inside locked computer cabinets within the IdenTrust Secure Room. Cabinet Keys are accessible by the same number of Trusted Role employees who have access to the Secure Room. CA and CSA Cryptographic Modules are secured in the locked computer cabinets within the IdenTrust Secure Room when in use. When not in use the Cryptographic Modules and activation materials are securely stored in the safes. The Security Office reviews the following on a periodic basis to determine if any Secure Room access violations have occurred, all of which are maintained by the Security Office:

- Written access logs;
- Video surveillance tapes; and
- Electronic 2-factor access logs

After review, all such logs are archived and kept securely offsite by the Security Office for not less than one year.

#### **5.1.2.2 Physical Access for CA, CSA, and RA Server-Side Equipment in the Disaster Recovery Facility**

The staff of the disaster recovery Datacenter facility performs checks of the facility at least once a day, covering the facility's access points, cameras, and other aspects of a physical walk-through. A record is kept that describes the types of checks performed, the time, and the person who performed them. Records are kept by facility staff for not less than one year and are available for review with external auditors as part of the WebTrust for CA and other audits.

Only IdenTrust Trusted Role personnel with relevant business needs may access the building and the IdenTrust secure cage. Such access requires preauthorization by the IdenTrust Security Office, permission by the building staff, and programmable electronic badges.

Access to the area where the secure cage is located requires 2-factor authentication including biometrics. The secure cage is physically secured by an IdenTrust-owned system that requires 2-person, dual factor authentication including biometrics. The cage is equipped with an IdenTrust-owned 24x7x365 camera system that is monitored and can be searched and logged, by the IdenTrust primary Security Office. The area surrounding the IdenTrust secure cage is also surveilled by building cameras that are constantly monitored by building staff. CA equipment is located inside locked computer cabinets within the IdenTrust secure cage. Cabinet keys are maintained by the same number of Trusted Role employees who have access to the secure cage.

#### **5.1.2.3 Physical Access for RA Client-side Equipment in the Primary Facility**

The building in which the RA client-side equipment is housed has restricted access during non-business hours, requiring preapproval and programmable electronic badges. IdenTrust's Security Office performs periodic checks and reviews of the security integrity of the RA room to ensure that alarms, access points, video cameras, storage

containers, access logging, etc., are operational and functioning correctly. A record is kept that describes the types of checks performed, the times, and the persons who performed them. Records are archived and kept securely offsite for no less than one year and are reviewed with external auditors annually.

Employees are prohibited from permitting unknown or unauthorized persons to gain access to the RA room. Authorization to enter must be obtained in advance from the Security Office or Operations Management. Visitors are allowed within the RA room only after properly identifying themselves and the purposes for their visits and are not allowed in the room without escorts. All entry to the RA Room is logged electronically.

Cryptographic Modules used to access RA workstations require Activation Data that is closely held and protected by workstation users. When not in use, each module is locked or under the control of its user.

In cases where RAs host client-side equipment, the RA and LRAs are obligated by contract and Policy to host the LRA workstation in a facility with controls that reduce the risk of unauthorized access to the equipment consistent with the level of security outlined above.

### **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**

To mitigate the risk of water damage, hosts, network equipment, and communications facilities for the CA system are housed on the second floor of the company's Datacenter. See details in [Section 5.1.1.1](#).

### **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;
- Water-based sprinkler fire suppression in business suites;
- Inergen fire suppression systems (containing inert gas) in the data processing areas, including the Secure Room;
- 24x7x365 onsite operators with fire control console/panel access; and
- Seismic separation between the Secure Room and office space which also serves as an interstitial gap to thwart fire spread.

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.

Server-based computer media containing sensitive materials is stored both within the Secure Room as described in [Section 5.1.2.1](#), 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.

The most sensitive materials, including Cryptographic Modules, tokens, and password copies, are stored within locked mini-vaults and their combinations are under IdenTrust control. Other material is placed in metal boxes that are secured with locks, with keys maintained under IdenTrust's normal 2-person control procedures. As noted above, boxes contain no labels identifying them as belonging to IdenTrust, or as containing sensitive materials; all labeling is designed not to reveal box contents.

Backup copies of PKI materials, including CA, CSA, and CMS Cryptographic Modules and activation materials, are securely stored.

In addition to the restricted access to the Datacenter facility and even tighter restrictions for access to the Secure Room, the safes are also tightly controlled. All removal or additions to the safes are tracked with logs requiring 2 trusted employees to sign them acknowledging such actions.

Shipment of materials to and from the off-site location is conducted via bonded couriers who are employees of the offsite facility. They do not have keys or combinations to the transport boxes and mini safes and have no specific knowledge of box or safe contents.

### **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.

Electronic media is disposed of in the following ways:

- Magnetic-storage media like hard disks and tapes are degaussed using an NSA-approved degaussing system that completely destroys all data and renders hard disks unusable.
- Flash media such as flash drives and solid-state hard drives are physically destroyed using mechanical means.

The Security Office is contacted for assistance in disposing of media and equipment which is no longer being used by the CA, RA, and Repository systems. Such media and equipment are stored at a level of security appropriate to the level of sensitivity of the information contained in the media and equipment until they can be effectively sanitized or destroyed. Key materials, for example, are stored in a safe within the IdenTrust Secure Room, as described in [Section 5.1.2.1](#).

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 TrustID system is backed up at the secure 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.

At least annually, backup tapes are consolidated, and archive media is identified and stored in the offsite storage vault to satisfy IdenTrust's data retention schedule. Components needed to restore the CA, RAs, and Repositories systems are stored in separate areas of the offsite vault, as described in [Section 5.1.6](#).

Only IdenTrust Trusted Role employees who are authorized by the Head of Operations or, if so, designated by the Security Office, may request material from the offsite storage facility. When a request is made to deliver backup material to IdenTrust facilities, the request is made by a Trusted Role employee who has been previously authorized as a requestor and has been identified to the offsite facility. That request is then verified via callback procedures by a second Trusted Role employee who has been similarly authorized and identified to the facility to approve such requests. When Key materials are delivered, they are received and signed for by 2 authorized Trusted Role employees.

## **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, suspension, or Revocation of TrustID Certificates, including access to restricted operations of IdenTrust's CA and RA systems, and Repository are for purposes of this 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 follows a documented procedure for appointing Individuals to Trusted Roles. Trusted Role employees who require Certificate system access are issued unique digital credentials – not user-names and passwords – to authenticate into the Certificate systems. All system activities can be traced back to that Individual. No group accounts, shared roles, or shared digital credentials are permitted.

All IdenTrust employees must follow the IdenTrust Employee Security Handbook which among other security procedures indicates that all employee workstations are automatically locked after 10 minutes of inactivity. This configuration cannot be changed by the employee.

IdenTrust performs a comprehensive user account audit every 3 months and deactivates any user account that is no longer required.

Lockout account access to Certificate systems after no more than 5 failed access attempts is not applicable when the access is authenticated via digital credentials.

Credentials issued to any privileged account or service account to access the secured facility hosting Certificate systems are revoked within one business day upon confirmation that the person is no longer in that role.

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 the CP translate into specific roles for the CA and RA, which include, but are not limited to, CA/RA administrators, system administration personnel, system operators, engineering personnel, and operations managers. For specifics, see the IdenTrust Trusted Roles Matrix Mapping table below.

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](#).

<b>IdenTrust Trusted Roles Matrix Mapping</b>					
<b>TrustID Role</b>	<b>IdenTrust-Internally Defined Roles</b>				
	<b>CA Administrator</b>	<b>LRA / Enterprise RA</b>	<b>System Administrator</b>	<b>Security Officer</b>	<b>RA Administrator</b>
<b>CA Administrator</b>	X				
<b>CA Officer</b>		X			
<b>CA Auditor</b>				X	
<b>CA Operator</b>			X		
<b>CSA Administrator</b>	X				
<b>CSA Auditor</b>				X	
<b>CSA Operator</b>			X		
<b>RA Administrator</b>					X
<b>RA Officer</b>		X			
<b>RA Auditor</b>				X	
<b>RA Operator</b>			X		

IdenTrust Trusted Roles Matrix Mapping					
TrustID Role	IdenTrust-Internally Defined Roles				
	CA Administrator	LRA / Enterprise RA	System Administrator	Security Officer	RA Administrator
RA Administrator					X

The following subsections provide a detailed description of the responsibilities for each Trusted Role.

### 5.2.1.1 Certificate Authority Trusted Roles

#### 5.2.1.1.1 CA Administrator

All Certificates issued under the IdenTrust TrustID Root Certificate, including the Root, are issued under the control of IdenTrust Operations management as operator and CA services provider. The responsibilities for CA functions are carried out by IdenTrust’s employees acting in their Trusted Roles and include administration and operation tasks described in the TrustID CP. The CA Administrator is a Trusted Role. 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.

#### **5.2.1.1.2 CA Agent**

Within IdenTrust, the CA Officer role is performed by an LRA. See [Section 5.2.4](#) for further detail. CA Certificates generation responsibility is also shared by Customer Support Representatives. See [Section 4.1.2.1](#) about IdenTrust secure registration messaging protocol for further detail.

#### **5.2.1.1.3 CA Auditor**

Within IdenTrust, the CA Auditor functions are performed by the IdenTrust Security Office with oversight by the IdenTrust Security Officer. See [Section 5.2.1.5.3](#) for details.

#### **5.2.1.1.4 CA Operator**

Within IdenTrust, the CA Operator functions are divided between the CA Administrator and the System Administrator. See [Section 5.2.1.5.1](#) for details on CA Operator's tasks performed by the System Administrator.

#### **5.2.1.1.5 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, 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.

All such controls are audited annually by a third party auditor as part of the WebTrust Program for Certification Authorities, in compliance with the *ISO 21188 Public Key Policy and Practices Framework* standard.

#### **5.2.1.1.6 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.

All such controls are audited annually by a third party auditor as part of the WebTrust Program for Certification Authorities, in compliance with *the ISO 21188 Public Key Policy and Practices Framework standard*.

### **5.2.1.2 Certificate Status Authority (CSA) Roles**

#### **5.2.1.2.1 CSA Administrator**

Within IdenTrust, CA Administrators also carry out the responsibilities of the CSA Administrator. The CSA Administrator responsibilities and operating procedures performed by IdenTrust CA Administrators, as they relate to CSA Operation, are as follows:

- Installation, configuration, and maintenance of the CSA software;
- Generating and backing up CSA Keys (performed under 2-person control);
- Management of CSA Key and Certificate lifecycle, including renewal of OSCP Responder Certificates (performed under 2-person control);
- Establishing and maintaining system accounts and configuring audit parameters; and
- Operation of the CSA equipment.

#### **5.2.1.2.2 CSA Agent**

Within IdenTrust the CA Agent and the CSA Agent are equivalent and interchangeable. See [Section 5.2.1.1.2 CA Agent](#).

#### **5.2.1.2.3 CSA Operator**

Within IdenTrust, the CSA Operator functions are divided between the CSA Administrator and the System Administrator. See [Section 5.2.1.5.1 System Administrator](#) for details on CSA Operator's tasks performed by the System Administrator.

#### **5.2.1.2.4 CSA Auditor**

Within IdenTrust, the CSA Auditor functions are performed by the IdenTrust Security Office with oversight by the IdenTrust Security Officer. See [Section 5.2.1.5.3 Security Officer](#) for details.

#### **5.2.1.2.5 CA Operator**

Within IdenTrust the CA Operator and the CSA Operator are equivalent and interchangeable.

### **5.2.1.3 Card Management System (“CMS”) Roles**

CMS services are offered to selected enterprise customers and the CMS roles typically handle these functions: Card issuance, Key Generation and storage, Certificate management, PIN management, card lifecycle management, user management, integration with PKI components, reporting and auditing, policy enforcement and remote card management. These functions are performed by CMS Operators at the enterprise customer system environment; therefore, no CMS Trusted Roles are required in this CPS.

#### **5.2.1.4 Registration Authority Roles**

The RAs operating under the TrustID CP, and this CPS are subject to all applicable terms and conditions therein. If a CA delegates Identity Proofing responsibility to an RA, then the RA must be bound to comply with the provisions of the TrustID CP and CPS under the contract between the CA and RA in which such delegation is made.

#### **5.2.1.4.1 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. See [Section 5.2.1.4.1](#) for details on RA Administrator's tasks performed by the System Administrator.

#### **5.2.1.4.2 RA Officer**

The RA Officer of an RA is a Trusted Role with duties for the RA that are the same as those of the LRA for IdenTrust. See [Section 5.2.1.4.4](#) for further detail.

Within IdenTrust, the RA Officer role is performed by an LRA.

#### **5.2.1.4.3 RA Auditor**

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

- Review, maintenance, and archiving of audit logs; and
- Performance or oversight of internal compliance audits to ensure that the RA is operating in accordance with this CPS.

Within IdenTrust, the RA Auditor functions are performed by the Security Officer. See [Section 5.2.1.5.3](#) for details.

#### **5.2.1.4.4 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 system;
- Receiving and distributing Certificates;
- Authenticating identity upon request for Revocation and executing Revocation;
- Authenticating identity upon request for suspension, executing suspension, and unsuspension;
- 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).

#### **5.2.1.4.5 Trusted Agent**

A Trusted Agent is an entity external to IdenTrust, acts as representative of the Sponsoring Organization, and that is obligated by contract, this CPS, and the TrustID CP to perform Identity Proofing in a trustworthy manner.

A Trusted Agent is confirmed through the Issuance of a business Certificate stored in a hardware Cryptographic Module that validates to a FIPS level equal to or higher than the Certificates for which the Trusted Agent will perform Identity Proofing. IdenTrust or the RA may provide software such as web pages, forms, instructions, and other resources to facilitate the work of Trusted Agents, but they do not have privileged access to IdenTrust's or the RA's systems used to issue and revoke Certificates.

The Trusted Agent has the following duties:

- Performing in-person or remote identification of Applicants/PKI Sponsors in accordance with guidelines specified in this CPS;
- Securely communicating requests to and responses from the LRA or Enterprise RA;
- Collecting copies of identification documents and declarations of identity; and
- Delivering end-user support to Applicants/PKI Sponsors and Subscribers (distribute cryptographic hardware, troubleshooting, assist with Revocation)

A Trusted Agent need not be a Trusted Role and as such, some of the requirements related to background checks below do not apply.

### **5.2.1.5 Other Roles**

The Trusted Role titles are defined in governing CP documents; however, the titles of Individuals within IdenTrust or an External RA who perform the duties associated with the CP-defined Trusted Roles do not align on a one-to-one basis. Additionally, there are other internally defined roles that are required to support the CA and/or RA operation. The following subsections describe other roles that have been defined as key to the IdenTrust CA and/or RA operation and fulfill the duties of the Trusted Roles as defined in by governing CP documents. The IdenTrust Trusted Role Matrix provided in [Section 5.2.1](#) provides a cross reference mapping of CP-defined Trusted Roles to internal IdenTrust Trusted Roles Matrix.

#### **5.2.1.5.1 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.

#### **5.2.1.5.2 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.

### 5.2.1.5.3 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 CPS.

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

- Requests to and responses from the CA 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 and Code Signing Certificates, performing quarterly self-audits to monitor Certificate Issuance quality described in [Section 8](#), [Section 8.5.1](#), [Section 8.6.1](#), 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 CPS.

### 5.2.1.5.4 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 or suspension processes; and
- Generating the External Root CA Certificate and Subordinate CA Certificate, re-keying, and Revocation (performed under 2-person control).

### 5.2.1.5.5 PKI Consultant

PKI Consultants are IdenTrust employees who coordinate the processes needed to securely onboard new CAs, RAs, and LRAs. PKI Consultant responsibilities include:

- Installation and configuration of RA software connecting to CA system;
- Assistance with Identity Proofing processes to be used by IdenTrust, RAs, and LRAs;
- Assistance with distributing Cryptographic Modules containing RA System Keys; and
- Configuration of RA System access rights to CA-provided services.

### 5.2.1.5.6 PKI Sponsor

A PKI Sponsor represents a Sponsoring Organization that may be named in the Certificate's Subject extension. The PKI Sponsor works with the LRA, Enterprise RA, or Trusted Agent to register appropriate information in accordance with [Section 4.1](#). The PKI Sponsor is responsible for the Electronic Device and has the duties of a Subscriber, including but not limited to protecting the Private Key of the Electronic Device.

A PKI Sponsor need not be a Trusted Role and as such, some of the requirements related to background checks below do not apply.

### 5.2.1.5.7 Operations Manager

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.

### 5.2.1.5.8 Enterprise RA

Enterprise RAs function as a limited LRA contractually and have the following responsibilities:

- Verifying identity via review and approval of documents provided by the PKI Sponsor;
- Entering PKI Sponsor and Subscriber information, verifying correctness, and approving requests;
- Securely communicating requests to and responses from the RA/CA system;
- Receiving, approving, and distributing Certificates; and
- Authenticating identity upon request for Revocation and executing Revocation.

IdenTrust retains all responsibilities of the RA as specified as the contract between IdenTrust and the institution using the Enterprise RAs.

## 5.2.2 Number of Persons Required per Task

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 5.1.2.1](#) 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 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 system;

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

Roles requiring separation of duties include (but are not limited to):

- **CA/CSA/CMS Administrator.** No person participating as IdenTrust CA/CSA/CMS Administrator will assume the role of Security Officer, LRA, Network Engineer, or Operations Manager.
- **Local Registration Authority.** An LRA may not assume an Operations Manager, CA/CSA/CMS Administrator, RA Administrator, System Administrator, Network Engineer, Security Officer, or management oversight role (Risk Management, Operations Management, Human Resources, or Executive Management).
- **RA Administrator** (whether an IdenTrust Internal RA Administrator or an External RA Administrator). An RA Administrator may not assume the Operations Manager, LRA, Network Engineer, or Security Officer role.
- **System Administrator.** A System Administrator may not assume the Security Officer, LRA or Operations Manager role.
- **Network Engineer.** The Network Engineer may not assume the Security Officer, LRA, CA/CSA/CMS Administrator, or Operations Manager role.
- **Security Officer.** The Security Officer may not serve in any other trusted role (e.g. the roles of CA/CSA/CMS Administrator, LRA, RA Administrator, Systems Administrator, or Network Engineer).
- **Help Desk Representative.** Help Desk Representatives may not serve in the role of CA/CSA/CMS Administrator, RA Administrator, System Administrator, or Network Engineer.
- **PKI Consultant.** PKI Consultants may not serve in the roles of CA/CSA/CMS Administrators, System



Administrators, Network Administrators, and Security Officers.

- **Operations Manager.** The Operations Manager may not serve as CA/CSA/CMS Administrator, Systems Administrator, LRA, or Network Engineer.
- **Software Engineer.** Software Engineer may not assume any other roles
- **Development Operations (DevOps).** Development Operations may not assume the LRA, Security Officer, Help Desk Representatives, Operations Manager or Software Engineer role.

## 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 the TrustID CP.

Contractor personnel employed to perform functions for IdenTrust pertaining to the TrustID CP and this CPS meet applicable requirements set forth in the CP, CPS, and System Security Plan (SSP).

IdenTrust takes appropriate administrative and disciplinary actions against personnel who have performed actions involving IdenTrust or its Repository not authorized in the TrustID CP and this CPS.

The following sections outline these controls.

### 5.3.1 Qualifications, Experience, and Clearance Requirements

Personnel who administer or operate components of the CA, CSA, and IdenTrust RA systems and RA systems, including LRAs (with the exception of Enterprise RAs explained below in [Section 5.3.3.3](#)), 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, this CPS, and the TrustID CP 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**

All individuals responsible for carrying out information verification responsibilities receive skill-enhancing training. This training encompasses fundamental Public Key Infrastructure knowledge, authentication and vetting policies and protocols (including the CA's CP and/or CPS), typical risks associated with the information verification process (such as phishing and other social engineering methods), and adherence to CA/B Forum BRs.

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 Validation Specialists to undertake CA/B Forum BR tasks, IdenTrust confirms the possession of essential skills by each specialist.

IdenTrust requires that all Validation Specialists successfully complete an assessment conducted by the internal compliance team. This assessment evaluates their understanding of the information verification requisites outlined in the CA/B Forum BRs.

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

#### **5.3.3.1 CA/CSA Administrator**

- Key Pair Generation and Certificate Issuance, re-keying and Revocation for Root CA, Issuing CAs, External CAs, and CSAs;
- Configuration and posting of Certificates and CRLs;
- Daily maintenance and other CA-, CSA-related administrative functions; and
- Initializing CA and CSA hardware.

#### **5.3.3.2 LRA**

- Verifying identity, either through personal contact or through Trusted Agents;
- Understanding common threats to the information verification process (including phishing and other social engineering tactics);
- Entry of Applicant/PKI Sponsors information and verifying correctness;
- Securely handling requests to and responses from CAs;
- Executing the Certificate Revocation process;
- Completing the Certificate Issuance process; and
- For Server Certificates, understanding the requirements in the TrustID CP for Identity Proofing of Server Certificate Issuance and passing an examination administered by IdenTrust or the RA covering those requirements.

#### **5.3.3.3 Enterprise RA**

- Verifying Certificate requests, employment, and FQDN(s);
- Understanding common threats to the information verification process (including phishing and other social engineering tactics);
- Entering of Applicant/PKI Sponsors information and verifying correctness;
- Securely handling requests to and responses from CAs;
- Executing the Certificate Revocation process;
- Completing the Certificate Issuance process; and
- Understanding the requirements in the TrustID CP for Identity Proofing of Certificate Issuance and passing IdenTrust training covering those requirements.

#### **5.3.3.4 System Administrator**

- Operating systems and software applications used within the PKI systems;
- Backup applications and procedures;
- Use of database tools including reporting and maintenance;
- Restriction for privileged system use; and
- Generation of audit data.

### 5.3.3.5 Network Engineer

- Network architecture and equipment used in the PKI;
- Proper and secure configuration and switching for the network;
- Intrusion detection monitoring; and
- Requirements for securing network transmissions.

### 5.3.3.6 Security Officer

- Security risk assessment and analysis;
- Security policies and guidelines;
- Computer attack trends, security threats, and vulnerabilities;
- Physical security and physical access controls;
- Networks, distributed systems trust relationships, PKI, and cryptosystems;
- Firewalls and other network security devices;
- Event logging and auditing; and
- Incident response and contingency planning.

### 5.3.3.7 Customer Support Representative

- End user systems;
- Proper and secure handling of sensitive customer information; and
- Use of trouble-tracking software.

### 5.3.3.8 Operations and Software Applications Used Within the PKI System;

- Network architecture; and
- Audit and risk management oversight.

## 5.3.4 Retraining Frequency and Requirements

Any significant change to the CA and RA systems requires that personnel receive additional training. Through 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 the CP and CPS under which they are operating, and a full review of all applicable policies and procedures.

Documentation identifying all personnel who received training and the level of training completed is maintained.

RAs are obligated by contract, this CPS, and the TrustID CP to retrain its personnel and maintain a record of the training provided.

## 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

Failure of any employee or agent of IdenTrust or an RA to comply with the provisions of the TrustID CP, this 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**

Independent contractors who are assigned to perform Trusted Roles are subject to the duties and all requirements of the TrustID CP and this CPS, including those described elsewhere in [Section 5.3](#). Independent contractors are subject to sanctions stated in [Section 5.3.6](#) for unauthorized actions or failure to comply with the provisions of the TrustID CP and this CPS.

### **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 the TrustID CP, relevant portions of this 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, the TrustID CP, this 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, the TrustID CP, and this 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 records events related to the security of their Certificate Systems, Certificate Management 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 CA/B Forum BRs.

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 CA/B Forum BRs and the IdenTrust 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:
    - a) an identifier that uniquely identifies the Network Perspective used;
    - b) the attempted domain name and/or IP address; and
    - c) 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. Successful and unsuccessful PKI system access attempts;
  2. PKI and security system actions performed;
  3. Security profile changes;
  4. Installation, update and removal of software on a Certificate System;
  5. System crashes, hardware failures, and other anomalies;
  6. Relevant router and firewall activities (as described in Section 5.4.1.1); and
  7. Entries to and exits from the CA facility.
4. 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.
5. Subscriber Certificate lifecycle management events, including:
  1. Certificate requests, renewal, and re-key requests, and revocation;
  2. All verification activities stipulated in the CA/B Forum BRs and the IdenTrust 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](#)).
6. Security events, including:
  1. Successful and unsuccessful PKI system access attempts;
  2. PKI and security system actions performed;
  3. Security profile changes;
  4. Installation, update and removal of software on a Certificate System;
  5. System crashes, hardware failures, and other anomalies;
  6. Firewall and router activities; and
  7. 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 record all significant events related to the operations of the equipment. Events recorded include those that occur to the routers, firewalls, and other network equipment; at each host; within applications and databases; and at all physical security checkpoints.

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

RAs are obligated by contract, this CPS, and the TrustID CP 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).

<b>TrustID Auditable Events</b>			
<b>Auditable Event</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>SECURITY AUDIT</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>Any changes to the audit parameters, e.g., audit frequency, type of event audited</b> - The operating system and applications automatically record modifications made to audit parameters; including date and time of modification, type of event, success or failure indication, and identification of user making the modification.	X	X	X
<b>Any attempt to delete or modify the audit logs</b> – The operating system automatically records all attempted modifications made to security audit configurations and files, including date and time of modification, type of event, success or failure indication, and identification of user making the modification.	X	X	X
<b>Relevant router and firewall activities</b> – As described in <a href="#">Section 5.4.4.1</a> . below			
<b>Obtaining a third party time-stamp</b>	N/A	N/A	N/A
<b>IDENTITY AND AUTHENTICATION</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>Successful and unsuccessful attempts to assume a role</b> – The operating system and applications automatically record: the date and time of attempted login, username asserted at the time of attempted login, and success or failure indication, are automatically logged.	X	X	X
<b>The value of maximum authentication attempts is changed</b> – The operating system logging facility automatically logs date and time, type of event, and identification of the user	X	X	X

<b>TrustID Auditable Events</b>			
<b>Auditable Event</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
making modification(s). Changes in configuration files, security profiles, and administrator privileges are logged through a combination of automatic and manual logging. All configuration changes are manually logged through change management procedures.			
<b>Maximum number of authentication attempts occurring during user login</b> – Date and time of attempted login, username asserted at the time of attempted login, and failures are recorded automatically by the operating system and application audit logs.	X	X	X
<b>An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts</b> – The date and time of the event and identification of the account holder and administrator are logged automatically by the operating system.	X	X	X
<b>An administrator changes the type of authenticator, e.g., from a password to a biometric</b> – Date and time, type of event, and identification of the user making the modification(s) are logged automatically by the operating system and manually through change management procedures.	X	X	X
Changes in configuration files, security profiles, and administrator privileges are logged through a combination of operating system and manual change management procedures.	X	X	X
<b>LOCAL DATA ENTRY</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>All security-relevant data that is entered in the system</b> – The system records the identity of the local operator performing local data entry so that the accepted data can be associated with the operator in the audit log.	X	X	X
<b>REMOTE DATA ENTRY</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>All security-relevant messages that are received by the system</b> – Date and time, Digital Signature/authentication mechanism, and message are automatically logged by the application.	X	X	X
<b>DATA EXPORT AND OUTPUT</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>All successful and unsuccessful requests for confidential and security-relevant information</b> – Date and time of attempted access, username or identity asserted at the time of the attempt, and record of success or failure, are logged through a combination of automatic and manual logging. Since such items may include unauthorized attempts to obtain information, manual logging by the Security Office also collects the name of the person reporting the event and the resolution.	X	X	X
<b>KEY GENERATION</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>Whenever a CA generates a Key</b> (not mandatory for a single session or one-time use symmetric Keys) – The CA system automatically records all significant events related to CA operations, including Key Generation and Certificate signing. Additionally, manual and audiovisual records of CA and CSA Key Generation are created. RA Key and Certificate generation events are automatically recorded by the CA system.	X	X	-
<b>PRIVATE KEY LOAD AND STORAGE</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>The loading of Component Private Keys</b> – A manual log of all physical access to production CA and CSA Cryptographic Modules is maintained by IdenTrust, and the log records each action is taken, the date and time the action was taken, and the name of the person who performed each action. A separate record of authorization to access Cryptographic Modules is also maintained that specifies the date, time, reason for access, and name of the authorizing person.	X	X	N/A

<b>TrustID Auditable Events</b>			
<b>Auditable Event</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>All access to Certificate Subject Private Keys retained within the CA for Key recovery purposes</b> – Date and time, messages between the CA and the requesting component, and indicator of success or failure are automatically logged.	X	N/A	N/A
<b>TRUSTED PUBLIC KEY ENTRY, DELETION, AND STORAGE</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>All changes to the trusted Public Keys, including additions and deletions,</b> are automatically logged through the applications and manually through IdenTrust’s change management process and access authorization forms.	X	X	X
<b>SECRET KEY STORAGE</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>The manual entry of secret Keys used for authentication</b> – Use of secret Keys (PED Keys) for access to the CAs’ and CSAs’ Cryptographic Modules is recorded manually at the time of cryptographic Key use. The log records the action(s) taken, the date and time the action were taken, and the name of the person who performed the action. A separate record of authorization to access Cryptographic Modules is also maintained that specifies the date, time, reason for access, and name(s) of the authorizing person(s).	X	X	N/A
<b>PRIVATE AND SECRET KEY EXPORT</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>The export of private and secret Keys (Keys used for a single session or message are excluded)</b> – Private and secret Key export involving the CA’s Cryptographic Modules take place in accordance with the principles of Separation of Duties/Multi-party Control stated in <a href="#">Section 5.2.4</a> . At the time of export, a manual log records the action that is taken, the date and time the action was taken, and the name(s) of the person(s) who performed the action. Separate records of access to Cryptographic Modules are also maintained that specify the date, time, reason for access, and name of the authorizing person(s).	X	X	N/A
<b>CERTIFICATE REGISTRATION</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>All Certificate requests</b> – Date and time of the request, type of event, and request information are automatically logged by the application. This includes Issuance, renewal, and re-key requests as well as sender/requester DN, Certificate serial number, initial application, method of the request (online, in-person, remote), source of verification, name of the document presented for Identity Proofing, all fields verified in the application, Certificate common name, new Validity Period dates, date and time of response and success or failure indication are automatically logged by the application, and all associated error messages and codes. Manual interactions with Participants such as via telephone call or in-person inquiries and results of verification calls will be logged either manually or in a computer-based recording/tracking system and include date/time, description of the interaction, and identity provided.	X	N/A	X
<b>CERTIFICATE REVOCATION</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>All Certificate Revocation requests</b> – Date and time of Revocation request, sender/requester DN, Certificate serial number, Subject DN of Certificate to revoke, End Entity’s common name, Revocation reason, date and time of response, and success or failure indication are automatically logged by the application; manual interactions with requestors such as via telephone call or in-person inquiries and requests for Revocation are logged manually or in a computer-based recording/tracking system. The date/time, description of interaction, and identity provided are also recorded.	X	N/A	X
<b>CERTIFICATE STATUS CHANGE APPROVAL</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>



<b>TrustID Auditable Events</b>			
<b>Auditable Event</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>The approval or rejection of a Certificate status change request</b> – Identity of the equipment operator who initiated the request, message contents, message source, destination, and success or failure indication are automatically logged by the application as well as actions taken on CAA Records to process Certificate Request validations.	X	X	X
<b>COMPONENT CONFIGURATION</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>Any security-relevant changes to the configuration of a component</b> – Date and time of modification, name of modifier, description of the modification, build information (i.e., size, version number) of any modified files, and the reason for modification are logged during change management processes.	X	X	X
<b>ACCOUNT ADMINISTRATION</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>Roles and users are added or deleted</b> – Date and time, type of event, and identification of the user making modification(s) are logged automatically and manually. Changed roles are logged through a combination of automatic and manual logging. All changes are manually logged through change management procedures. Change management records capture the date and time and type of change, the reason for the change of role, and authorization and approval records.	X	X	-
<b>The access control privileges of a user account or a role are modified</b> – Date and time, type of event, and identification of user making modification are logged automatically and manually. Changes in configuration files, security profiles, and administrator privileges are logged through a combination of automatic and manual logging. All changes are manually logged through change management procedures. Change management records capture the date and time and type of change, the reason for modification, and authorization and approval records.	X	X	-
<b>CERTIFICATE PROFILE MANAGEMENT</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>All changes to the Certificate Profile</b> – Change management records capture date and time and type of change, the reason for modification, and authorization and approval records.	X	N/A	N/A
<b>REVOCAION PROFILE MANAGEMENT</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>All changes to the Revocation profile</b> – Change management records capture date and time and type of change, the reason for modification, and authorization and approval records.	X	N/A	N/A
<b>CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>All changes to the Certificate Revocation list profile</b> – Change management records capture date and time and type of change, the reason for modification, and authorization and approval records.	X	N/A	N/A
<b>MISCELLANEOUS</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>Appointment of an Individual to a Trusted Role</b> – Date of the appointment, type of Trusted Role, name of the appointee, and authorizing signature are manually logged.	X	X	X
<b>Designation of personnel for multi-party control</b> – Date of the appointment, name of the appointee, and authorizing signature are manually logged.	X	-	N/A
<b>Installation of the Operating System</b> – Date and time of server installation, name of the installer, and details of the installation process are manually recorded during installation. The automatic security auditing capabilities of the underlying operating system hosting the	X	X	X

TrustID Auditable Events			
Auditable Event	CA	CSA	RA
software are enabled during installation. All changes are also manually logged through change management procedures.			
<b>Installation of the PKI application</b> – Date and time of installation, name of the installer, and details of the installation process are recorded during installation. All changes are also logged through change management procedures.	X	X	X
<b>Installation of hardware Cryptographic Modules</b> – A manual list of hardware Cryptographic Modules is maintained, and the list records action taken, date and time action were taken, and the name of the person who performed the action.	X	X	X
<b>Removal of hardware Cryptographic Modules</b> – A manual list of hardware Cryptographic Modules is maintained, and the list records action taken, date and time action were taken, and the name of the person who performed the action.	X	X	X
<b>Destruction of Cryptographic Modules</b> – A manual list of Cryptographic Modules is maintained, and the list records action taken, date and time action were taken, and the name of the person who performed the action.	X	X	X
<b>System Startup</b> – Date and time of system startup are automatically logged in the system’s event log.	X	X	X
<b>Logon attempts to PKI Applications</b> – For CA, RA, and CSA application access – the date and time of the event, type of event, the identity of the user accessing the system, and success or failure indication are automatically logged by the application.	X	X	X
<b>Receipt of hardware / software</b> – Kept manually in a database that records the hardware and software possessed, licensed, or owned.	X	X	X
<b>Attempts to set passwords</b> – Date and time, the identity of the user, and success or failure indication of an attempt to set password are kept automatically by the operating system/application or manually in a password change log.	X	X	X
<b>Attempts to modify passwords</b> – Date and time, the identity of the user, and success or failure indication of an attempt to modify password are kept by the operating system/application or manually in a password change log.	X	X	X
<b>Back up of the internal CA database</b> – Date and time of the backup event and location of backup are kept manually in a backup log.	X	-	-
<b>Restoration from a backup of the internal CA database</b> – Dates and times of restoration tests are kept in a disaster recovery log.	X	-	-
<b>File manipulation (e.g., creation, renaming, moving)</b> – for the operating system and related files that do not change with system operation, the file system records the identity of the local operator who created or last modified the file so that the creation, renaming or moving of files can be associated with the operator. This is kept automatically by the operating system audit and logging facility.	X	-	-
<b>Posting of any material to a Repository</b> – Date and time of posting, transaction identifier, and success or failure indication are automatically logged by the application. For CRL and OCSP generation and publication to directory – date and time of generation, DN of IdenTrust, and success or failure of publication of CRL and OCSP entry are automatically logged by the application.	X	-	-
<b>Access to the internal CA database</b> – Date and time of login, username asserted at the time of attempted login, and success or failure indication, are automatically logged by the database audit log.	X	-	-

<b>TrustID Auditable Events</b>			
<b>Auditable Event</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>All Certificate compromise notification requests</b> – Date and time of notification, the identity of the person making the notification, identification of entity compromised, and a description of the compromise are logged manually by the person who receives the notification (e.g., Customer Support, RA Operators, etc.) and by RA/RA Operators’ system processing logs.	X	N/A	X
<b>Loading Cryptographic Modules with Certificates</b> – A manual log of all physical access to production CA and CSA tokens is maintained, and the log records action taken (including transferring Keys to or from and backing up the tokens), date and time action was taken and the name of the person who performed the action. A separate record of authorization to access tokens is also maintained that specifies the date, time, reason for access, and name of the authorizing person.	X	X	N/A
<b>Shipment of Cryptographic Modules</b> – Receipt, servicing (e.g., Keying, or other cryptologic manipulations), and shipping of modules are manually recorded for CA, CSA, and RA production tokens. Recording contains information regarding action taken, (e.g., return, receipt), date and time action was taken, name of person performing action, and reason for action.	X	X	N/A
<b>Zeroizing Cryptographic Modules</b> – A manual list of modules is maintained, and the list records action taken, date and time action were taken, name of the person who performed the action, name, and role of the person authorizing the action.	X	X	N/A
<b>Re-key of the CA</b> – CA, CSA, and RA systems automatically record all significant events related to their respective operations, including Key Generation for re-keying. Additionally, manual and audiovisual records of CA Key Generation are created. RA re-keying and Certificate generation events are also automatically recorded by the CA system.	X	X	N/A
<b>CONFIGURATION CHANGES TO THE PKI SERVERS INVOLVING:</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>Hardware</b> – All changes are manually logged through change management procedures.	X	X	X
<b>Software</b> – All changes are manually logged through change management procedures.	X	X	X
<b>Operating System</b> – All changes are manually logged through change management procedures.	X	X	X
<b>Patches</b> – All changes are manually logged through change management procedures.	X	X	X
<b>Security Profiles</b> – All changes are manually logged through change management procedures.	X	X	X
<b>PHYSICAL ACCESS / SITE SECURITY</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>
<b>Personnel Access to room housing component</b> – A manual recording of physical access to the CA facility Secure Rooms is maintained through physical logs that include recording the date(s) and time(s) of arrival and departure, the person(s) accessing the Secure Room, and reason(s) for access.	X	-	-
<b>Physical access to System Components</b> – Logged through a combination of automatic and manual logs based upon the type of component and type of access.	X	X	-
<b>Known or suspected violations of physical security</b> – For any known or suspected violations of physical security, date/time, description of the suspected event, name of the person reporting the event, and resolution are manually logged by the Security Office.	X	X	X
<b>ANOMALIES</b>	<b>CA</b>	<b>CSA</b>	<b>RA</b>

TrustID Auditable Events			
Auditable Event	CA	CSA	RA
<b>Software error conditions</b> – Date and time of the event, and description of the event are automatically logged by the application reporting the event or by the operating system.	X	X	X
<b>Software check integrity failures</b> – Date and time of the event, and description of the event are automatically logged by the application reporting the event or by the operating system.	X	X	X
<b>Receipt of improper messages</b> – Date and time of the event, and description of the event are automatically logged by the application reporting the event or by the operating system.	X	X	X
<b>Misrouted messages</b> – Date and time of the event and description of the event are automatically logged by the application reporting the event or by the operating system.	X	X	X
<b>Network attacks (suspected or confirmed)</b> – Date and time, description of the suspected event, name of the person reporting the event, and resolution are manually logged by a Security Officer.	X	X	X
<b>Equipment failure</b> – Date/time, description of the suspected event, name of the person reporting the event, and resolution are manually logged by a Security Officer.	X	X	-
<b>Electrical power outages</b> – Date/time, description of the suspected event, name of the person reporting the event, and resolution are manually logged by a Security Officer.	X	X	-
<b>Uninterruptible Power Supply (UPS) failure</b> – Date/time, description of the suspected event, name of the person reporting the event, and resolution are manually logged by a Security Officer.	X	X	-
<b>Obvious and significant network service or access failures</b> – Date/time, description of the suspected event, name of the person reporting the event, and resolution are manually logged by a Security Officer.	X	X	-
<b>Violations of Certificate Policy</b> – Date/time, description of the suspected event, name of the person reporting the event, and resolution are manually logged by a Security Officer.	X	X	X
<b>Violations of Certification Practice Statement</b> – Date/time, description of the suspected event, name of the person reporting the event, and resolution are manually logged by a Security Officer.	X	X	X
<b>Resetting Operating System clock</b> – Date/time, description of the suspected event, name of the person is automatically logged by the operating systems logging facility.	X	X	X

#### 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.

#### 5.4.1.2 Types of Events Recorded for Timestamp Authorities

The Timestamp Authority must log the following information and make these records available to its Qualified Auditor as proof of the Timestamp Authority’s compliance with the CS BRs:

1. Physical or remote access to a timestamp server, including the time of the access and the identity of the individual accessing the server,
2. History of the timestamp server configuration,
3. Any attempt to delete or modify timestamp logs,
4. Security events, including:
  1. Successful and unsuccessful Timestamp Authority access attempts;
  2. Timestamp Authority server actions performed;
  3. Security profile changes;
  4. System crashes and other anomalies; and
  5. Firewall and router activities;
5. Revocation of a timestamp certificate,
6. Major changes to the timestamp server's time, and
7. System startup and shutdown.

#### **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, this CPS, and the TrustID CP 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:
  - a. the destruction of the CA Private Key; or
  - b. 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 [Section 4.1.2.1](#) 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, this CPS, and the TrustID CP 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, this CPS, and the TrustID CP 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**

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, this CPS, and the TrustID CP 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, this CPS, and the TrustID CP 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 CA systems, 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 (i) within one week of receiving a request from the CA/B Forum, (ii) after any system or network changes that the CA determines are significant, and (iii) 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.

IdenTrust does one of the following within 96 hours of the discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process:

- Remediate the Critical Vulnerability;
- If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to (1) vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0) and (2) systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; or
- Document the factual basis for the CA's determination that the vulnerability does not require remediation because (a) the CA disagrees with the NVD rating, (b) the identification is a false positive, (c) the exploit of the vulnerability is prevented by compensating controls or an absence of threats; or (d) other similar reasons.
- Apply recommended security patches to Certificate Systems within six (6) months of the security patch's availability, unless the CA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

RAs are obligated by contract, this CPS, and the TrustID CP to implement controls that allow them to perform routine self-assessments.



## 5.5 RECORDS ARCHIVAL

### 5.5.1 Types of Records Archived

IdenTrust retains and archives all data through the life of TrustID PKI Certificates. Archive records are maintained locally for at least 3 months and archived offsite for at least 10 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;
- Certificate Policy;
- Certificate Practices Statement;
- 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 CPS, and the TrustID CP 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**

Archive records are maintained locally for at least 3 months and archived offsite for at least 10 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 CPS, and the TrustID CP to implement controls that allow them to retain records and copies of the application that can read those files for 10 years and 6 months.

### **5.5.3 Protection of Archive**

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, this CPS, and the TrustID CP 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**

IdenTrust does not have a backup archival facility because 3 copies of each archive log are maintained in separate locations. 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 Datacenter or Secure Room.

### **5.5.5 Requirements for Times-Stamping of Records**

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**

Upon proper request, IdenTrust will create, package, and send copies of archived information. Archived information is provided and verified using the formats and media explained in [Section 5.5.2](#). Access to archive data is restricted to authorized personnel in accordance with [Section 9.3](#) and [Section 9.4](#).

Archived data is retrieved from secure storage using IdenTrust's procedures for accessing archived material. Requested archived material is identified by inventory number, which was recorded for the materials when they were originally placed in the locked storage containers for archival. The request procedure requires 2 IdenTrust Trusted Role employees – a requestor and an approver – to complete the request for retrieval from the archive storage facility. Material is delivered to a predefined destination by a bonded courier employed by the storage facility. Identification of the receiving party is checked, a receipt is signed by the receiving party, and physical custody of the archive material is transferred back to IdenTrust. The materials are stored in the Secure Room until they can be reviewed and/or copied in a forensically sound manner for the requestor. The materials are then returned to the archive storage facility.

RAs are obligated by contract, this CPS, and the TrustID CP to implement procedures around the creation, verification, packaging, transmission, and storage of archive information. These procedures shall be provided to IdenTrust.

## **5.6 KEY CHANGEOVER**

IdenTrust provides for the extension and/or continuation of its self-signed root Certificates before their expiration through a Key rollover process involving signing the new Public Key with the old Private Key, and vice versa. Upon Key changeover, only the new Key is used for Certificate signing purposes. The older Valid Certificate remains available to verify old signatures until all of the Certificates signed using the associated Private Key have also expired. IdenTrust CA's signing Key has a Validity Period as described in [Section 6.3.2](#).

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.

## 5.7.2 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 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 Datacenter 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 CPS;
- Distribute its new CA Certificate using the reliable out-of-band means allowed by this CPS;
- Issue new CA Certificates to Subordinate CAs in accordance with this 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.

### 5.7.3.1 Compromise of Issuing CA or External CA Private Key

In the event that any Issuing CA or External CA Private Key has been or is suspected to have been compromised, the highest-ranking IdenTrust Operations Manager available will convene a meeting of management representatives to assess the situation and take appropriate action. IdenTrust Trusted Role personnel will implement the procedural steps and tasks that have been outlined for Private Key compromise in the security incident response plan, including:

- Quantifying the scope, extent, and effects of the compromise;
- Revoking the Subordinate CA Certificate and ensuring that it is promptly included in a published CRL;
- Explaining the situation to all employees and notifying all interested parties (either by Certificate-based communication, via telephone call, or written letter sent by courier service). Recipients of this communication will include:
  - The IdenTrust PMA;
  - All RAs, Enterprise RAs, and LRAs; and
  - All Subscribers.

As soon as possible, the IdenTrust PMA will investigate the incident, and if necessary, will forensically record and analyze the causes of the compromise.

A report will be prepared and delivered to the IdenTrust PMA concerning the causes of the compromise and what measures have been or will be taken to prevent a future recurrence.

After the factors leading up to the Private Key compromise can be satisfactorily addressed, IdenTrust will generate a new Key Pair and Subordinate CA Certificate with a new DN, in accordance with CA Key Generation ceremony procedures. IdenTrust will issue new Subscriber, Enterprise RA, and LRA Certificates; upon completing Identity Proofing processes outlined in [Section 3.2](#), signing them with the new Subordinate CA Certificate; and will issue a new, blank CRL.

Any .p7c, .cer, or other PKCS#7 files that contain or refer to the Certificate, Public Key, or corresponding Private Key will be replaced with new files to reflect that a new CA Certificate has been issued. All appropriate HTTP pointers will be updated to ensure proper path construction and validation.

### 5.7.3.2 Compromise of the Root Private Key

When Revocation of the Root CA Certificate is required, in addition to the foregoing procedures, IdenTrust will immediately notify all browsers that have that specified root. A new Root CA Key Pair, self-signed Root CA Certificate with new DN, and CRL will be generated in a Key Generation ceremony consistent with the procedures of [Section 6.1.1](#).

RAs are required by contract to facilitate the replacement of the revoked Root CA Certificate with the new Root CA Certificate in Subscriber and Relying Party applications. IdenTrust will also notify all Participants and browsers

that the new Root CA Certificate is available in a secure area of the IdenTrust website (HTTPS) where it can be downloaded through a server-side encrypted session.

Cross-certified CAs will be asked to submit new Certificate requests.

IdenTrust will notify all interested parties via email, telephone call, or written letter sent by courier service. In addition, IdenTrust will set up an informational secure site (<https://>) that establishes a server-side session.

### **5.7.3.3 Compromise of the CSA Key**

OCSP Responder Certificates are issued with the 'nocheck' extension (id-pkix-ocsp-nocheck) specifying that OCSP Responder Certificates are not checked by the Relying Party applications for the lifetime of the Certificate. If the CSA Signing Key has been or is suspected to have been compromised, then the highest-rank IdenTrust Operations Manager available will convene a meeting of personnel involved in CSA operations to assess the degree and scope of the compromise. If it is determined that Private Keys were compromised, a new OCSP Responder Key Pair and Certificate will be immediately created (signed by the Subordinate CA Certificate) and installed in the OCSP Responder as soon as possible.

For any period of compromise, all signed validations for that period (during which the CSA Key was suspected to have been compromised) will be reviewed and re-signed with a new Key.

### **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.

#### **5.7.4.1 Customer Service Center**

IdenTrust implements and maintains a TrustID Customer Service Center to provide assistance and services to Subscribers and Relying Parties, and a system for receiving, recording, responding to, and reporting TrustID problems within its organization. The IdenTrust customer service center is directly available during standard working hours in all continental U.S. time zones, Monday through Friday, excluding U.S. federal holidays. During holidays, weekend days, and hours not directly covered, an answering service is available with the ability to reach Customer Support Representatives that are on call.

IdenTrust Customer Service Center assists Subscribers with Certificate- and Key-related issues. Such issues include, but are not limited to, problems with Key Generation and Certificate installation. Those concerns can include but are not limited to problems with accessing information and inquiries of a general nature.

IdenTrust can provide help to users when a security incident occurs in the system and share information concerning common vulnerabilities and threats. A security incident is defined to be any adverse event that threatens the security of information resources. Adverse events include compromises of integrity, DoS/DdoS, compromises of confidentiality, loss of accountability, or damage to any part of the system.

#### **5.7.4.2 Entity Public Key is Revoked**

In the event of the need for Revocation of a CA Certificate issued to an Issuing CA, IdenTrust will immediately notify: (i) the PMA; (ii) all CAs to whom it has issued Cross-Certified Subordinate CA Certificates; (iii) all of its RAs;

(iv) all Subscribers; and (v) all Individuals or Organizations who are responsible for a Certificate used to an Electronic Device. IdenTrust also will: (i) publish the CA Certificate serial number on an appropriate CRL; and (ii) revoke all Cross-Certified Subordinate CA Certificates signed with the revoked CA Certificate. After addressing the factors that led to Revocation, IdenTrust may: (i) generate a new CA signing Key Pair; and (ii) re-issue TrustID Certificates to all End Entities and ensure all CRLs and ARLs are signed using the new Key. In the event of the need for Revocation of any other entity's Digital Signature Certificate, refer to the procedures described in [Section 4.9](#)

## 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 following:

### 5.8.1 Termination of RA

- Archival of all audit logs and other records before termination;
- Delivery of current operating records to a responsible successor RA that will provide Certificate Revocation services for the remaining terms of Certificates and accept the assignment of any related, contracted-for support services. Note that if the termination is for convenience, or other non-security related reasons and provisions have been made to continue compromise recovery, compliance, and security audit, archive, Revocation, and data recovery services, then the Certificates approved by the RA do not need to be revoked. However, all RA System and LRA Certificates will be revoked;
- Refund of pro rata portions of Certificate fees and any payments for services that will not be delivered;
- Ensuring the transfer to, and preservation of, archived records by a responsible RA successor for the archive retention period specified in [Section 5.5.2](#);
- Surrender and/or zeroization of Cryptographic Modules containing Private Keys in accordance with [Section 6.2.9](#) and Revocation of all Certificates, if necessary; and
- If a successor RA will be assuming responsibilities for existing customers, provisions for such transition, e.g., replacement Certificates, customer relations, etc.

### 5.8.2 Termination of Contractual Relationship with a Sponsoring Organization with Enterprise RAs

- Archival of all paper records, if any, before termination;
- Delivery of current operating records to a responsible successor Sponsoring Organization with Enterprise RAs that will provide Certificate Revocation services for the remaining terms of Certificates and accept the assignment of any related, contracted-for support services. Note that if the termination is for convenience, or other non-security related reasons, and provisions have been made to continue compromise recovery, compliance and security audit, archive, and Revocation, then the Certificates approved by the Enterprise RA do not need to be revoked. However, all TrustID Business Certificates issued to that Enterprise RA will be revoked;
- Ensuring the transfer to, and preservation of, archived records by a responsible Enterprise RA successor for the archive retention period specified in [Section 5.5.2](#);
- Surrender and/or zeroization of Cryptographic Modules containing Private Keys in accordance with [Section 6.2.9](#) and Revocation of all Certificates, if necessary; and

- If a successor Enterprise RA will be assuming responsibilities for existing Sponsoring Organization with an Enterprise RA addendum agreement with IdenTrust, provisions for such transition, e.g., replacement Certificates, customer relations, etc.

### **5.8.3 Termination of Issuer CA**

In the case of an Issuer CA termination, all the steps above will occur, with these exceptions:

- Revocation of all Certificates issued under the CA will not be optional;
- Revocation will be effected before revoking the CA Certificate; and
- the nextUpdate in the CRL will be past the expiry date of all Certificates issued by the CA. OCSP validation will not be available since its Certificate must be revoked.

### **5.8.4 Termination of Root CA**

In the event that IdenTrust ceases operation, all Subscribers, Sponsoring Organizations, RAs, CMAs, Repositories, and Authorized Relying Parties will be promptly notified of the termination. Browsers will also be informed about the termination. All TrustID Certificates issued by IdenTrust that reference the TrustID CP will be revoked no later than the time of termination. All current and archived CA Identity Proofing, Certificate, validation, Revocation, renewal, Policy and practices, billing, and audit data will be transferred to the PMA (or designated body) within 24 hours of IdenTrust cessation and in accordance with the TrustID CP. Transferred data will not include any data unrelated to the TrustID CP. No Key recovery enabled Repository data will be co-mingled with this data.

## 6 TECHNICAL SECURITY CONTROLS

Technical controls are implemented to reduce the probability of threat to IdenTrust's TrustID system and its data's integrity. The IdenTrust's Security Office selects the mix of controls, technologies, and procedures that best fits the risk profile of the system. IdenTrust, and all RAs, CSAs, CMAs, and Repositories, implement appropriate technical security controls.

### 6.1 KEY PAIR GENERATION AND INSTALLATION

#### 6.1.1 Key Pair Generation

Key Pairs for all PKI Service Providers and End Entities are generated in such a way that the Private Key is not known by other than the Key holder. Acceptable ways to accomplish this include: (i) requiring all Participants to generate their own Keys using a Trustworthy System; (ii) directing Participants not to reveal the Private Keys to anyone else; and/or (iii) having keys generated in hardware Tokens from which the Private Key cannot be extracted. Despite the foregoing, all PKI Service Provider Keys (other than Repositories) are generated and stored in Tokens. Key Pairs for Repositories and End Entities can be generated and stored in either hardware or software Cryptographic Modules.

##### 6.1.1.1 CA Key Pair Generation

Cryptographic Keying material used by IdenTrust to sign Certificates, CRLs, or status information is generated in a FIPS-140 validated Cryptographic Module. IdenTrust Cryptographic Modules meet FIPS 140-1/2 Level 3.

The CA 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

All Keys for Issuing CAs and RAs are randomly generated in a Token. Any pseudo-random numbers used for Key generation material are generated by a FIPS approved method.



### 6.1.1.3 Subscriber Key Pair Generation

Key Pairs for Subscribers can be generated in either hardware or software. For Subscribers, validated software or hardware is used to generate pseudo-random numbers, Key Pairs, and symmetric Keys. Any pseudo-random numbers used for Key generation material are generated by a FIPS approved method.

Subscriber signature Private Keys will not be generated by IdenTrust.

In those cases where Key Pairs are generated by IdenTrust on behalf of the Subscribers (e.g., Encryption Key Pair), IdenTrust implements procedures to ensure that the Cryptographic Module is not activated by an unauthorized entity, this is further explained below in [Section 6.1.2.1](#).

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 4.9.1.1.2](#);
5. The Public Key corresponds to an industry-demonstrated weak Private Key. For requests submitted on or after November 15, 2024, 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. If the server Subscriber Certificate will contain an extKeyUsage extension containing either the values id-kp-serverAuth [[RFC 5280](#)] or anyExtendedKeyUsage [[RFC 5280](#)], IdenTrust shall not generate a Key Pair on behalf of a server Subscriber, and shall not accept a certificate request using a Key Pair previously generated by IdenTrust.

### 6.1.2 Private Key Delivery to Subscriber

IdenTrust does not generate the Key Pairs for Subscriber Certificates that have an EKU extension containing the KeyPurposeId id-kp-serverAuth or anyExtendedKeyUsage.

In most cases, a Private Key will be generated and remain within the crypto boundary of the Cryptographic Module. If the owner of the Cryptographic Module generates the Key, then there is no need to deliver the Private Key. If a Key is not generated by the intended Key holder, then the person generating the Key in the Cryptographic Module (e.g., "smart card") must securely deliver the Cryptographic Module to the intended Key holder. Accountability for the location and state of the Cryptographic Module must be maintained until both delivery and possession occur. The recipient will acknowledge receipt of the Cryptographic Module to the Issuing CA or the RA. If the End Entity generates the Key, and the Key will be stored by and used by the application that generated it, or on a hardware Token in the possession of the End Entity, no further action is required. If the Key must be extracted for use by other applications or in other locations, a protected data structure (such as defined

in [PKCS#12]) will be used. The resulting file may be kept on a magnetic medium or transported electronically. See [Section 6.4.1](#) - Activation Data Generation and Installation.

If IdenTrust generates the Private Key on behalf of the Subscriber where the Private Keys will be transported to the Subscriber, then the entity generating the Private Key shall either transport the Private Key in hardware with an activation method that is equivalent to 128 bits of encryption or encrypt the Private Key with at least 128 bits of encryption strength. IdenTrust does store Subscriber Private Keys in clear text.

The material used to activate/protect the Private Key (e.g., a password used to secure a PKCS 12 file) is delivered to the Subscriber securely and separately from the container holding the Private Key.

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.

For delivery of an encryption Private Key, 2 methods are available as described in the following sub-sections:

#### **6.1.2.1 IdenTrust Key Generation**

Immediately after the encryption Private Keys are generated, they are encrypted and stored in the escrow database when enabled. Then during the Certificate retrieval process, the system assembles and downloads, over a server-authenticated SSL/TLS-Encrypted session, the secure PKCS#12 file and its password to the Subscriber's computer or Cryptographic Module directly, which ensures that only the Subscriber and the escrowed copies exist (when enabled). During this process, the Subscriber acknowledges the receipt of the encryption Private Key.

If the secure PKCS#12 file is for a hardware-stored Certificate, it is downloaded directly to the hardware Cryptographic Module in a way that is transparent to the Subscriber. If the secure file is for a software-stored Certificate, it might be downloaded directly and transparently; or require the Subscriber's intervention to complete the process; the choice will depend on specific implementations.

#### **6.1.2.2 Subscriber Key Generation**

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.

IdenTrust does not deliver Cryptographic Modules with Private Keys in them, instead of Private Keys are generated in a blank Cryptographic Module previously delivered to the Applicant/Subscriber through a postal method that allows tracking and confirmation delivery.

#### **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. 2 methods are used to bind the verified identity to the Public Key:

1. During the Certificate Issuance phase, the Applicant/PKI Sponsor's information, PKCS#10, and a hash of the Applicant/PKI Sponsor-provided Account Password are bound together via the server-authenticated SSL/TLS-Encrypted transmission to IdenTrust. Only the Applicant/PKI Sponsor knows the Account

Password because only the Account Password hash is stored. After Identity Proofing, the LRA provides an Activation Code to the Applicant/PKI Sponsor through an out-of-band verified channel. The secret Account Password and Activation Code are used in combination by the Applicant/PKI Sponsor to retrieve the Certificate during a subsequent server-authenticated SSL/TLS-encrypted session.

2. During the registration process, an LRA enrolls the Applicant/PKI Sponsor and approves the Issuance of a Certificate to the Subscriber. Activation Code(s) is/are generated and sent out-of-band to the Applicant/PKI Sponsor to a verified destination. 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 during the same session.

Another method of delivery is available for Enterprise RAs when working with PKI Sponsors within their Sponsoring Organization as verified by IdenTrust.

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 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)
4. 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, the TrustID CP, and this CPS to ensure the Subscriber receives the Root CA Certificate in a trustworthy fashion.

## 6.1.5 Key Sizes

### 6.1.5.1 Root and Subordinate CA Certificates Key Sizes

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.

### 6.1.5.2 Subscriber Certificates Key Sizes

- 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.

For Code Signing and Timestamp Authority Certificates:

- If the Key is RSA, then the modulus must be at least 3072 bits in length.
- If the Key is ECDSA, then the curve must be one of NIST P-256, P-384, or P-521.

The IdenTrust OCSF Responders will respond using SHA-256 or higher hash algorithms.

## 6.1.6 Public Key Parameters Generation and Quality Checking

### 6.1.6.1 Public Key Parameters Generation

Cryptographic Modules and associated software platforms used by CAs, the CSA, and Subscribers and RAs have been validated as conforming to FIPS 186-2 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.

The public exponent is in the range between  $2^{16}+1$  and  $2^{256}-1$ . The modulus is an odd number, not the power of a prime, and has no factors smaller than 752.

### 6.1.6.2 Parameter Quality Checking

Parameters for DSA are checked as specified in the current FIPS 186 version. IdenTrust will use Cryptographic Modules conforming to FIPS 186-3 as vendors make products available.

## 6.1.7 Key Usage Purposes (as per X509 v3 Key Usage Field)

The use of a specific Key is determined by the Key Usage extension in the X.509 Certificate. Certificate Key Usage and Key Usage fields are used in accordance with the [RFC 5280](#).

IdenTrust does not use Private Keys corresponding to Root 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 OCSF Response verification.

IdenTrust may opt to add additional extensions as long as IdenTrust as a CA is aware of the reason for including the data in the Certificate and its verification is addressed in this CPS. IdenTrust certifies Public Keys for use in signing or encrypting, but not both, except as specified below.

IdenTrust sets the Key Usage bits in all IdenTrust TrustID Infrastructure Certificates in accordance with IdenTrust Certificate Profiles as described in [Section 7](#).

#### **6.1.7.1 CA and Cross- Certified Subordinate CA Certificates**

All CA signature Private Keys are used only to sign Certificates and CRLs.

The following Key Usage values are present in the CA Certificates: (i) CRL Signature; and (ii) Key Certificate Signature.

##### **6.1.7.1.1 Restrictions on CA's Private Key Use**

IdenTrust, as the CA and CMA, implements a Root CA Certificate that is used only to sign Subordinate CA Certificates and provide validation services (i.e., OCSP Certificate and CRLs). Subordinate CA Certificates issued by IdenTrust are similarly used to sign Certificates and provide validation services only.

RAs, Enterprise RAs, and LRAs who are provided with TrustID Certificates to perform their daily functions, use these Certificates mainly for communication with Subscribers and access control to RA systems. If the RA is an automated system, the Private Key and Certificate are only used for access control and communication protection between the RA and the CA.

##### **6.1.7.2 Subordinate CA Certificates**

The following Key Usage values are present in the Subordinate CA Certificates: (i) Digital Signature; (ii) Certificate Signing; (iii) Off-line CRL Signing; (iv) CRL Signing; and (v) may include Non-Repudiation.

##### **6.1.7.3 Secure Email Certificates**

The following Key Usage values are present in the Subscribers Secure Email Certificates: (i) Digital Signature; and (ii) Key Encipherment.

The following Extended Key Usage value is present: (i) Secure Email and (ii) it may include Client Authentication and/or Microsoft Encrypting File System.

##### **6.1.7.4 Signing / Encryption Certificates (including Personal and Business)**

The following Key Usage values may be present in the Subscribers Certificates: (i) Digital Signature; (ii) Key Encipherment; (iii) Data Encipherment; and (iv) Non-repudiation. The following Extended Key Usage value may be present: (i) Client Authentication; (ii) Secure Email; (iii) Document Signing; and (iv) Smart Card Logon.

##### **6.1.7.5 VPN IPSec and OCSP Signing Certificates**

The following Key Usage values are present in the VPN IPSec, OCSP Signing, and Digital Signature.

The following Extended Key Usage values are present in VPN IPSec Certificates: (i) Server Authentication; (ii) Client Authentication; (iii) IP sec end system Certificate {1.3.6.1.5.5.7.3.5}; (iv) IP sec end system tunnel {1.3.6.1.5.5.7.3.6}; (v) IP sec end system user {1.3.6.1.5.5.7.3.7}; (vi) IP sec intermediate system usage {1.3.6.1.5.5.8.2.2}.

The following Extended Key Usage values are present in OCSP Signing Certificates: (i) id-kp-OCSPSigning and {1.3.6.1.5.5.7.3.9}.

##### **6.1.7.6 OV Server Certificates**

The following Key Usage values are present in the server Certificates: (i) Digital Signature and (ii) Key Encipherment.

The following Extended Key Usage values are present: (i) Server Authentication (ip-kp-serverAuth); and (ii) Client Authentication (ip-kp-clientAuth).

#### **6.1.7.7 FATCA Organization Certificates**

The following Key Usage values are present in the FATCA Organization Certificates: (i) Digital Signature and (ii) Key Encipherment.

The following Extended Key Usage values may be present: (i) Client Authentication (ip-kp-clientAuth); and (ii) Secure Email.

#### **6.1.7.8 EV Server Certificates**

The following Key Usage values are present in the server Certificates: (i) Digital Signature and (ii) Key Encipherment.

The following Extended Key Usage values are present: (i) Server Authentication (ip-kp-serverAuth); and (ii) Client Authentication (ip-kp-clientAuth).

### **6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS**

IdenTrust's CAs, RAs, CSAs, and CMAs each protect their Private Key(s) in accordance with the provisions of the TrustID CP, this CPS and the CA/B F. BRs.

#### **6.2.1 Cryptographic Module Standards and Controls**

IdenTrust uses only FIPS 140-1/2 Level 3-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.

Subscribers will store their Certificates in at least FIPS 140-1/2 Level 1-validated software Cryptographic Modules. If a Subscriber uses a hardware Cryptographic Module, other than TrustID Secure Email Certificates only, it will be validated to at least FIPS 140-1/2 Level 2. Higher levels are available if desired. These modules will not allow the user to export Key Pairs in clear text. All Trusted Agents, Enterprise RAs, and LRAs are required to use hardware Cryptographic Modules that are at least FIPS 140-1/2 Level 2-validated, except for TrustID Secure Email Software Certificates.

For TrustID Code Signing, TrustID Time-Stamping, Signing Authority, and AATL enabled Certificates (See OIDs in [Section 1.2.2](#)), the corresponding Key Pairs are generated and stored in hardware Cryptographic Modules that are validated at a minimum of FIPS 140-2 Level-2 or equivalent standard. For TrustID Card CIV Authentication Certificates and TrustID CIV Device Certificates, the corresponding Key Pairs are generated and stored in hardware Cryptographic Modules that are validated at a minimum of FIPS 140-1/2 Level 1 or equivalent standards or Trusted Platform Module as approved by the IdenTrust PMA and published in the TrustID CP, Appendix A.

Upon request, IdenTrust will provide at least FIPS 140-1 or FIPS 140-2 Level 2-validated Cryptographic Modules for Key Pair Generation and storage of Private Keys.

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.

If a Subscriber uses a hardware Cryptographic Module for TrustID Secure Email Certificates, any non-FIPS compliant device is acceptable as this Certificate type does not attest Identity, only control/ownership over an Email Address.

## **6.2.2 Private Key (N out of M) Multi-Person Control**

The CA and CSA signature Private Keys are stored in the Secure Room under multi-person control as discussed in [Section 5.1.2.1](#). 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 CA Encryption Keys**

No stipulation.

### **6.2.3.3 Escrow of Subscriber's Signature Private Keys**

IdenTrust does not escrow Subscriber's signature Private Keys. RAs are prohibited under the TrustID CP and this CPS from escrowing the signature Private Keys of Subscribers.

### **6.2.3.4 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**

Under 2-person control, IdenTrust backs up CA Private Keys on cloned Cryptographic Modules to obviate the need to re-key in the case of hardware failure.

2 copies of the Root CA Certificate are created in separate Cryptographic Modules. 2 copies of all other CAs are created in a shared Cryptographic Module. All backup Cryptographic Modules are FIPS 140-1/2 level 3-validated.

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 5.1.2.1](#).

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](#).



When the Root CA and all other CAs Keys are no longer needed, the Cryptographic Module containing them is zeroized in accordance with [Section 6.2.9](#).

IdenTrust will not archive the Private Keys for any Issuing CA or External CA that is not IdenTrust. Those Private keys will be held exclusively by that Issuing CA or External CA. If those keys are communicated to another party, IdenTrust will revoke the Certificates.

#### **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.

#### **6.2.4.3 Backup of Subscriber's Key Management Private Keys**

Encryption Private Keys may be backed up as long as they remain under the control of the Subscriber and are protected and used under conditions protected at a level no lower than stipulated for the primary version of the Key. This level of protection for the Encryption Private Key includes not backing it up in clear text outside of the module.

#### **6.2.4.4 Backup of CSA Private Key**

Under 2-person control, IdenTrust backs up CSA Private Keys on cloned Cryptographic Modules to obviate the need to re-key in the case of hardware failure.

2 copies of all CSAs are created in a shared Cryptographic Module. All backup Cryptographic Modules are FIPS 140-1/2 Level 3-rated.

The backup of all other CSA 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 5.1.2.1](#).

IdenTrust stores the CSA Private Keys and one of the copies in the Secure Room. The second backup of the CSA signature Private Keys are kept in a secure off-site facility.

When the CSA Keys are no longer needed, the Cryptographic Module containing them is zeroized in accordance with [Section 6.2.9](#).

### **6.2.5 Private Key Archival**

Under no circumstances, IdenTrust archives the signature Private Key of a Subscriber or its CA signature Private Keys.

Parties other than the Subordinate CA are not allowed to archive the Subordinate CA Private Keys without authorization by the Subordinate CA.

For some purposes, such as data recovery, IdenTrust will archive Encryption Keys for Subscribers (decided on an implementation specific basis). As part of the Certificate Issuance/Key escrow process for designated Certificates, Subscribers are notified that the Encryption Private Keys associated with their encryption Certificates will be escrowed. As explained in [Section 4.12.1](#), during the Key Generation event, the Private Key is stored in an encrypted file (a PKCS#12), and the information needed to decrypt the encrypted Private Key consists of a system-generated code (a strong passphrase) that is itself encrypted. The escrowed Key and passphrase files are stored in the KED. IdenTrust archives the database where escrowed encryption Private Keys are held. The controls around this archive are explained in [Section 5.1.6](#).



## 6.2.6 Private Key Transfer Into or From a Cryptographic Module

CA and CSA Private Keys are generated on a FIPS 140-1/2 Level 3 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. The CA Private Keys are backed up in accordance with [Section 6.2.4.1](#).

Subscriber’s signature Private Keys are generated and kept inside of Cryptographic Modules.

Encryption Private Keys are generated outside of the Subscriber’s Cryptographic Module. For initial delivery or delivery after a Key recovery request, a secure data structure (e.g., PKCS#12 file) will be used. As additional security, the secure file will be protected by the use of a server-authenticated SSL/TLS session during the retrieval process.

## 6.2.7 Private Key Storage on Cryptographic Module

### 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, FIPS 140-3 level 3 Cryptographic Modules.

For Code Signing Certificates and other Certificates held on hardware Cryptographic Modules, Subscriber’s Private Keys are maintained in Cryptographic Modules evaluated at FIPS Level 2 and never appear in plaintext. For Subscribers using a software-based Cryptographic Module, the module may store Private Keys in any form as long as the Keys are not accessible without an authentication mechanism.

If IdenTrust generates the Private Key on behalf of a Subordinate CA, then IdenTrust will encrypt the Private Key for transport to the Subordinate CA. If IdenTrust becomes aware that a Subordinate CA’s Private Key has been communicated to any unintended person or an organization not affiliated with the Subordinate CA, then IdenTrust will revoke all Certificates that include the Public Key corresponding to the communicated Private Key.

### 6.2.7.2 Private Key Storage for Timestamp Authorities

Effective April 15, 2025, a Time-stamping Authority generate and protect Private Keys associated with its Root CA certificates and new Subordinate CA certificates with a validity period of greater than 72 months containing the id-kp-timeStamping KeyPurposeId in the extKeyUsage extension (per [section 7.1.2.2-extKeyUsage](#)) in the [CS BR](#), in a Cryptographic Module conforming to the requirements specified in [Section 6.2.7.1](#), maintained in a High Security Zone and in an offline state or air-gapped from all other networks.

Timestamp Certificates issued on or after April 15, 2025, issued by a Timestamp Authority Subordinate CA with a validity period greater than 72 months, must be signed by a Private Key generated and protected in a Cryptographic Module conforming to the requirements specified in [Section 6.2.7.1](#), maintained in a high security zone and in an offline state or air-gapped from all other networks.

### 6.2.7.3 Private key storage for Signing Services

The Signing Service ensures that a Subscriber’s Private Key is generated, stored, and used in a secure environment that has controls to prevent theft or misuse. The Signing Service enforces multi-factor authentication or server-to-server authentication to access and authorize Code Signing.

For Code Signing Certificates, Signing Services shall protect Subscriber Private Keys in a Cryptographic Module conforming to at least FIPS 140-2 level 3 or Common Criteria EAL 4+.

Techniques that must be used to satisfy this requirement include:

1. Use of a Cryptographic Module, verified by means of a FIPS or Common Criteria certificate; or
2. A cloud-based key generation and protection solution with the following requirements:
  1. Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module that conforms to the specified requirements;
  2. Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key.

### **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 a FIPS 140-1/2 module specification. Subscribers of Business Certificates are instructed to protect their Private Key from unauthorized use with a strong password. Subscribers are obligated by contract, the TrustID CP, and this 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**

The CA 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 5.1.2.1](#).

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

Public Keys are archived as part of the Certificate archival.

### 6.3.2 Certificate Operational Periods and Key Pair Usage Periods

All 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	20 years
Subordinate CAs Human and Others	No stipulation	15 years
CSA OCSP Responder	No stipulation	3 years
LRA (Signature/Encryption) End Entity Human (S/MIME) End Entity FATCA Organization	No stipulation	825 days
End Entity server	No stipulation	398 days
End Entity Code Signing	No stipulation	39 months
Time-Stamping CA	15 months	72 months
Time-Stamping End Entity	15 months	15 months
CIV Device	No stipulation	5 years
CIV Card Authentication	No stipulation	3 years

\* Subscriber Key Pair must be replaced in accordance with the provisions of [Section 3.3](#).

#### 6.3.2.1 Restrictions on CA's Private Key Use

The Private Key used by IdenTrust for issuing Certificates is used only for signing such Certificates and, optionally, CRLs or other validation services responses. A Private Key held by an RA, if any, is: (i) considered the IdenTrust CA's Private Key; (ii) is held by the RA as a fiduciary; and (iii) will not be used by the RA for any other purposes, except those specifically agreed to between IdenTrust and the RA. Further, any other Private Key used by an RA for purposes associated with its RA functions will not be used for any other purpose without the express permission by IdenTrust. The Private Key used by each RA in connection with the Issuance of Certificates is used only for communications relating to the approval or Revocation of such Certificates.

## **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 140-1/2 Level 3. 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**

The TrustID Policy makes no stipulation on the life of Activation Data; however, it should be changed periodically to decrease the likelihood that it has been discovered.

## **6.5 COMPUTER SECURITY CONTROLS**

IdenTrust operates a variety of commercial software and hardware systems to provide CA, CSA, RA, and Repository services. IdenTrust operates these software systems on Linux and Windows platforms. These systems are regularly scanned for potential security compromises and software is run locally to prevent such compromises. Machines running on the Windows platform are for client interface purposes only.

### **6.5.1 Specific Computer Security Technical Requirements**

All IdenTrust TrustID 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.

Users are required to identify themselves uniquely before being allowed to perform any actions on the system. IdenTrust's TrustID system internally maintains the identity of all users throughout their active sessions on the system and can link actions to specific users. Identification data is kept current by adding new users and deleting

former ones. User IDs that are inactive on the system for a specific period of time (e.g., 3 months) are disabled. IdenTrust authenticates all data requests from the application.

The System security Plan (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.

TrustID accountability covers a trusted path between the user and the system. A trusted path is a secure means of communication between the user and the system. For example, when a user types in their account name and password, the user wants to be sure that it is the system that the user is talking to, not a malicious program that someone else has left running on the terminal.

Users are restricted to data files, processing capability, or peripherals, and type of access (read, write, execute, delete) to the minimum necessary for the efficient completion of their job responsibilities. IdenTrust's physical access controls are designed and/or configured to provide the least privilege.

IdenTrust provides technical access controls designed to provide the least privilege and protections against unauthorized access to IdenTrust's 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.

The systems support a lockout threshold if excessive invalid access attempts are input, and record when an administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts. User IDs are revoked if a password attempt threshold failed login attempts are exceeded.

IdenTrust's systems can create, maintain, and protect from modification, unauthorized access, or destruction an audit trail of accesses to the resources it protects in accordance with federal law, regulations, and guidelines. Activity auditing capabilities are employed and enabled on all TrustID information systems to maintain a record of system activity by system or application processes and by users. Automated tools are used to log system activity and alert System and Security Office personnel via multiple channels, if possible, security events are detected. Trusted Role personnel are required to follow up on critical security events.

## **6.5.2 Computer Security Rating**

The IdenTrust Issuing CA system servers use equipment and operating systems with the following attributes: (i) self-protection; (ii) process isolation; (iii) discretionary access control; (iv) object reuse controls; (v) Individual Identity Proofing; and (vi) a protected audit records.

## **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.

IdenTrust has a process in place to minimize the likelihood of any component being tampered with. Vendors selected are chosen based on their reputation in the market, ability to deliver a quality product, and the likelihood of remaining viable companies in the future. Controls ensure that management is involved in the vendor selection and purchase decision process. External purchasing paperwork will only generically identify the purpose for which the component will be used. CA, CSA, RA, and LRA hardware and software PKI components are shipped directly to a trusted employee using shipping providers that have shipment tracking mechanisms allowing continuous tracking. Tracking information is provided to IdenTrust directly by the equipment vendor. Cryptographic Modules are received in tamper-evident containers. Cryptographic Module's shipment specific information (e.g., Serial number) is requested by IdenTrust to confirm the content when it is received. Other major PKI components (i.e., servers) are shipped under standard conditions. When received, a chain of custody is maintained from that point forward and information provided by the vendor during the purchase order process is used to confirm the correct equipment has been received.

IdenTrust dedicates a PKI platform specifically to its PKI operations including the CA, CSA, and RA functions. This includes server hardware, operating system software, Cryptographic Module, and PKI application software. No non-PKI applications are installed on those PKI platforms. Functionality for CA, CSA, and RA as well as databases, networking, and physical housing are shared with other certification systems.

IdenTrust maintains controls to prevent malicious software from being loaded. CA, CSA, and internal RA platforms are protected by a host-based fault integrity checker and other systems that monitors files in the system at least weekly to alert of any unapproved changes; if changes are found, the System Administrators are informed, CA Administrator and Security Officers enabling them to correct the situation. LRAs are required to take reasonable care to prevent malicious software from being loaded on their equipment. Only applications required to perform the RA functions are loaded on an LRA's computer, and all such software will be obtained from sources authorized by local Policy. Data on LRA equipment must be scanned for malicious code on first use and at least weekly afterward. Equipment updates are purchased or developed in the same manner as original equipment and are installed by trusted and trained personnel in a defined manner.

When IdenTrust uses Linting software developed by third parties, it will monitor for updated versions of that software and plan for updates no later than three (3) months from the release of the update.

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 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 properly 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 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.

Issuing Systems, Certificate Management 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 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.

IdenTrust's CA system is connected to one network and is protected against known network attacks. The IdenTrust Root is kept in a high security zone and in an offline state or air-gapped from all other networks and turned on under controlled conditions only when necessary for signing Subordinate CA Certificates.

RAs and their LRAs are obligated by this CPS and the TrustID CP to implement Network Security controls consistent with this CPS and the TrustID CP.

Credentials issued to any privileged account or service account to access the secured facility hosting Certificate systems are revoked within 24 hours upon confirmation that the person is no longer in that role. Recommended security patches to Certificate systems are tested and applied within 30 days for "high" rated vulnerabilities, within 45 days for "medium" rated vulnerabilities. "Critical" rated vulnerabilities are evaluated for testing and application as soon as possible. IdenTrust also evaluates the criticality of security patches and may adjust the vendor ratings to reflect existing compensating controls.

Remote access to IdenTrust's TrustID system is restricted to secure methods employing approved Identity Proofing as well as intrusion detection and unauthorized access monitoring. Such access is restricted to devices owned or controlled by IdenTrust, must be over an encrypted channel, and must be made to a designated intermediary device such as a firewall VPN or proxy server.

If encryption is used to prevent unauthorized access to sensitive files as part of the system or application access control procedures, the following information is provided:

- The cryptographic methodology (e.g., secret Key and Public Key) used;
- If a specific off-the-shelf product is used, the name of the product;
- If the product and the implementation method meet federal standards (e.g., Data Encryption Standard, Digital Signature Standard), include that information; and

- Cryptographic Key management procedures for Key Generation, distribution, storage, entry, use, destruction, and archiving.

Additional system/network controls are incorporated based on the [NetSec BR](#).

## 6.8 TIME-STAMPING

IdenTrust's 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.
- Time-Stamping Service responses

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

TrustID Certificates contain Public Keys used for authenticating the sender of electronic messages and verifying the integrity of such messages -- i.e., Public Keys used for Digital Signature verification. TrustID Certificates are issued in the X.509 version 3 format unless another format is necessary to facilitate secure wireless communications or interoperability with devices using Wireless Application Protocol (WAP) or other technologies. Nothing in this CPS would require an Authorized Relying Party to use or process non-standard Certificates. Where applicable, TrustID Certificates include a reference to the OID for the Certificate type identified by this CPS within the appropriate field. This CPS or other publicly available document identify the Certificate extensions supported.

IdenTrust meets the technical requirements set forth in [Section 2.2](#) - Publication of Information, [Section 6.1.5](#) Key Sizes, and [Section 6.1.6](#) - Public Key Parameters Generation and Quality Checking.

IdenTrust Subscriber server Certificates issued prior to September 15, 2023, are issued in accordance with the Certificate Profile specified in the [TLS BR v1.8.6](#).

For all TrustID Certificates, IdenTrust generates non-sequential Certificate serial numbers greater than zero (0) and less than  $2^{159}$  containing at least 64 bits of output from a CSPRNG.

#### 7.1.1 Version Number(s)

IdenTrust only issues X.509 Certificates, version 3 Certificates. (i.e., populated with the integer "3")

#### 7.1.2 Certificate Content and Extensions

This section specifies the IdenTrust TrustID Certificate content and extensions based on the [RFC 5280](#) and applicable subsequent updates via the [RFC 6818](#).



### 7.1.2.1 Root CA Certificates

Root CA Certificates Name Fields	
Field	Description
version	Present. v3(2).
serialNumber	Present. A non-sequential unique number greater than zero (0) and less than $2^{159}$ containing at least 64 bits of output from a CSPRNG.
signature	See <a href="#">Section 7.1.3.2</a> .
issuer	Encoded value byte-for-byte identical to the encoded subject.
validity	See <a href="#">Section 6.3.2</a> .
subject	See <a href="#">Section 7.1.4.3.1</a>
subjectPublicKeyInfo	See <a href="#">Section 7.1.3.1</a> .
authorityKeyIdentifier	May be present and not marked critical. If present, the keyIdentifier field is present and identical to the subjectKeyIdentifier field.
basicConstraints	Present and marked critical. The cA field is set to true; the pathLenConstraint field is not present.
keyUsage	Present and marked critical. The bit positions for keyCertSign and cRLSign are set. If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit is set.
subjectKeyIdentifier	Present and not marked critical. Contains the value that is included in the keyIdentifier extension in certificates issued by this root.

### 7.1.2.2 Subordinate CA Certificates

#### 7.1.2.2.1 Subordinate CA S/MIME Certificates

Subordinate CA S/MIME Certificates - Name Fields	
Field	Description
version	Present. v3(2).
serialNumber	Present A non-sequential unique number greater than zero (0) and less than $2^{159}$ containing at least 64 bits of output from a CSPRNG.
signature	See <a href="#">Section 7.1.3.2</a> .
issuer	Encoded value byte-for-byte identical to the encoded subject. See <a href="#">Section 7.1.4.1</a> .
validity	See <a href="#">Section 6.3.2</a> .

Subordinate CA S/MIME Certificates - Name Fields	
Field	Description
Subject Distinguished Name	<p><b>countryName:</b> The two-letter ISO 3161-1 country code for the country</p> <p><b>organizationName:</b> Present, the CA's name or DBA. IdenTrust may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations, e.g., if the official record shows "Company Name Incorporated", the CA may use "Company Name Inc." or "Company Name".</p> <p><b>commonName:</b> Present; the content is an identifier for the certificate such that the certificate's name is unique across all certificates issued by IdenTrust, i.e. "IdenTrust TrustID SMIME CA 1".</p>
subjectPublicKeyInfo	See <a href="#">Section 7.1.3.1</a> .
authorityKeyIdentifier	Present and not marked critical. The keyIdentifier field is present and identical to the subjectKeyIdentifier field of the Issuing CA.
basicConstraints	Present and marked critical. The cA field is set to true; the pathLenConstraint field may be present.
certificatePolicies	Present and not marked critical. Includes one or more policy identifiers as defined in <a href="#">Section 1.2.2</a> or the anyPolicy identifier (2.5.29.32.0). It may include a cPSuri, and it may include a userNotice qualifier. See <a href="#">Section 7.1.8.1</a> for expected values.
cRLDistributionPoints	Present and not marked critical. It contains the HTTP URL of the IdenTrust's CRL service.
keyUsage	Present and marked critical. The bit positions for keyCertSign and cRLSign are set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit is set.
subjectKeyIdentifier	Present and not marked critical. It contains a value that is included in the keyIdentifier field of the authorityKeyIdentifier extension in Certificates issued by the Subordinate CA.
extKeyUsage	Present and not marked critical. It contains id-kp-emailProtection and it may contain id-kp-clientAuth; It does not contain id-kp-serverAuth, id-kp-codeSigning, id-kp-timeStamping, id-kp-OCSPSigning or anyExtendedKeyUsage. It may contain other values.
authorityInformationAccess	Present and not marked critical. It contains the HTTP URL of the Issuing CA OCSP responder id-ad-ocsp (accessMethod = 1.3.6.1.5.5.7.48.1) and the HTTP URL of the Issuing CA Certificate id-ad-calssuers (accessMethod= 1.3.6.1.5.5.7.48.2).
nameConstraints	May be present and marked critical.

### 7.1.2.2.2 Subordinate CA Server Certificates

Subordinate CA Server Certificates - Name Fields	
Field	Description
version	Present. v3(2).
serialNumber	Present. A non-sequential unique number greater than zero (0) and less than $2^{159}$ containing at least 64 bits of output from a CSPRNG.
signature	See <a href="#">Section 7.1.3.2</a> .
issuer	Encoded value byte-for-byte identical to the encoded subject. See <a href="#">Section 7.1.4.1</a> .
validity	See <a href="#">Section 6.3.2</a> .
subject	countryName: The two-letter ISO 3161-1 country code for the country organizationName: Present, the CA's name or DBA. IdenTrust may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations, e.g., if the official record shows "Company Name Incorporated", the CA may use "Company Name Inc." or "Company Name". commonName: Present; the content is an identifier for the certificate such that the certificate's name is unique across all certificates issued by IdenTrust, i.e. "IdenTrust TrustID Server CA 1".
subjectPublicKeyInfo	See <a href="#">Section 7.1.3.1</a> .
authorityKeyIdentifier	Present and not marked critical. The keyIdentifier field is present and identical to the <b>subjectKeyIdentifier</b> field of the Issuing CA.
basicConstraints	Present and marked critical. The cA field is set to true; the pathLenConstraint field may be present.
certificatePolicies	Present and not marked critical. Includes one or more policy identifiers as defined in <a href="#">Section 1.2.2</a> or the anyPolicy identifier (2.5.29.32.0). It may include a cPSuri. See <a href="#">Section 7.1.8.1</a> for expected values.
crlDistributionPoints	Present and not marked critical. It contains the HTTP URL of the CA's CRL service.
keyUsage	Present and marked critical. The bit positions for keyCertSign and cRLSign are set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit is set.
extKeyUsage	Present and not marked critical. It contains id-kp-serverAuth and it may contain id-kp-clientAuth. It does not contain id-kp-codeSigning, id-kp-emailProtection, id-kp-timestamping, id-kp-OCSPSigning, Precertificate Signing Certificate (OID:1.3.6.1.4.1.11129.2.4.4) or anyExtendedKeyUsage. It may contain other values.
authorityInformationAccess	Present and not marked critical.

Subordinate CA Server Certificates - Name Fields	
Field	Description
	It contains the HTTP URL of the Issuing CA OCSP responder id-ad-ocsp (accessMethod = 1.3.6.1.5.5.7.48.1) and the HTTP URL of the Issuing CA Certificate id-ad-calssuers (accessMethod= 1.3.6.1.5.5.7.48.2).
subjectKeyIdentifier	Present and not marked critical. It contains a value that is included in the keyIdentifier field of the authorityKeyIdentifier extension in Certificates issued by the Subordinate CA.
nameConstraints	May be present and marked critical.
Signed Certificate Timestamp List	May be present and not marked critical. If present, the Signed Certificate Timestamp List extension contents must be an OCTET STRING containing the encoded SignedCertificateTimestampList, as specified in <a href="#">RFC 6962 Section 3.3</a> . Each SignedCertificateTimestamp included within the SignedCertificateTimestampList must be for a PreCert LogEntryType that corresponds to the current certificate.

### 7.1.2.2.3 Subordinate CA Code Signing Certificates

Subordinate CA Code Signing Certificates - Name Fields	
Field	Description
version	Present. v3(2).
serialNumber	Present. A non-sequential unique number greater than zero (0) and less than $2^{159}$ containing at least 64 bits of output from a CSPRNG.
signature	See <a href="#">Section 7.1.3.2</a>
issuer	Encoded value byte-for-byte identical to the encoded subject. See <a href="#">Section 7.1.4.1</a>
validity	See <a href="#">Section 6.3.2</a>
subject	countryName: The two-letter ISO 3161-1 country code for the country organizationName: Present, the CA's name or DBA. IdenTrust may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations, e.g., if the official record shows "Company Name Incorporated", the CA may use "Company Name Inc." or "Company Name". commonName: Present; the content is an identifier for the certificate such that the certificate's name is unique across all certificates issued by IdenTrust, i.e. "TrustID Code Signing CA 1".
subjectPublicKeyInfo	See <a href="#">Section 7.1.3.1</a> .
authorityKeyIdentifier	Present and not marked critical. The keyIdentifier field is present and identical to the <b>subjectKeyIdentifier</b> field of the Issuing CA.
basicConstraints	Present and marked critical.

Subordinate CA Code Signing Certificates - Name Fields	
Field	Description
	The cA field is set to true; the pathLenConstraint field may be present.
certificatePolicies	Present and not marked critical. Includes one or more policy identifiers as defined in <a href="#">Section 1.2.2</a> or the anyPolicy identifier (2.5.29.32.0). It may include a cPSuri and it may include a userNotice qualifier. See <a href="#">Section 7.1.8.1</a> for expected values.
crlDistributionPoints	Present and not marked critical. It contains the HTTP URL of the CA's CRL service.
keyUsage	Present and marked critical. The bit positions for keyCertSign and cRLSign are set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit is set.
extKeyUsage	Present and not marked critical. It contains id-kp-codeSigning.
authorityInformationAccess	Present and not marked critical. It contains the HTTP URL of the Issuing CA OCSP responder id-ad-ocsp (accessMethod = 1.3.6.1.5.5.7.48.1) and the HTTP URL of the Issuing CA Certificate id-ad-caIssuers (accessMethod= 1.3.6.1.5.5.7.48.2).
subjectKeyIdentifier	Present and not marked critical. It contains a value that is included in the keyIdentifier field of the authorityKeyIdentifier extension in Certificates issued by the Subordinate CA.

#### 7.1.2.2.4 Subordinate CA Time-Stamping Certificates

Subordinate CA Time-Stamping Certificates - Name Fields	
Field	Description
version	Present. v3(2).
serialNumber	Present A non-sequential unique number greater than zero (0) and less than $2^{159}$ containing at least 64 bits of output from a CSPRNG.
signature	See <a href="#">Section 7.1.3.2</a> .
issuer	Encoded value byte-for-byte identical to the encoded subject. See <a href="#">Section 7.1.4.1</a> .
validity	See <a href="#">Section 6.3.2</a> .
subject	countryName: Present, the two-letter ISO 3161-1 country code for the country. organizationName: Present, the CA's name or DBA. IdenTrust may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations, e.g., if the official record shows "Company Name Incorporated", the CA may use "Company Name Inc." or "Company Name".

Subordinate CA Time-Stamping Certificates - Name Fields	
Field	Description
	commonName: Present; the content is an identifier for the certificate such that the certificate's name is unique across all certificates issued by IdenTrust, i.e. "TrustID Timestamping CA 1".
subjectPublicKeyInfo	See <a href="#">Section 7.1.3.1</a> .
authorityKeyIdentifier	Present and not marked critical. The keyIdentifier field is present and identical to the subjectKeyIdentifier field of the Issuing CA.
basicConstraints	Present and marked critical. The cA field is set to true; the pathLenConstraint field may be present.
certificatePolicies	Present and not marked critical. Includes one or more policy identifiers as defined in <a href="#">Section 1.2.2</a> or the anyPolicy identifier (2.5.29.32.0). It may include a cPSuri and it may include a userNotice qualifier. See <a href="#">Section 7.1.8.1</a> for expected values.
crlDistributionPoints	Present and not marked critical. It contains the HTTP URL of the CA's CRL service.
keyUsage	Present and marked critical. The bit positions for keyCertSign and cRLSign are set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit is set.
extKeyUsage	Present and not marked critical. It contains id-kp-timestamping.
authorityInformationAccess	Present and not marked critical. It contains the HTTP URL of the Issuing CA OCSP responder id-ad-ocsp (accessMethod = 1.3.6.1.5.5.7.48.1) and the HTTP URL of the Issuing CA Certificate id-ad-caIssuers (accessMethod= 1.3.6.1.5.5.7.48.2).
subjectKeyIdentifier	Present and not marked critical. It contains a value that is included in the keyIdentifier field of the authorityKeyIdentifier extension in Certificates issued by the Subordinate CA.

#### 7.1.2.2.5 Subordinate CA Device Certificates

Subordinate CA Device Certificates - Name Fields	
Field	Description
version	Present. v3(2).
serialNumber	Present. A non-sequential unique number greater than zero (0) and less than $2^{159}$ containing at least 64 bits of output from a CSPRNG.
signature	See <a href="#">Section 7.1.3.2</a> .
issuer	Encoded value byte-for-byte identical to the encoded subject. See <a href="#">Section 7.1.4.1</a> .

Subordinate CA Device Certificates - Name Fields	
Field	Description
validity	See <a href="#">Section 6.3.2</a> .
subject	<p>countryName: Present, the two-letter ISO 3161-1 country code for the country.</p> <p>organizationName: Present, the CA's name or DBA. IdenTrust may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations, e.g., if the official record shows "Company Name Incorporated", the CA may use "Company Name Inc." or "Company Name".</p> <p>commonName: Present; the content is an identifier for the certificate such that the certificate's name is unique across all certificates issued by IdenTrust, i.e. "TrustID Device CA 1".</p>
subjectPublicKeyInfo	See <a href="#">Section 7.1.3.1</a> .
authorityKeyIdentifier	<p>Present and not marked critical.</p> <p>The keyIdentifier field is present and identical to the subjectKeyIdentifier field of the Issuing CA.</p>
basicConstraints	<p>Present and marked critical.</p> <p>The cA field is set to true; the pathLenConstraint field may be present.</p>
certificatePolicies	<p>Present and not marked critical.</p> <p>Includes one or more policy identifiers as defined in <a href="#">Section 1.2.2</a> or the anyPolicy identifier (2.5.29.32.0). It may include a cPSuri and it may include a userNotice qualifier. See <a href="#">Section 7.1.8.1</a> for expected values.</p>
crlDistributionPoints	<p>Present and not marked critical.</p> <p>It contains the HTTP URL of the CA's CRL service.</p>
keyUsage	<p>Present and marked critical.</p> <p>The bit positions for keyCertSign and cRLSign are set.</p>
extKeyUsage	<p>Present and not marked critical.</p> <p>It contains id-kp-clientAuth, id-kp-ipsecEndSystem, id-kp-ipsecUser, id-kp-ipsecIKE, iKEIntermediate, ipsecTunnel, and id-PIV-cardAuth. It may contain other values.</p>
authorityInformationAccess	<p>Present and not marked critical.</p> <p>It contains the HTTP URL of the Issuing CA OCSF responder id-ad-ocsp (accessMethod = 1.3.6.1.5.5.7.48.1) and the HTTP URL of the Issuing CA Certificate id-ad-caIssuers (accessMethod= 1.3.6.1.5.5.7.48.2).</p>
subjectKeyIdentifier	<p>Present and not marked critical.</p> <p>It contains a value that is included in the keyIdentifier field of the authorityKeyIdentifier extension in Certificates issued by the Subordinate CA.</p>

### 7.1.2.3 Subscriber Certificates

#### 7.1.2.3.1 Subscriber S/MIME Certificates

Subscriber S/MIME Certificates - Name Fields	
Field	Description
version	Present. v3(2).
serialNumber	Present. A non-sequential unique number greater than zero (0) and less than $2^{159}$ containing at least 64 bits of output from a CSPRNG.
signature	See <a href="#">Section 7.1.3.2</a> .
issuer	Encoded value byte-for-byte identical to the encoded subject. See <a href="#">Section 7.1.4.1</a> .
validity	See <a href="#">Section 6.3.2</a> .
Subject Distinguished Name	See <a href="#">Section 7.1.4.3.3</a> Subject Distinguished Name – S/MIME Certificates
certificatePolicies	Present and not marked critical. Includes at least one or more policy identifiers as defined in <a href="#">Section 1.2.2</a> . It may include a cPSuri, and it may include a userNotice qualifier. See <a href="#">Section 7.1.8.1</a> for expected values.
cRLDistributionPoints	Present and not marked critical. It contains at least one distributionPoint whose fullName value includes a GeneralName of type uniformResourceIdentifier that includes a URI where the Issuing CA's CRL can be retrieved. Every uniformResourceIdentifier have the URI scheme HTTP. Other schemes are not present.
authorityInformationAccess	Present and not marked critical. Id-ad-ocsp: It may contain one or more accessMethod values of type id-ad-ocsp that specifies the URI of the Issuing CA's OCSP responder. When provided, every accessMethod will have the URI scheme HTTP. Other schemes are not present. Id-ad-calssuers: Contain at least one accessMethod value of type id-ad-calssuers that specifies the URI of the Issuing CA's Certificate. When provided, every accessMethod shall have the URI scheme HTTP. Other schemes are not present.
basicConstraints	May be present and marked critical. The cA field is set to false; the pathLenConstraint field is not present.
keyUsage	Present and marked critical.



Subscriber S/MIME Certificates - Name Fields	
Field	Description
	<p><b><u>RSA Strict Profile</u></b>  For signing only, bit positions is set for digitalSignature and it may be set for nonrepudiation.  For key management only, bit positions are set for keyEncipherment.  For dual use, bit positions are set for digitalSignature and keyEncipherment and may be set for nonrepudiation.</p> <p><b><u>RSA Multipurpose Profile</u></b>  For signing only, bit positions are set for digitalSignature and may be set for nonrepudiation.  For key management only, bit positions are set for keyEncipherment and may be set for dataEncipherment.  For dual use, bit positions are set for digitalSignature and keyEncipherment and may be set for nonrepudiation and dataEncipherment.</p>
	<p><b><u>ECDSA Strict Profile</u></b>  For signing only, bit positions are set for digitalSignature and may be set for nonrepudiation.  For key management only, bit positions are set for keyAgreement and may be set for encipherOnly or decipherOnly.  For dual use, bit positions are set for digitalSignature and keyAgreement and may be set for nonrepudiation and for encipherOnly or decipherOnly (only if keyAgreement is set).</p> <p><b><u>ECDSA Multipurpose Profile</u></b>  For signing only, bit positions are set for digitalSignature and may be set for nonrepudiation.  For key management only, bit positions are set for keyAgreement and may be set for encipherOnly or decipherOnly.  For dual use, bit positions are set for digitalSignature and keyAgreement and may be set for nonrepudiation and for encipherOnly or decipherOnly (only if keyAgreement is set).</p>
extkeyUsage	Present and not marked critical. <b><u>Strict Profile:</u></b> Only id-kp-emailProtection is present. <b><u>Multipurpose Profile:</u></b> id-kp-emailProtection and other values may be present The values id-kp-serverAuth, id-kp-codeSigning, id-kp-timeStamping, and anyExtendedKeyUsage are not present.
authorityKeyIdentifier	Present and not marked critical. The keyIdentifier field is present and identical to the subjectKeyIdentifier field of the Issuing CA.
subjectAlternativeName	Present and not marked critical unless the subject field is an empty sequence. This extension contains at least one GeneralName entry of the following types: <ul style="list-style-type: none"> <li>- Rfc822Name and/or</li> <li>- otherName of type id-on-SmtpUTF8Mailbox.</li> <li>- otherName: userPrincipalName</li> </ul>
subjectKeyIdentifier	Present and not marked critical. Unique value generated as defined in the <a href="#">RFC 5280 Section 4.2.1.2</a> .

### 7.1.2.3.2 Subscriber Server Certificates

Subscriber Server Certificates - Name Fields	
Field	Description
version	Present. v3(2).
serialNumber	Present. A non-sequential unique number greater than zero (0) and less than $2^{159}$ containing at least 64 bits of output from a CSPRNG.
signature	See <a href="#">Section 7.1.3.2</a> .
issuer	Encoded value byte-for-byte identical to the encoded subject. See <a href="#">Section 7.1.4.1</a> .
validity	notBefore: A value within 48 hours of the Certificate signing operation. notAfter: See <a href="#">Section 6.3.2</a> .
Subject Distinguished Name	See <a href="#">Section 7.1.4.3.4</a> Subject Distinguished Name Subscriber DV Server Certificates See <a href="#">Section 7.1.4.3.5</a> Subject Distinguished Name Subscriber OV Server Certificates See <a href="#">Section 7.1.4.3.6</a> Subject Distinguished Name Subscriber EV Server Certificates
authorityKeyIdentifier	Present and not marked critical. The keyIdentifier field is present and identical to the subjectKeyIdentifier field of the Issuing CA.
basicConstraints	May be present and marked critical. The cA field is set to false; the pathLenConstraint field is not present.
certificatePolicies	Present and not marked critical. Includes one or more policy identifiers as defined in <a href="#">Section 1.2.2</a> . It may include a cPSuri. See <a href="#">Section 7.1.8.1</a> for expected values.
cRLDistributionPoints	Present and not marked critical. It contains the HTTP URL of the IdenTrust's CRL service.
keyUsage	Present and marked critical. permitted values for RSA public keys are: digitalSignature, keyEncipherment, and dataEncipherment. Permitted values for ECC public keys are digitalSignature and keyAgreement.
subjectAltName	Present and not marked critical. Contains at least one dNSName or iPAddress General Name. If the subject field of the certificate is an empty sequence, this extension is marked critical.
extKeyUsage	Present and not marked critical. It contains id-kp-serverAuth and it may contain id-kp-ClientAuth.
authorityInformationAccess	Present and not marked critical. It contains the HTTP URL of the Issuing CA OCSP responder id-ad-ocsp (accessMethod = 1.3.6.1.5.5.7.48.1) and the HTTP URL of the Issuing CA Certificate id-ad-caIssuers (accessMethod= 1.3.6.1.5.5.7.48.2).
subjectKeyIdentifier	May be present and not marked critical.

Subscriber Server Certificates - Name Fields	
Field	Description
	Unique value generated as defined in the <a href="#">RFC 5280 Section 4.2.1.2</a> .
Signed Certificate Timestamp List	<p>May be present and not marked critical.</p> <p>If present, the Signed Certificate Timestamp List extension contents must be an OCTET STRING containing the encoded SignedCertificateTimestampList, as specified in <a href="#">RFC 6962 Section 3.3</a>.</p> <p>Each SignedCertificateTimestamp included within the SignedCertificateTimestampList must be for a PreCert LogEntryType that corresponds to the current certificate.</p>
signatureAlgorithm	An encoded value that is byte-for-byte identical to the tbsCertificate.signature.

### 7.1.2.3.3 Subscriber Code Signing Certificates

Subscriber Code Signing Certificates - Name Fields	
Field	Description
version	Present. v3(2)
serialNumber	Present. A non-sequential unique number greater than zero (0) and less than $2^{159}$ containing at least 64 bits of output from a CSPRNG.
signature	See <a href="#">Section 7.1.3.2</a> .
issuer	Encoded value byte-for-byte identical to the encoded subject. See <a href="#">Section 7.1.4.1</a> .
validity	See <a href="#">Section 6.3.2</a> .
Subject Distinguished Name	See <a href="#">Section 7.1.4.3.7</a> Subject Distinguished Name Subscriber Non-EV Code Signing Certificates See <a href="#">Section 7.1.4.3.8</a> Subject Distinguished Name Subscriber EV Code Signing Certificates
authorityKeyIdentifier	Present and not marked critical. The keyIdentifier field is present and identical to the subjectKeyIdentifier field of the Issuing CA.
basicConstraints	May be present and marked critical. The cA field is set to false; the pathLenConstraint field is not present.
certificatePolicies	Present and not marked critical. Includes at least one or more policy identifiers as defined in <a href="#">Section 1.2.2</a> . It may include a cPSuri. See <a href="#">Section 7.1.8.1</a> for expected values.
cRLDistributionPoints	Present and not marked critical. It contains the HTTP URL of the IdenTrust's CRL service.
keyUsage	Present and marked critical. The bit position for digitalSignature is set. The Bit positions for keyCertSign and cRLSign are not set. All other bit positions are not set
subjectAltName	Not present
extKeyUsage	Present and marked non-critical. It contains id-kp-codeSigning

Subscriber Code Signing Certificates - Name Fields	
Field	Description
	<p>It may contain Lifetime Signing OID (1.3.6.1.4.1.311.10.3.13); id-kp-emailProtection and Document Signing (1.3.6.1.4.1.311.3.10.3.12)</p> <p>The values id-kp-serverAuth, id-kp-codeSigning, id-kp-timeStamping, and anyExtendedKeyUsage are not present.</p>
authorityInformationAccess	<p>Present and not marked critical.</p> <p>It contains the HTTP URL of the Issuing CA OCSP responder id-ad-ocsp (accessMethod = 1.3.6.1.5.5.7.48.1) and the HTTP URL of the Issuing CA Certificate id-ad-calssuers (accessMethod= 1.3.6.1.5.5.7.48.2).</p>
subjectKeyIdentifier	<p>May be present and not marked critical.</p> <p>Unique value generated as defined in the <a href="#">RFC 5280 Section 4.2.1.2</a>.</p>
signatureAlgorithm	An encoded value that is byte-for-byte identical to the tbsCertificate.signature.

#### 7.1.2.3.4 Subscriber Time-Stamping Certificates

Subscriber Time-Stamping Certificates - Name Fields	
Field	Description
Version	<p>Present.</p> <p>v3(2)</p>
serialNumber	<p>Present.</p> <p>A non-sequential unique number greater than zero (0) and less than <math>2^{159}</math> containing at least 64 bits of output from a CSPRNG.</p>
Signature	See <a href="#">Section 7.1.3.2</a> .
Issuer	Encoded value byte-for-byte identical to the encoded subject. See <a href="#">Section 7.1.4.1</a> .
validity	See <a href="#">Section 6.3.2</a> .
Subject Distinguished Name	See <a href="#">Section 7.1.4.3.9</a> Subject Distinguished Name Time-Stamping Certificates
authorityKeyIdentifier	<p>Present and not marked critical.</p> <p>The keyIdentifier field is present and identical to the subjectKeyIdentifier field of the Issuing CA.</p>
basicConstraints	<p>Present and marked critical.</p> <p>The cA field is set to false; the pathLenConstraint field is not present.</p>
certificatePolicies	<p>Present and not marked critical.</p> <p>Includes at least one or more policy identifiers as defined in <a href="#">Section 1.2.2</a>.</p> <p>It may include a cPSuri and a User Notice. See <a href="#">Section 7.1.8.1</a> for expected values.</p>
cRLDistributionPoints	<p>Present and not marked critical.</p> <p>It contains the HTTP URL of the IdenTrust's CRL service.</p>
keyUsage	Present and marked critical

Subscriber Time-Stamping Certificates - Name Fields	
Field	Description
	The bit position for digitalSignature is set. The Bit positions for keyCertSign and cRLSign are not set. All other bit positions are not set
subjectAltName	Present and not marked critical. Contains at least one dNSName or iPAddress General Name. If the subject field of the certificate is an empty sequence, this extension is marked critical.
extKeyUsage	Present and marked critical. It contains id-kp-timeStamping These EKUs are not present: anyExtendedKeyUsage or id-kp-serverAuth
authorityInformationAccess	Present and not marked critical. It contains the HTTP URL of the Issuing CA OCSP responder id-ad-ocsp (accessMethod = 1.3.6.1.5.5.7.48.1) and the HTTP URL of the Issuing CA Certificate id-ad-caIssuers (accessMethod= 1.3.6.1.5.5.7.48.2).
subjectKeyIdentifier	May be present and not marked critical. Unique value generated as defined in the <a href="#">RFC 5280 Section 4.2.1.2</a> .
signatureAlgorithm	An encoded value that is byte-for-byte identical to the tbsCertificate.signature.

### 7.1.2.3.5 Subscriber CIV Device Certificates

Subscriber CIV Device Certificates - Name Fields	
Field	Description
version	Present. v3(2)
serialNumber	Present. A non-sequential unique number greater than zero (0) and less than $2^{159}$ containing at least 64 bits of output from a CSPRNG.
signature	See <a href="#">Section 7.1.3.2</a> .
issuer	Encoded value byte-for-byte identical to the encoded subject. See <a href="#">Section 7.1.4.1</a> .
validity	See <a href="#">Section 6.3.2</a> .
Subject Distinguished Name	See <a href="#">Section 7.1.4.3.10</a> Subject Distinguished Name CIV Device Certificates
authorityKeyIdentifier	Present and not marked critical. The keyIdentifier field is present and identical to the subjectKeyIdentifier field of the Issuing CA.
basicConstraints	May be present and marked critical. The cA field is set to false; the pathLenConstraint field is not present.
certificatePolicies	Present and not marked critical. Includes at least one or more policy identifiers as defined in <a href="#">Section 1.2.2</a> . It may include a cPSuri and a User Notice. See <a href="#">Section 7.1.8.1</a> for expected values.

Subscriber CIV Device Certificates - Name Fields	
Field	Description
cRLDistributionPoints	Present and not marked critical. It contains the HTTP URL of the IdenTrust's CRL service.
keyUsage	Present and marked critical. permitted values for RSA public keys are: digitalSignature, keyEncipherment, and dataEncipherment. Permitted values for ECC public keys are digitalSignature and keyAgreement.
subjectAltName	Present and not marked critical. Contains at least one dNSName or iPAddress General Name, or a URI, or an Email Address or OtherName.
extKeyUsage	Present and not marked critical. It contains id-kp-serverAuth and it may contain id-kp-ClientAuth.
authorityInformationAccess	Present and not marked critical. It contains the HTTP URL of the Issuing CA OCSP responder id-ad-ocsp (accessMethod = 1.3.6.1.5.5.7.48.1) and the HTTP URL of the Issuing CA Certificate id-ad-caIssuers (accessMethod= 1.3.6.1.5.5.7.48.2).
subjectKeyIdentifier	May be present and not marked critical. Unique value generated as defined in the <a href="#">RFC 5280 Section 4.2.1.2</a> .
signatureAlgorithm	An encoded value that is byte-for-byte identical to the tbsCertificate.signature.

### 7.1.2.3.6 Subscriber CIV Card Authentication Certificates

These certificates may be issued from the S/MIME Subordinate CA with the appropriate value in the extKeyUsage extension.

Subscriber CIV Card Authentication Certificates - Name Fields	
Field	Description
version	Present. v3(2)
serialNumber	Present. A non-sequential unique number greater than zero (0) and less than $2^{159}$ containing at least 64 bits of output from a CSPRNG.
signature	See <a href="#">Section 7.1.3.2</a> .
issuer	Encoded value byte-for-byte identical to the encoded subject. See <a href="#">Section 7.1.4.1</a> .
validity	See <a href="#">Section 6.3.2</a> .
Subject Distinguished Name	See <a href="#">Section 7.1.4.3.11</a> Subject Distinguished Name CIV Card Authentication Certificates
authorityKeyIdentifier	Present and not marked critical. The keyIdentifier field is present and identical to the subjectKeyIdentifier field of the Issuing CA.
basicConstraints	May be present and marked critical.

Subscriber CIV Card Authentication Certificates - Name Fields	
Field	Description
	The cA field is set to false; the pathLenConstraint field is not present.
certificatePolicies	Present and not marked critical. Includes at least one or more policy identifiers as defined in <a href="#">Section 1.2.2</a> . It may include a cPSuri and a User Notice. See <a href="#">Section 7.1.8.1</a> for expected values.
cRLDistributionPoints	Present and not marked critical. It contains the HTTP URL of the IdenTrust's CRL service.
keyUsage	Present and marked critical. digitalSignature
subjectAltName	Present and not marked critical.
extKeyUsage	Present and not marked critical. It contains id-PIV-cardAuth.
authorityInformationAccess	Present and not marked critical. It contains the HTTP URL of the Issuing CA OCSP responder id-ad-ocsp (accessMethod = 1.3.6.1.5.5.7.48.1) and the HTTP URL of the Issuing CA Certificate id-ad-calssuers (accessMethod= 1.3.6.1.5.5.7.48.2).
subjectKeyIdentifier	Present and not marked critical. Unique value generated as defined in the <a href="#">RFC 5280 Section 4.2.1.2</a> .
signatureAlgorithm	An encoded value that is byte-for-byte identical to the tbsCertificate.signature.

### 7.1.2.3.7 Subscriber Administrative CA and RA Certificates

These certificates may be issued from the S/MIME Subordinate CA with the appropriate value in the extKeyUsage extension.

Subscriber Card Administrative CA and RA Certificates - Name Fields	
Field	Description
version	Present. v3(2)
serialNumber	Present. A non-sequential unique number greater than zero (0) and less than 2 <sup>159</sup> containing at least 64 bits of output from a CSPRNG.
signature	See <a href="#">Section 7.1.3.2</a> .
issuer	Encoded value byte-for-byte identical to the encoded subject. See <a href="#">Section 7.1.4.1</a> .
validity	See <a href="#">Section 6.3.2</a> .
Subject Distinguished Name	commonName: The Personal Name shall contain the name of the Subject. The Personal Name may be presented as subject:givenName and/or subject:surname. The Personal Name shall be a meaningful representation of the Subject's name as verified under <a href="#">Section 3.2.4</a> . organizationName: The organization name or DBA. IdenTrust may include information in this field that differs slightly from the verified name, such as common variations or

### Subscriber Card Administrative CA and RA Certificates - Name Fields

Field	Description
	<p>abbreviations, provided that IdenTrust documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows “Company Name Incorporated”, IdenTrust may use “Company Name Inc.” or “Company Name”.</p> <p>countryName: Present. The two-letter ISO 3161-1 country code for the country.</p> <p>If a Country is not represented by an official ISO 3166-1 country code, IdenTrust specifies the ISO 3166-1 user-assigned code of XX, indicating that an official ISO 3166-1 alpha-2 code has not been assigned.</p>
authorityKeyIdentifier	<p>Present and not marked critical.</p> <p>The keyIdentifier field is present and identical to the subjectKeyIdentifier field of the Issuing CA.</p>
basicConstraints	<p>May be present and marked critical.</p> <p>The cA field is set to false; the pathLenConstraint field is not present.</p>
certificatePolicies	<p>Present and not marked critical.</p> <p>Includes at least one or more policy identifiers as defined in <a href="#">Section 1.2.2</a>. It may include a cPSuri and a User Notice. See <a href="#">Section 7.1.8.1</a> for expected values.</p>
cRLDistributionPoints	<p>Present and not marked critical.</p> <p>It contains the HTTP URL of the IdenTrust’s CRL service.</p>
keyUsage	<p>Present and marked critical.</p> <p>Bit positions for digitalSignature, keyEncipherment, and dataEncipherment are set. The bit position for nonrepudiation may be set.</p>
subjectAltName	<p>Present and not marked critical.</p>
authorityInformationAccess	<p>Present and not marked critical.</p> <p>It contains the HTTP URL of the Issuing CA OCSP responder id-ad-ocsp (accessMethod = 1.3.6.1.5.5.7.48.1) and the HTTP URL of the Issuing CA Certificate id-ad-calssuers (accessMethod= 1.3.6.1.5.5.7.48.2).</p>
subjectKeyIdentifier	<p>Present and not marked critical.</p> <p>Unique value generated as defined in the <a href="#">RFC 5280 Section 4.2.1.2</a>.</p>
signatureAlgorithm	<p>An encoded value that is byte-for-byte identical to the tbsCertificate.signature.</p>

#### 7.1.2.3.8 OCSP Responder Certificates

Root CA certificate: Same as in [Section 7.1.2.1](#).

### OCSP Responder Certificates - Name Fields

Field	Description
version	<p>Present.</p> <p>v3(2)</p>
serialNumber	<p>Present.</p>



OCSP Responder Certificates - Name Fields	
Field	Description
	A non-sequential unique number greater than zero (0) and less than 2 <sup>159</sup> containing at least 64 bits of output from a CSPRNG.
signature	See <a href="#">Section 7.1.3.2</a> .
issuer	Encoded value byte-for-byte identical to the encoded subject. See <a href="#">Section 7.1.4.1</a> .
validity	See <a href="#">Section 6.3.2 - CSA OCSP Responder</a>
Subject Distinguished Name	<p>commonName: Present; the content is an identifier for the certificate such that the certificate's name is unique across all certificates issued by IdenTrust, i.e. "TrustID CA[n] OCSP Signer".</p> <p>organizationName: Present, the CA's name or DBA. IdenTrust may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations, e.g., if the official record shows "Company Name Incorporated", the CA may use "Company Name Inc." or "Company Name".</p> <p>countryName: Present, the two-letter ISO 3161-1 country code for the country.</p>
authorityKeyIdentifier	<p>Present and not marked critical.</p> <p>The keyIdentifier field is present and identical to the subjectKeyIdentifier field of the Issuing CA.</p>
basicConstraints	<p>May be present and marked critical.</p> <p>The cA field is set to false; the pathLenConstraint field is not present.</p>
keyUsage	<p>Present and marked critical.</p> <p>Bit position for digitalSignature is set.</p>
subjectAltName	Present and not marked critical.
extKeyUsage	<p>Present and not marked critical.</p> <p>It contains id-kp-OCSPSigning.</p>
id-pkix-ocsp-nocheck	<p>Present and not marked critical.</p> <p>The value is null.</p>
authorityInformationAccess	<p>Present and not marked critical.</p> <p>It contains the HTTP URL of the Issuing CA OCSP responder id-ad-ocsp (accessMethod = 1.3.6.1.5.5.7.48.1) and the HTTP URL of the Issuing CA Certificate id-ad-caIssuers (accessMethod= 1.3.6.1.5.5.7.48.2).</p>
subjectKeyIdentifier	<p>Present and not marked critical.</p> <p>Unique value generated as defined in the <a href="#">RFC 5280 Section 4.2.1.2</a>.</p>
signatureAlgorithm	An encoded value that is byte-for-byte identical to the tbsCertificate.signature.

#### 7.1.2.4 All Certificates

All fields and extensions are set in accordance with the [RFC 5280](#). IdenTrust does not issue a Certificate that contains a keyUsage flag, extKeyUsage value, Certificate extension, or other data not specified in [Section 7.1.2.2](#), unless IdenTrust is aware of a reason for including the data in the Certificate.

IdenTrust does not issue a Certificate with:

1. Extensions that do not apply in the context of the public Internet (such as an extKeyUsage value for a service that is only valid in the context of a privately managed network), unless:
  - i. such value falls within an OID arc for which the Applicant demonstrates ownership, or
  - ii. the Applicant can otherwise demonstrate the right to assert the data in a public context; or
  - iii. the extension is defined within an open standards specification and intended for use by other organizations. A Certificate that includes such an extension must conform to the specifications of the open standard and of CA/B Forum requirements.
2. Field or extension values which have not been validated according to the processes and procedures described in the CA/B Forum BRs or this CPS.

### **7.1.3 Algorithm Object Identifiers**

#### **7.1.3.1 SubjectPublicKeyInfo**

IdenTrust issues Certificates with the following subjectPublicKeyInfo field attributes:

##### **7.1.3.1.1 RSA**

For RSA Key Pairs, IdenTrust use the RSA key sha256WithRSAEncryption, OID = 1.2.840.113549.1.1.1 algorithm identifier. The parameters must be present and must be an explicit null. IdenTrust does not use a different RSA to indicate an RSA Key.

When encoded, the AlgorithmIdentifier for RSA keys is byte-for-byte identical with the following hex-encoded bytes: 300d06092a864886f70d0101010500.

##### **7.1.3.1.2 ECDSA**

For ECDSA Key Pairs, IdenTrust use an ECDSA key using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters use only one these 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 is 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**

All objects signed by IdenTrust Private Key conform to CA/B F. BR on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.

In particular, it applies to all of the following objects and fields:

- The signatureAlgorithm field of a Certificate or Precertificate.
- The signature field of a TBSCertificate (for example, as used by either a Certificate or Precertificate).
- The signatureAlgorithm field of a CertificateList
- The signature field of a TBSCertList
- The signatureAlgorithm field of a BasicOCSPResponse.

No other encodings are permitted for these fields.

### 7.1.3.2.1 RSA

IdenTrust use one of the following signature algorithms and encodings. When encoded, the AlgorithmIdentifier is 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:

```
304106092a864886f70d01010a3034a00f300d0609608648016503040201
0500a11c301a06092a864886f70d010108300d0609608648016503040201
0500a203020120
```

- RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes:

Encoding:

```
304106092a864886f70d01010a3034a00f300d0609608648016503040202
0500a11c301a06092a864886f70d010108300d0609608648016503040202
0500a203020130
```

- RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes:

Encoding:

```
304106092a864886f70d01010a3034a00f300d0609608648016503040203
0500a11c301a06092a864886f70d010108300d0609608648016503040203
0500a203020140
```

In addition, IdenTrust may use the following signature algorithm and encoding if all of the following conditions are met:

- If used within a Certificate, such as the signatureAlgorithm field of a Certificate or the signature field of a TBSCertificate:
  - The new Certificate is a Root CA Certificate or Subordinate CA Certificate that is a Cross-Certificate; and,
  - There is an existing Certificate, issued by the same issuing CA Certificate, using the following encoding for the signature algorithm; and,
  - The existing Certificate has a unique serialNumber that is at least 64-bits long; and,
  - The only differences between the new Certificate and existing Certificate are one of the following:
    - A new subjectPublicKey within the subjectPublicKeyInfo, using the same algorithm and key size; and/or,
    - A new serialNumber, of the same encoded length as the existing Certificate; and/or
    - The new Certificate's extKeyUsage extension is present, has at least one key purpose specified, and none of the key purposes specified are the id-kp-serverAuth (OID: 1.3.6.1.5.5.7.3.1) or the anyExtendedKeyUsage (OID: 2.5.29.37.0) key purposes; and/or
    - The new Certificate's basicConstraints extension has a pathLenConstraint that is zero.
- If used within an OCSP response, such as the signatureAlgorithm of a BasicOCSPResponse:
  - The producedAt field value of the ResponseData must be earlier than 2022-06-01 00:00:00 UTC; and,

- All unexpired, un-revoked Certificates that contain the Public Key of the CA Key Pair and that have the same Subject Name must also contain an extKeyUsage extension with the only key usage present being the id-kp-ocspSigning (OID: 1.3.6.1.5.5.7.3.9) key usage.
- If used within a CRL, such as the signatureAlgorithm field of a CertificateList or the signature field of a TBSCertList:
  - The CRL is referenced by one or more Root CA or Subordinate CA Certificates; and,
  - The Root CA or Subordinate CA Certificate has been issued one or more Certificates using the following encoding for the signature algorithm.

### 7.1.3.2.2 ECDSA

IdenTrust uses 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

### 7.1.4.1 Name Encoding for CAs

For every valid Certification Path (as defined by [RFC 5280, Section 6](#)):

- For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate shall be byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA Certificate.
- For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate shall be byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to [RFC 5280, Section 7.1](#), and including expired and revoked Certificates.

When encoding a Name, IdenTrust ensures that:

- Each Name contains an RDNSSequence.
- Each RelativeDistinguishedName contains exactly one AttributeTypeAndValue.
- Each RelativeDistinguishedName, if present, is encoded within the RDNSSequence in the order that it appears in the following [Section 7.1.4.2](#).
- Each Name must not contain more than one instance of a given AttributeTypeAndValue across all RelativeDistinguishedNames unless explicitly allowed in the CA/B Forum BRs.

### 7.1.4.2 Subject Attribute Encoding

By issuing the Certificate, the IdenTrust CA represents that it followed the procedure set forth in the TrustID CP and this CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

Subject attributes shall not contain only metadata such as ' ', '-', and ' ' (i.e., space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

### 7.1.4.2.1 Subscriber S/MIME Certificates

#### 7.1.4.2.1.1 Subscriber S/MIME Subject DN Attributes for Mailbox-Validated Profile

Subject Attribute Encoding S/MIME Mailbox-Validated Profile		
Attribute	Multipurpose	Strict
commonName	May	May
organizationName	Shall not	Shall not
organizationalUnitName	Shall not	Shall not
organizationIdentifier	Shall not	Shall not
givenName	Shall not	Shall not
Surname	Shall not	Shall not
Pseudonym	Shall not	Shall not
serialNumber	May	May
emailAddress	May	May
Title	Shall not	Shall not
streetAddress	Shall not	Shall not
localityName	Shall not	Shall not
stateOrProvinceName	Shall not	Shall not
postalCode	Shall not	Shall not
countryName	Shall not	Shall not
Other	Shall not	Shall not

#### 7.1.4.2.1.2 Subscriber S/MIME Subject DN Attributes for Organization-Validated Profile

Subject Attribute Encoding S/MIME Organization-Validated Profile		
Attribute	Multipurpose	Strict
commonName	May	May
organizationName	Shall	Shall
organizationalUnitName	May	May
organizationIdentifier	Shall	Shall
givenName	Shall not	Shall not
Surname	Shall not	Shall not
Pseudonym	Shall not	Shall not
serialNumber	May	May
emailAddress	May	May
Title	Shall not	Shall not

Subject Attribute Encoding S/MIME Organization-Validated Profile		
Attribute	Multipurpose	Strict
streetAddress	May	Shall not
localityName	May	May
stateOrProvinceName	May	May
postalCode	May	Shall not
countryName	May	May
Other	Shall not	Shall not

#### 7.1.4.2.1.3 Subscriber S/MIME Subject DN Attributes for Sponsor-Validated Profile

Subject Attribute Encoding S/MIME Sponsor-Validated Profile		
Attribute	Multipurpose (See Note)	Strict (See Note)
commonName	May	May
organizationName	Shall	Shall
organizationalUnitName	May	May
organizationIdentifier	Shall	Shall
givenName	May	May
Surname	May	May
Pseudonym	May	May
serialNumber	May	May
emailAddress	May	May
Title	May	May
streetAddress	May	Shall not
localityName	May	May
stateOrProvinceName	May	May
postalCode	May	Shall not
countryName	May	May
Other	Shall not	Shall not

**Note:** Multipurpose and Strict Generation profiles shall include either subject:givenName and/or subject:surname, or the subject:pseudonym.

#### 7.1.4.2.1.4 Subscriber S/MIME Subject DN Attributes for Individual-Validated Profile

Subject Attribute Encoding S/MIME Individual-Validated Profile		
Attribute	Multipurpose (See Note)	Strict (See Note)
commonName	May	May

Subject Attribute Encoding S/MIME Individual-Validated Profile		
Attribute	Multipurpose (See Note)	Strict (See Note)
organizationName	May	Shall not
organizationalUnitName	May	Shall not
organizationIdentifier	May	Shall not
givenName	May	May
Surname	May	May
Pseudonym	May	May
serialNumber	May	May
emailAddress	May	May
Title	May	May
streetAddress	May	Shall not
localityName	May	May
stateOrProvinceName	May	May
postalCode	May	Shall not
countryName	May	May
Other	May	Shall not

#### 7.1.4.2.2 Subscriber Server Certificates Subject DN Attributes

When IdenTrust includes attributes in the Certificate subject field that are listed in the table below, those attributes are encoded in the relative order as they appear in the table and follow the specified encoding requirements for the attribute.

Subject Attribute Encoding OV Server Certificates				
Attribute	OID	Specification	Encoding Requirements	Max Length <sup>6</sup>
domainComponent	0.9.2342.19200300.100.1.25	<a href="#">RFC 4519</a>	IA5String	63
countryName	2.5.4.6	<a href="#">RFC 5280</a>	PrintableString	2
stateOrProvinceName	2.5.4.8	<a href="#">RFC 5280</a>	UTF8String or PrintableString	128
localityName	2.5.4.7	<a href="#">RFC 5280</a>	UTF8String or PrintableString	128
organizationName	2.5.4.10	<a href="#">RFC 5280</a>	UTF8String or PrintableString	64
commonName	2.5.4.3	<a href="#">RFC 5280</a>	UTF8String or PrintableString	64

Encoding and other requirements for selected attributes.

<sup>6</sup> ASN.1 length limits for DirectoryString are expressed as character limits, not byte limits

When IdenTrust includes attributes in the Certificate subject field that are listed in the table below, those attributes are encoded in the relative order as they appear in the table and follow the specified encoding requirements for the attribute.

Subject Attribute Encoding EV Server Certificates				
Attribute	OID	Specification	Encoding Requirements	Max Length <sup>7</sup>
businessCategory	2.5.4.15	X.520	UTF8String or PrintableString	128
jurisdictionCountry	1.3.6.1.4.1.311.60.2.1.3	<a href="#">EV TLS BR</a>	PrintableString	2
jurisdictionStateOrProvince	1.3.6.1.4.1.311.60.2.1.2	<a href="#">EV TLS BR</a>	UTF8String or PrintableString	128
jurisdictionLocality	1.3.6.1.4.1.311.60.2.1.1	<a href="#">EV TLS BR</a>	UTF8String or PrintableString	128
serialNumber	2.5.4.5	<a href="#">RFC 5280</a>	PrintableString	64

### 7.1.4.2.3 Subscriber Code Signing Certificates Subject DN Attributes

Subject Attribute Encoding Non-EV Code Signing Certificates				
Attribute	OID	Specification	Encoding Requirements	Max Length <sup>8</sup>
countryName	2.5.4.6	<a href="#">RFC 5280</a>	PrintableString	2
stateOrProvinceName	2.5.4.8	<a href="#">RFC 5280</a>	UTF8String or PrintableString	128
localityName	2.5.4.7	<a href="#">RFC 5280</a>	UTF8String or PrintableString	128
organizationName	2.5.4.10	<a href="#">RFC 5280</a>	UTF8String or PrintableString	64
commonName	2.5.4.3	<a href="#">RFC 5280</a>	UTF8String or PrintableString	64

Subject Attribute Encoding EV Code Signing Certificates				
Attribute	OID	Specification	Encoding Requirements	Max Length <sup>9</sup>
businessCategory	2.5.4.15	X.520	UTF8String or PrintableString	128
jurisdictionCountry	1.3.6.1.4.1.311.60.2.1.3	<a href="#">EV TLS BR</a>	PrintableString	2
jurisdictionStateOrProvince	1.3.6.1.4.1.311.60.2.1.2	<a href="#">EV TLS BR</a>	UTF8String or PrintableString	128
jurisdictionLocality	1.3.6.1.4.1.311.60.2.1.1	<a href="#">EV TLS BR</a>	UTF8String or PrintableString	128
serialNumber	2.5.4.5	<a href="#">RFC 5280</a>	PrintableString	64

<sup>7</sup> ASN.1 length limits for DirectoryString are expressed as character limits, not byte limits

<sup>8</sup> ASN.1 length limits for DirectoryString are expressed as character limits, not byte limits

<sup>9</sup> ASN.1 length limits for DirectoryString are expressed as character limits, not byte limits



#### 7.1.4.2.4 Subscriber Timestamping and CIV Device Certificates

Subject Attribute Encoding Timestamping and CIV Device Certificates				
Attribute	OID	Specification	Encoding Requirements	Max Length <sup>9</sup>
commonName	2.5.4.3	<a href="#">RFC 5280</a>	UTF8String or PrintableString	64
organizationalUnitName	2.5.4.11	<a href="#">RFC 5280</a>	UTF8String or PrintableString	64
organizationName	2.5.4.10	<a href="#">RFC 5280</a>	UTF8String or PrintableString	64
countryName	2.5.4.6	<a href="#">RFC 5280</a>	PrintableString	2

#### 7.1.4.3 Subject Distinguished Name Fields

##### 7.1.4.3.1 Subject Distinguished Name – Root Certificates

Subject Distinguished Name – Root CA Certificates	
Field	Contents
countryName (OID: 2.5.4.6)	The two-letter ISO 3161-1 country code for the country
organizationName (OID: 2.5.4.10)	Present. The name of organization owner of the Root CA, i.e. "IdenTrust".
commonName (OID 2.5.4.3)	Present. The content is an identifier for the certificate such that the certificate's name is unique across all certificates issued by IdenTrust, i.e. "IdenTrust Commercial Root CA 1".

##### 7.1.4.3.2 Subject Distinguished Name – Subordinate CA Certificates

Subject Distinguished Name – Subordinate CA Certificates	
Field	Contents
commonName (OID 2.5.4.3)	Present. The content is an identifier for the certificate such that the certificate's name is unique across all certificates issued by IdenTrust,
organizationName (OID 2.5.4.10)	Present. The CA's name or DBA. IdenTrust may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations, e.g., if the official record shows "Company Name Incorporated", the CA may use "Company Name Inc." or "Company Name".
countryName (OID: 2.5.4.6)	Present. The two-letter ISO 3161-1 country code for the country.

##### 7.1.4.3.3 Subject Distinguished Name – Subscriber S/MIME Certificates

Subject Distinguished Name – Subscriber S/MIME Certificate Fields	
Field	Contents
commonName (OID: 2.5.4.3)	<b>Mailbox-Validated:</b> Validated Email Address If present, the Mailbox Address contains a rfc822Name or otherName value of type id-on-SmtpUTF8Mailbox from extensions:subjectAltName.

Subject Distinguished Name – Subscriber S/MIME Certificate Fields	
Field	Contents
	<p><b>Organization-Validated:</b> organizationName or Email Address</p> <p><b>Sponsor-Validated:</b> Personal Name or Email Address</p> <p><b>Individual-Validated:</b> Personal Name or Email Address</p> <p>If present, the Personal Name contains the name of the Subject. The Personal Name is presented as subject:givenName and/or subject:surname.</p> <p>If the subject:commonName contains a Pseudonym, then the subject:givenName and/or subject:surname attributes shall not be present. If present, the Pseudonym shall contain the subject:pseudonym if that Subject attribute is also present. If the subject:commonName contains a Personal Name, then the subject:pseudonym attribute shall not be present.</p>
organizationName (OID: 2.5.4.10)	Present in Organization-Validated or Sponsor-Validated Certificates. Contains the Subject’s full legal organization name or DBA verified in accordance with the requirements of <a href="#">Section 3.2.2.2</a> . IdenTrust may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that IdenTrust documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows “Company Name Incorporated”, IdenTrust may use “Company Name Inc.” or “Company Name”.
organizationalUnitName (OID: 2.5.4.11)	May be present. If present, IdenTrust confirms that the subject:organizationalUnitName is the full legal organization name of an Affiliate of the organizationName in the Certificate and has been verified in accordance with the requirements of <a href="#">Section 3.2.2.2</a> .
organizationIdentifier (OID: 2.5.4.97)	Present in Organization-Validated or Sponsor-Validated Certificates. Contains a Registration Reference for a Legal Entity assigned in accordance to the identified Registration Scheme. See additional syntax requirements in <a href="#">Section 7.1.4.2.2 Subject distinguished name fields (d) of the S/MIME BR</a> .
givenName (OID: 2.5.4.42) and/or surname (OID: 2.5.4.4)	If present, the subject:givenName field and subject:surname field contains a Natural Person Subject’s name as verified under <a href="#">Section 3.2.4</a> . Subjects with a single legal name shall provide the name in the subject:surname attribute.
localityName (OID: 2.5.4.7)	Is present if stateOrProvinceName is absent; may be present otherwise. If present, contains the Subject’s verified locality information. This field shall only be used if the subject:countryName field is present.
stateOrProvinceName (OID: 2.5.4.8)	Is present if localityName is absent; may be present otherwise. If present, contains the Subject’s verified state or province information. This field shall only be used if the subject:countryName field is present.
countryName (OID: 2.5.4.6)	Present. The two-letter ISO 3161-1 country code for the country. If a Country is not represented by an official ISO 3166-1 country code, IdenTrust specifies the ISO 3166-1 user-assigned code of XX, indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

#### 7.1.4.3.4 Subject Distinguished Name Subscriber DV Server Certificates

Subject Distinguished Name – Subscriber DV Server Certificate Fields	
Field	Contents
commonName (OID: 2.5.4.3)	May be present; If present, contains exactly one entry that is one of the values contained in the subjectAltName extension encoded as follows:

Subject Distinguished Name – Subscriber DV Server Certificate Fields	
Field	Contents
	<ul style="list-style-type: none"> <li>If the value is an IPv4 address, then the value must be encoded as an IPv4Address as specified in the <a href="#">RFC 3986, Section 3.2.2</a>.</li> <li>If the value is an IPv6 address, then the value must be encoded in the text representation specified in the <a href="#">RFC 5952, Section 4</a>.</li> <li>If the value is a Fully-Qualified Domain Name or Wildcard Domain Name, then the value must be encoded as a character-for-character copy of the dNSName entry value from the subjectAltName extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name must be encoded as LDH Labels, and P-Labels must not be converted to their Unicode representation.</li> </ul> <p>Subject attributes must not contain only metadata such as ‘.’, ‘-’, and ‘ ’ (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.</p>
countryName (OID: 2.5.4.6)	<p>May be present. The two-letter ISO 3161-1 country code for the country.</p> <p>If a Country is not represented by an official ISO 3166-1 country code, IdenTrust specifies the ISO 3166-1 user-assigned code of XX, indicating that an official ISO 3166-1 alpha-2 code has not been assigned.</p>

#### 7.1.4.3.5 Subject Distinguished Name Subscriber OV Server Certificates

Attributes appear within the subject field of Subscriber OV server Certificates in this relative order:

Subject Distinguished Name – Subscriber OV Server Certificate Fields	
Field	Contents
domainComponent 0.9.2342.19200300.100.1.25	<p>May be present. If present, this field contains a Domain Label from a Domain Name. The domainComponent fields for the Domain Name are in a single ordered sequence containing all Domain Labels from the Domain Name. The Domain Labels are encoded in the reverse order to the on-wire representation of domain names in the DNS protocol, so that the Domain Label closest to the root is encoded first. Multiple instances may be present</p>
countryName (OID: 2.5.4.6)	<p>Present. The two-letter ISO 3161-1 country code for the country.</p> <p>If a Country is not represented by an official ISO 3166-1 country code, IdenTrust specifies the ISO 3166-1 user-assigned code of XX, indicating that an official ISO 3166-1 alpha-2 code has not been assigned.</p>
stateOrProvinceName (OID: 2.5.4.8)	<p>Is present if localityName is absent; may be present otherwise. If present, contains the Subject’s verified state or province information.</p>
localityName (OID: 2.5.4.7)	<p>Is present if stateOrProvinceName is absent; may be present otherwise. If present, contains the Subject’s verified locality information.</p>
organizationName (OID: 2.5.4.10)	<p>Present. This field contains the Subject’s name and/or DBA/tradename. IdenTrust may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that IdenTrust documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows “Company Name Incorporated”, IdenTrust may use “Company Name Inc.” or “Company Name”. If both are included, the DBA/tradename shall appear first, followed by the Subject’s name in parentheses.</p>

Subject Distinguished Name – Subscriber OV Server Certificate Fields	
Field	Contents
commonName (OID: 2.5.4.3)	<p>May be present; If present, contains exactly one entry that is one of the values contained in the subjectAltName extension encoded as follows:</p> <ul style="list-style-type: none"> <li>• If the value is an IPv4 address, then the value must be encoded as an IPv4Address as specified in the <a href="#">RFC 3986, Section 3.2.2</a>.</li> <li>• If the value is an IPv6 address, then the value must be encoded in the text representation specified in the <a href="#">RFC 5952, Section 4</a>.</li> <li>• If the value is a Fully-Qualified Domain Name or Wildcard Domain Name, then the value must be encoded as a character-for-character copy of the dNSName entry value from the subjectAltName extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name must be encoded as LDH Labels, and P-Labels must not be converted to their Unicode representation.</li> </ul> <p>Subject attributes must not contain only metadata such as ‘, ‘-’, and ‘ ’ (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.</p>

#### 7.1.4.3.6 Subject Distinguished Name - Subscriber EV Server Certificates

Subject Distinguished Name – Subscriber EV Server Certificate Fields	
Field	Contents
Jurisdiction of Incorporation or Registration fields	<p><b>Country</b> (OID: 1.3.6.1.4.1.311.60.2.1.3) – Present: &lt;Verified ISO country code of incorporation of the sponsoring organization&gt;.</p> <p><b>State or Province</b> (OID: 1.3.6.1.4.1.311.60.2.1.2) - May be present: &lt;Verified state or province of incorporation of sponsoring organization &gt;<b>Locality</b> (OID: 1.6.1.4.1.311.60.2.1.1) - May be present: &lt;Verified city of incorporation of the sponsoring organization &gt;.</p>
businessCategory (OID: 2.5.4.15)	<p>Present.</p> <p>This field must contain one of the following strings: “Private Organization”, “Government Entity”, “Business Entity”, or “Non-Commercial Entity” depending upon whether the Subject qualifies under the terms of <a href="#">Section 4.1.1 of EV TLS BR</a>.</p>
serialNumber (OID: 2.5.4.5)	<p>Present.</p> <p>For Private Organizations, this field contains the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration shall be entered into this field in any one of the common date formats.</p> <p>For Government Entities that do not have a Registration Number or readily verifiable date of creation, IdenTrust enters appropriate language to indicate that the Subject is a Government Entity.</p> <p>For Business Entities, the Registration Number that was received by the Business Entity upon government registration is entered in this field. For those Business entities that register with an Incorporating Agency or Registration Agency in a jurisdiction that does not issue numbers pursuant to government registration, the date of the registration is entered into this field in any one of the common date formats.</p>
countryName (OID: 2.5.4.6)	<p>Present. The two-letter ISO 3161-1 country code for the country.</p>

Subject Distinguished Name – Subscriber EV Server Certificate Fields	
Field	Contents
	If a Country is not represented by an official ISO 3166-1 country code, IdenTrust specifies the ISO 3166-1 user-assigned code of XX, indicating that an official ISO 3166-1 alpha-2 code has not been assigned.
stateOrProvinceName (OID: 2.5.4.8)	Is present if localityName is absent; may be present otherwise. If present, contains the Subject’s verified state or province information.
localityName (OID: 2.5.4.7)	Is present if stateOrProvinceName is absent; may be present otherwise. If present, contains the Subject’s verified locality information.
organizationName (OID: 2.5.4.10)	<p>Present. This field contains the Subject’s full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject’s Jurisdiction of Incorporation or Registration or as otherwise verified by IdenTrust as provided herein. IdenTrust abbreviate the organization prefixes or suffixes in the organization name, e.g., if the official record shows “Company Name Incorporated” IdenTrust may include “Company Name, Inc.” When abbreviating a Subject’s full legal name as allowed by this subsection, IdenTrust will use abbreviations that are not misleading in the Jurisdiction of Incorporation or Registration. In addition, an assumed name or DBA name used by the Subject may be included at the beginning of this field, provided that it is followed by the full legal organization name in parenthesis.</p> <p>If the combination of names or the organization name by itself exceeds 64 characters, the IdenTrust may abbreviate parts of the organization name, and/or omit non-material words in the organization name in such a way that the text in this field does not exceed the 64-character limit; provided that IdenTrust checks this field in accordance with <a href="#">Section 7.1.2.21 of the EV TLS BR</a> and a Relying Party will not be misled into thinking that they are dealing with a different organization. In cases where this is not possible, IdenTrust will not issue the EV Server Certificate.</p>
commonName (OID: 2.5.4.3)	May be present; If present, this field must contain a single Domain Name owned or controlled by the Subject and to be associated with the Subject’s server.

#### 7.1.4.3.7 Subject Distinguished Name - Subscriber Non-EV Code Signing Certificates

Subject Distinguished Name – Subscriber Non-EV Code Signing Certificate Fields	
Field	Contents
Common Name (OID: 2.5.4.3)	Present, the verified legal name of the Sponsoring Organization as verified under <a href="#">Section 3.2.2.2</a> .
organizationalUnitName (OID: 2.5.4.11)	May be present. If present, IdenTrust confirms that the subject:organizationalUnitName is the full legal organization name of an Affiliate of the organizationName in the Certificate and has been verified in accordance with the requirements of <a href="#">Section 3.2.2.2</a> .
organizationName (OID: 2.5.4.10)	Present. The Subject’s name or DBA verified in accordance with the requirements of <a href="#">Section 3.2.2.2</a> . IdenTrust may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that IdenTrust documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows “Company Name Incorporated”, IdenTrust may use “Company Name Inc.” or “Company Name”.
serialNumber	May be present. For Private Organizations, this field must contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in

Subject Distinguished Name – Subscriber Non-EV Code Signing Certificate Fields	
Field	Contents
(OID: 2.5.4.5)	<p>its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration shall be entered into this field in any one of the common date formats.</p> <p>For Government Entities that do not have a Registration Number or readily verifiable date of creation, IdenTrust enters appropriate language to indicate that the Subject is a Government Entity.</p> <p>For Business Entities, the Registration Number that was received by the Business Entity upon government registration is entered in this field. For those Business entities that register with an Incorporating Agency or Registration Agency in a jurisdiction that does not issue numbers pursuant to government registration, the date of the registration is entered into this field in any one of the common date formats.</p>
localityName (OID: 2.5.4.7)	Is present if stateOrProvinceName is absent; may be present otherwise. If present, contains the Subject’s verified locality information.
stateOrProvinceName (OID: 2.5.4.8)	Is present if localityName is absent; may be present otherwise. If present, contains the Subject’s verified state or province information.
countryName (OID: 2.5.4.6)	<p>Present. The two-letter ISO 3161-1 country code for the country.</p> <p>If a Country is not represented by an official ISO 3166-1 country code, IdenTrust specifies the ISO 3166-1 user-assigned code of XX, indicating that an official ISO 3166-1 alpha-2 code has not been assigned.</p>

#### 7.1.4.3.8 Subject Distinguished Name Subscriber EV Code Signing Certificates

Subject Distinguished Name – Subscriber EV Code Signing Certificate Fields	
Field	Contents
Common Name (OID: 2.5.4.3)	Present, the verified legal name of the Sponsoring Organization as verified under <a href="#">Section 3.2.2.2</a> .
organizationalUnitName (OID: 2.5.4.11)	May be present. If present, IdenTrust confirms that the subject:organizationalUnitName is the full legal organization name of an Affiliate of the organizationName in the Certificate and has been verified in accordance with the requirements of <a href="#">Section 3.2.2.2</a> .
organizationName (OID: 2.5.4.10)	Present. The Subject’s name or DBA verified per <a href="#">Section 3.2.2.2 of the EV TLS BR</a> . IdenTrust may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that IdenTrust documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows “Company Name Incorporated”, IdenTrust may use “Company Name Inc.” or “Company Name”.
businessCategory (OID: 2.5.4.15)	Present. This field must contain one of the following strings: “Private Organization”, “Government Entity”, “Business Entity”, or “Non-Commercial Entity” depending upon whether the Subject qualifies under the terms of <a href="#">Section 4.1.1 of the EV TLS BR</a> .
Jurisdiction of Incorporation or Registration fields	<p><b>jurisdictionCountryName</b> (OID: 1.3.6.1.4.1.311.60.2.1.3) – Present: &lt;Verified ISO country code of incorporation of the sponsoring organization&gt;.</p> <p><b>jurisdictionStateOrProvinceName</b> (OID: 1.3.6.1.4.1.311.60.2.1.2) - May be present: &lt;Verified state or province of incorporation of sponsoring organization &gt;</p>

Subject Distinguished Name – Subscriber EV Code Signing Certificate Fields	
Field	Contents
	<p><b>jurisdictionLocalityName</b> (OID: 1.3.6.1.4.1.311.60.2.1.1) - May be present: &lt;Verified city of incorporation of the sponsoring organization &gt;.</p> <p>These fields must not contain information that is not relevant to the level of the incorporating agency or Registration Agency.</p>
serialNumber (OID: 2.5.4.5)	<p>Present. For Private Organizations, this field must contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration shall be entered into this field in any one of the common date formats.</p> <p>For Government Entities that do not have a Registration Number or readily verifiable date of creation, IdenTrust enters appropriate language to indicate that the Subject is a Government Entity.</p> <p>For Business Entities, the Registration Number that was received by the Business Entity upon government registration is entered in this field. For those Business entities that register with an Incorporating Agency or Registration Agency in a jurisdiction that does not issue numbers pursuant to government registration, the date of the registration is entered into this field in any one of the common date formats.</p>

#### 7.1.4.3.9 Subject Distinguished Name - Time-Stamping Certificates

Subject Distinguished Name – Subscriber Time-Stamping Certificate Fields	
Field	Contents
commonName (OID: 2.5.4.3)	TrustID Timestamp Authority[x] x= a unique number i.e.
organizationName (OID: 2.5.4.10)	IdenTrust
countryName (OID: 2.5.4.6)	The two-letter ISO 3161-1 country code for the country

#### 7.1.4.3.10 Subject Distinguished Name - Subscriber CIV Device Certificates

Subject Distinguished Name – Subscriber CIV Device Certificate Fields	
Field	Contents
commonName (OID: 2.5.4.3)	A unique name that identifies the device.
serialNumber (OID: 2.5.4.5)	The subject:serialNumber may be used to contain a unique identifier assigned by IdenTrust or RA to identify and/or to disambiguate the Subscriber
organizationalUnitName (OID: 2.5.4.11)	May be present. If present, IdenTrust confirms that the subject:organizationalUnitName is the full legal organization name of an Affiliate of the organizationName in the Certificate and has been verified in accordance with the requirements of <a href="#">Section 3.2.3</a> .
organizationName (OID: 2.5.4.10)	May be present. The device’s organization name or DBA. IdenTrust may include information in this field that differs slightly from the verified name, such as common



Subject Distinguished Name – Subscriber CIV Device Certificate Fields	
Field	Contents
	variations or abbreviations, provided that IdenTrust documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows “Company Name Incorporated”, IdenTrust may use “Company Name Inc.” or “Company Name”.
countryName (OID: 2.5.4.6)	Present. The two-letter ISO 3161-1 country code for the country.  If a Country is not represented by an official ISO 3166-1 country code, IdenTrust specifies the ISO 3166-1 user-assigned code of XX, indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

#### 7.1.4.3.11 Subject Distinguished Name - Subscriber CIV Card Authentication Certificates

Subject Distinguished Name – Subscriber CIV Card Authentication Certificate Fields	
Field	Contents
commonName (OID: 2.5.4.3)	The Personal Name shall contain the name of the Subject. The Personal Name may be presented as subject:givenName and/or subject:surname. The Personal Name shall be a meaningful representation of the Subject’s name as verified under <a href="#">Section 3.2.4</a> .
serialNumber (OID: 2.5.4.5)	The subject:serialNumber may be used to contain a unique identifier assigned by IdenTrust or RA to identify and/or to disambiguate the Subscriber
organizationalUnitName (OID: 2.5.4.11)	May be present. If present, IdenTrust confirms that the subject:organizationalUnitName is the full legal organization name of an Affiliate of the organizationName in the Certificate and has been verified in accordance with the requirements of <a href="#">Section 3.2.3</a> .
organizationName (OID: 2.5.4.10)	May be present. The device’s organization name or DBA. IdenTrust may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that IdenTrust documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows “Company Name Incorporated”, IdenTrust may use “Company Name Inc.” or “Company Name”.
countryName (OID: 2.5.4.6)	Present. The two-letter ISO 3161-1 country code for the country.  If a Country is not represented by an official ISO 3166-1 country code, IdenTrust specifies the ISO 3166-1 user-assigned code of XX, indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

#### 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.

For a Subordinate CA Certificate to be considered Technically Constrained, the Certificate includes an Extended Key Usage (EKU) extension specifying all extended key usages for which the Subordinate CA Certificate is authorized to issue Certificates. The anyExtendedKeyUsage KeyPurposeId does not appear within this extension.

In the case of Subordinate CA Certificates, for which the associated Private Key is under the control of an Issuing CA other than IdenTrust and that issues server Certificates, IdenTrust will include both the Name Constraint and Extended Key Usage extensions in the Subordinate CA Certificate.



When issuing a Subordinate CA Certificate, IdenTrust conducts a scripted Key Generation ceremony that encompasses all procedures set forth in the TrustID CP and this CPS. The Key Generation Script is compiled by using the Subordinate CA Certificate Profile to define all attributes, including Subject Information, to be included in the Subordinate CA Certificate. Verification of Subject Information for accuracy is completed before the Subordinate CA Certificate Issuance.

For server Certificates, the Certificate's Extended Key Usage extension will, at a minimum, contain the id-kp-serverAuth and may contain the id-kp-clientAuth.

If the Subordinate CA Certificate includes the id-kp-emailProtection extended key usage, then for the subordinate CA Certificate to be considered Technically Constrained it shall include the nameConstraints X.509v3 extension with constraints on rfc822Name and directoryName as follows:

1. For each rfc822Name in permittedSubtrees, each rfc822Name shall contain either a FQDN or a U+002E FULL STOP (".") character followed by a FQDN. The rfc822Name shall not contain an email address. IdenTrust confirms that the Applicant has registered the FQDN contained in the rfc822Name or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of [Section 3.2.2.3](#).
2. For each directoryName in permittedSubtrees, IdenTrust confirm the Applicant's and/or Subsidiary's Organizational name and location such that end entity Certificates issued from the Subordinate CA Certificate will be in compliance with [Section 7.1.2.4 of the TLS BR](#).

The Certificate's Name Constraint extension will include constraints on dNS Name, iPAddress, and/or DirectoryName. The constraints are specific to the Issuing CA and are documented in the Certificate Profile.

If the Subordinate CA Certificate is not allowed to issue Certificates with an iPAddress, then the Subordinate CA Certificate will specify the entire Ipv4 and Ipv6 address ranges in excludedSubtrees. The Subordinate CA Certificate will include within 'excludedSubtrees' an iPAddress 'GeneralName' of 8 zero octets (covering the Ipv4 address range of 0.0.0.0/0). The Subordinate CA Certificate will also include within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the Ipv6 address range of::0/0). Otherwise, the Subordinate CA Certificate will include at least one iPAddress in permitted subtrees.

All IdenTrust Subordinate CA's issued from IdenTrust publicly trusted roots per MRSP within 7 days after Issuance and before the Subordinate CA is allowed to issue Certificates.

### **7.1.6 Certificate Policy Object Identifier**

IdenTrust CA and Subscriber Certificates issued under this CPS shall assert at least one or more of the policy OIDs listed in [Section 1.2.2](#).

### **7.1.7 Usage of Policy Constraints Extension**

The Policy constraints extension in Certificates issued by the Root CA Certificates to Subordinate CA Certificates is not populated.

### **7.1.8 Policy Qualifiers Syntax and Semantics**

Certificates not subject to the CA/B Forum BR with a Policy qualifier in the Certificate Policies extensions may contain a User Notice that incorporates this CPS by reference and makes this CPS binding on all Participants, including any potential Relying Party. By using or otherwise relying on a Certificate, the Relying Party accepts and consents to not only the language in the User Notice, but also to the applicability of this CPS including limitations of liability, disclaimers of warranties, applicable law, and other notices and disclosures made herein that may be determined to have been necessarily made within the Certificate.

### 7.1.8.1 Policy Qualifiers

If present, Policy qualifiers are populated as follows:

<b>[2]</b> <b>Certificate Policy:</b>	Policy Qualifier Id=CPS Qualifier: <a href="https://secure.identrust.com/Certificates/policy/ts/">https://secure.identrust.com/Certificates/policy/ts/</a>
<b>[1,2]</b> <b>Policy Qualifier Info:</b>	Policy Qualifier Id=User Notice <sup>10</sup> Qualifier: Notice Text=This TrustID Certificate has been issued in accordance with IdenTrust’s TrustID Certificate Policy found at: <a href="https://secure.identrust.com/Certificates/policy/ts/">https://secure.identrust.com/Certificates/policy/ts/</a>

### 7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The Certificate Policies extension indicates that the use of the Certificate is restricted to one of the identified Certificate Policies and the Certificate must only be used in accordance with the provisions of at least one of the listed CPs.

IdenTrust shall have no liability for damages asserted by anyone who has used the Certificate for an inappropriate purpose or in an inappropriate manner, as stipulated in the TrustID CP.

### 7.1.10 Inhibit Any Policy Extension

IdenTrust may assert InhibitAnyPolicy in CA Certificates. When used, the extension is not marked critical, to support legacy applications that cannot process InhibitAnyPolicy.subjectKeyidentifier

## 7.2 CRL PROFILE

CRLs issued by IdenTrust comply with the following CRL profile, which incorporates, and is derived from the [RFC 5280](#). Except as explicitly noted, all normative requirements imposed by the [RFC 5280](#) shall apply, in addition to the normative requirements imposed by the TLS BR.

A full and complete CRL is a CRL whose scope includes all Certificates issued by the CA.

A partitioned CRL (sometimes referred to as a “sharded CRL”) is a CRL with a constrained scope, such as all Certificates issued by IdenTrust during a certain period of time (“temporal sharding”). Aside from the presence of the Issuing Distribution Point extension (OID 2.5.29.28) in partitioned CRLs, both CRL formats are syntactically the same from the perspective of this profile.

Minimally, IdenTrust issues either a “full and complete” CRL or a set of “partitioned” CRLs which cover the complete set of Certificates issued by IdenTrust. When issuing only partitioned CRLs, the combined scope of those CRLs must be equivalent to that of a full and complete CRL.

IdenTrust does not issue indirect CRLs (i.e., the issuer of the CRL is not the issuer of all Certificates that are included in the scope of the CRL).

For Code Signing and Time-Stamping Certificates, the serial number of a revoked Certificate must remain on the CRL for at least 10 years after the expiration of the Certificate. Application Software Suppliers may require

---

<sup>10</sup> The User Notice Policy Qualifier is not present on Server CA or Server Subscriber Certificates issued post September 15, 2023.

IdenTrust to support a longer life-time in its contract. If a Code Signing Certificate contains the Lifetime Signing OID, the Code Signature becomes invalid when the Code Signing Certificate expires, even if the Code Signature is timestamped. Because the Lifetime Signing OID is intended to be used with test purposes only, IdenTrust may cease maintaining revocation information for a Code Signing Certificate with the Lifetime Signing OID after the Code Signing Certificate expires.

If a Code Signing Certificate previously has been revoked, and IdenTrust later becomes aware of a more appropriate revocation date, then IdenTrust may use that revocation date in subsequent CRL entries for that Code Signing Certificate.

### 7.2.1 Version Number(s)

IdenTrust issues X.509 version two (2) CRLs (i.e., populated with integer “1”). CRLs conform to the [RFC 5280](#) and applicable subsequent updates via [RFC 6818](#); these CRLs may contain the basic fields and contents specified below:

Signature Algorithm	sha256WithRSAEncryption, OID = 1.2.840.113549.1.1.11
---------------------	------------------------------------------------------

The correct signature algorithm depends on the algorithm used to sign the associated CA in accordance with [Section 6.1.5](#).

Field	Value
Issuer	DN of issuer of CRL
thisUpdate	Issue date of the CRL in UTC format
nextUpdate	Date by which next CRL will be issued in UTC format
Revoked Certificates List	List of revoked Certificates, including the serial number, revocation date and revocation reason code.
Issuer’s Signature	[Signature]

### 7.2.2 CRL and CRL Entry Extensions

IdenTrust CRLs comply with Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile.

CRL and CRL Entry Extensions	
Field	Value
authorityKeyIdentifier	Present and not marked critical. The keyIdentifier field is present and identical to the subjectKeyIdentifier field of the Issuing CA.
CLRNumber	Present and not marked critical. An integer greater than or equal to zero (0) and less than $2^{159}$ and convey a strictly increasing sequence.

Revoked Certificates Component	
Field	Value
serialNumber	Present. Must be byte-for-byte identical to the serialNumber contained in the revoked certificate.

Revoked Certificates Component	
Field	Value
revocationDate	Present. 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 <a href="#">RFC 5280</a> 'reasonCode' field not marked critical, as follows: <ul style="list-style-type: none"> <li><b>0. unspecified:</b> Represented by the omission of a reasonCode. Must be omitted if the CRL entry is for a Certificate not technically capable of causing issuance unless the CRL entry is for a Subscriber Certificate subject to these TLS BR revoked prior to July 15, 2023.</li> <li><b>1. keyCompromise:</b> Indicates that it is known or suspected that the Subscriber's Private Key has been compromised.</li> <li><b>3. affiliationChanged:</b> 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.</li> <li><b>4. Superseded:</b> 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 the CA has revoked the Certificate for compliance reasons such as the Certificate does not comply with the TLS BR or this CPS.</li> <li><b>5. cessationOfOperation:</b> 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.</li> <li><b>6. certificateHold:</b> Must not be included if the CRL entry is for (1) a Certificate subject to the BR, or (2) a Certificate not subject to the BR and was either (A) issued on-or-after 2020-09-30 or (B) has a notBefore on-or-after 2020-09-30.</li> <li><b>9. privelegeWithdrawn:</b> 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.</li> </ul>

The LRA, Enterprise RA, or Trusted Agent, when the request is submitted via email, will document the reason for the request and archive this documentation. Unless the revocation reason is "Unspecified ([RFC 5280](#) CRLReason #0)", the above revocation reason codes are included in the CRLs issued by IdenTrust, except for "Unspecified ([RFC 5280](#) CRLReason #0)".

### 7.2.2.1 CRL Issuing Distribution Point

Partitioned CRLs must contain an Issuing Distribution Point extension. The distributionPoint field of the Issuing Distribution Point extension is present. Additionally, the fullName field of the DistributionPointName value is present, and its value conforms to the following requirements:

1. If a Certificate within the scope of the CRL contains a CRL Distribution Points extension, then at least one of the uniformResourceIdentifiers in the CRL Distribution Points's fullName field must be included in the fullName field of the CRL's Issuing Distribution Point extension. The encoding of the uniformResourceIdentifier value in the Issuing Distribution Point extension is byte-for-byte identical to the encoding used in the Certificate's CRL Distribution Points extension.
2. Other GeneralNames of type uniformResourceIdentifier may be included.
3. Non-uniformResourceIdentifier GeneralName types are not included.

The `indirectCRL` and `onlyContainsAttributeCerts` fields is set to `FALSE` (i.e., not asserted).

IdenTrust may set either of the `onlyContainsUserCerts` and `onlyContainsCACerts` fields to `TRUE`, depending on the scope of the CRL.

IdenTrust does not assert both of the `onlyContainsUserCerts` and `onlyContainsCACerts` fields.

The `onlySomeReasons` field should not be included; if included, then IdenTrust will provide another CRL whose scope encompasses all revocations regardless of reason code.

This extension should not be used for full and complete CRLs.

### **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 requires Relying Parties to refer to the local clock to check for response freshness.

IdenTrust does not support the `nonce` extension in responses.

##### **7.3.2.1 singleExtensions**

The `singleExtensions` of an OCSP response does not contain the `reasonCode` (OID 2.5.29.21) CRL entry extension.

## 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

IdenTrust has a regularly scheduled compliance audit mechanism in place to ensure that the requirements of the TrustID CP, this CPS and the CA/B Forum BR 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.S.I § 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.

IdenTrust also conducts a separate internal audit to ensure the server, Code Signing, Time-Stamping and S/MIME Certificates are adhering to requirements of the TrustID CP and the CA/B Forum BR for quality Issuance. These are conducted quarterly on randomly selected 3% of the server Certificates chosen from the period immediately after the prior audit. Results from these quarterly audits are saved and provided upon request to third party auditors meeting the criteria in [Section 8.2](#).

### 8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

IdenTrust has passed previous audits that have demonstrated compliance with the TrustID CP and this 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 (a) Technically Constrained in line with [Section 7.1.4.2](#) and audited in line with [Section 8](#) only in regards to self-audits, or (b) unconstrained and fully audited in line with all remaining requirements from the CA/B Forum BR. 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.

IdenTrust will conduct or require a separate audit using the standards in [Appendix A](#) when assessing server Certificates issues for Sponsoring Organizations with Enterprise RAs.

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 does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in [Section 8.4](#), then, before issuing Publicly-Trusted Certificates, the CA shall successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in [Section 8.4](#). The point-in-time readiness assessment shall be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates and shall be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.

### 8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

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<sup>11</sup>, certification systems, and the like, as well as Internet security issues (such as management of a security perimeter), operations of secure Datacenters, 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.

Moreover, in auditing secure information systems, the independent firm should be guided by generally accepted standards for evaluating secure information systems such as ISO 27001, Annex B of ANSI X9.79, WebTrust for Certificate Authorities, or ISO 21188. The engagement of the auditing firm takes the form of a contract obligating the firm to assign members of its professional auditing staff to perform the audit when required. The contracted independent firm must also carry an omissions insurance with Policy limits of at least one million US dollars in coverage. While the audit is being performed, those staff must, by agreement, perform the audit as their primary responsibility.

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.

---

<sup>11</sup> For Enterprise RAs, the firm must be experienced in information system auditing and may be a qualified third party or a qualified independent internal auditing group.

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 its TrustID CP and this 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 the TrustID CP, this 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 [Audit logging procedures](#).

SOC2 and CA WebTrust are 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 the TrustID CP, this 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 – Code Signing Baseline Requirements 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](#).

The audit covers all IdenTrust obligations under the [CS BR](#) regardless of whether they are performed directly by the IdenTrust, an RA, or subcontractor.

### 8.4.2 Signing Service Assessment

For Audit Periods starting after June 30, 2024, the Signing Service must undergo a conformity assessment audit for compliance with the [CS BR](#) performed in accordance with the “WebTrust for Certification Authorities – Code Signing Baseline Requirements 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](#).

### 8.4.3 Timestamp Authority Assessment

The Timestamp Authority must undergo a conformity assessment audit for compliance with the [CS BR](#) performed in accordance with the “WebTrust for Certification Authorities – Code Signing Baseline Requirements v2.2 or newer” and “WebTrust for Certification Authorities – Network Security – Version 1.0 or newer scheme.

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 the TrustID CP or this 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 due consideration.

### 8.5.1 Actions Taken as a Result of Internal Audit Deficiency

If the quarterly internal SSL/TLS Certificate audit shows discrepancies between Certificates and the requirements of the TrustID CP and this CPS, the following actions will be performed:

- The Security Officer will note the discrepancy;
- The Security Officer will notify the Head of Operations about the discrepancy;
- The Head of Operations will address any identified discrepancies with IdenTrust;
- IdenTrust will correct any deficiencies noted during compliance reviews, as specified by the Security Officer, including proposing a remedy and expected time for completion.

## 8.6 COMMUNICATION OF RESULTS

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 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.

Sponsoring Organizations with Enterprise RAs will report their audit results to the IdenTrust security office as described in [Section 8.5.1](#).

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.

For Audit Reports in which the Audit Period includes a date later than August 1, 2020, then the requirements set forth in the remainder of this [Section 8.6](#) shall be met.

The Audit Report contains at least the following clearly-labeled information:

1. name of the organization being audited;
2. name and address of the organization performing the audit;
3. the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross Certificates, that were in-scope of the audit;
4. audit criteria, with version number(s), that were used to audit each of the Certificates (and associated keys);
5. a list of the CA policy documents, with version numbers, referenced during the audit;
6. whether the audit assessed a period of time or a point in time;
7. the start date and end date of the Audit Period, for those that cover a period of time;
8. the point in time date, for those that are for a point in time; and
9. the date the report was issued, which will necessarily be after the end date or point in time date;

An authoritative English language version of the publicly available audit information is provided by the Qualified Auditor and IdenTrust CA to ensure that it is publicly available. The Audit Report is available as a PDF, with text searchable for all information required. Each SHA-256 fingerprint within the Audit Report is in uppercase letters and does not contain colons, spaces, or line feeds.

### **8.6.1 Communication of Internal Audit Results**

The results of IdenTrust's internal Certificate Issuance quality audit for server Certificates for IdenTrust and Sponsoring Organizations with Enterprise RAs are fully documented, and reports resulting from it are submitted to Operations Management for review by risk management within 30 calendar days of the date of their completion by the Security Officer. Such reports will identify the CP and CPS used in the assessment including their dates and version numbers.

## **8.7 SELF-AUDITS**

During the period in which IdenTrust Technically Constrained Subordinate CA issues Certificates, IdenTrust monitors adherence to the TrustID CP and CPS, to strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one Certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

Self-audits on server Certificates, S/MIME Certificates, and Code Signing Certificates are performed in accordance with the CA/B Forum BR. IdenTrust may conduct self-audit on other Certificate Types to validate reasonable compliance with browser's root store CA Policies.

IdenTrust uses a linting process to verify the technical accuracy of Certificates within the selected sample set independently of previous linting performed on the same Certificates.

## **8.8 REVIEW OF DELEGATED THIRD PARTIES**

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

## **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 the TrustID CP and this 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 of the TrustID CP.

### **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 the TrustID CP.

### **9.3.2 Information Not Within the Scope of Confidential Information**

TrustID Certificates and related status information (including CRLs), and individual 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 the TrustID CP and this 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 the TrustID CP and this 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**

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: (i) authorized by the TrustID CP; (ii) required to disclose by law, governmental rule or regulation, or court order; or (iii) 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 Section 9.13 of the TrustID CP.

### **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 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 the TrustID CP and this 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

IdenTrust as Issuing CA is responsible for all aspects of the Issuance and management of a TrustID Certificate including:

- The application and enrollment process;
- The legal existence of the applicant Organization
- The Identity Proofing process as described in [Section 3.2](#);
- The verification of authorization by Domain Name Registrant as described in [Section 3.2.2.4](#).
- The Applicant's right to use the Mailbox Address as described in [Section 3.2.6.3](#).
- Validation of Authority as described in [Section 3.2.5](#)
- The Accuracy of the information as described in [Section 3.2.2.7](#)
- The actual Certificate manufacturing process;
- Publication of the Certificate;
- Revocation of the Certificate;
- Maintaining an online 24x7 publicly accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates as described in [Section 2.1](#);
- Renewal of the Certificate; and
- Ensuring that all aspects of IdenTrust services and CA operations and infrastructure related to Certificates issued under the TrustID CP and this CPS are performed in accordance with the requirements, representations, and warranties of the TrustID CP, CPS, and the CA/B Forum BR including the following:

#### 9.6.1.1 Notification of Certificate Issuance and Revocation

IdenTrust has an online Certificate status database or CRLs available to End Entities in accordance with Section 4.10 of the TrustID CP.

#### 9.6.1.2 Subscriber Warranties

IdenTrust provides the following warranties to all Subscribers of TrustID Certificates that IdenTrust issues under the TrustID CP and this CPS:

- IdenTrust has issued and managed the TrustID certificate in accordance with the applicable Subscriber Agreement (and in accordance with the TrustID CP, if the TrustID CP has been incorporated by reference in the Subscriber Agreement; and in accordance with this cps, if this cps has been incorporated by reference in the Subscriber Agreement); and
- The TrustID Certificate meets all requirements of the applicable Subscriber Agreement (and the TrustID CP, if the TrustID CP has been incorporated by reference in the Subscriber Agreement; and this CPS, if this CPS has been incorporated by reference in the Subscriber Agreement).

Such warranties shall be made as of: (i) the time of the Subscriber's Acceptance of the TrustID Certificate; and (ii) the time that the Subscriber's TrustID Certificate is used during its Operational Period.

### **9.6.1.3 Authorized Relying Party Warranties**

IdenTrust, in its sole discretion, may provide a validation warranty as described in Section 9.6.1.3 of the TrustID CP to an Authorized Relying Party by expressly including such a warranty in the applicable Authorized Relying Party Agreement.

### **9.6.1.4 Warranty Limitations**

The warranties offered to both Subscribers and Authorized Relying Parties will be subject to all limitations set forth in the TrustID CP, this CPS, and the applicable agreement between such entity and IdenTrust (e.g., Subscriber Agreement, Authorized Relying Party Agreement). In addition and without limitation, coverage by any warranties offered by IdenTrust is completely excluded in the event of: (i) the End Entity's (a) improper use of Certificates or Key Pairs, (b) failure to safeguard Private Keys, (c) failure to comply with the provisions of the TrustID CP, this CPS or of any agreement with IdenTrust or an RA, or (d) other actions of End Entity giving rise to any loss; (ii) events beyond the reasonable control of IdenTrust or the RAs; and (iii) time limitations for the filing of claims, which shall be the lesser of the time specified in the relevant agreement between IdenTrust and the End Entity and the time specified in Section 9.17.1.5 of the TrustID CP.

### **9.6.1.5 Time between Certificate Request and Issuance**

The provisions of Section 9.6.1.5 of the TrustID CP shall apply.

### **9.6.1.6 Certificate Revocation and Renewal**

IdenTrust must notify an End Entity when a TrustID Certificate bearing the End Entity's DN is issued or revoked.

### **9.6.1.7 End Entity Agreements**

IdenTrust will enter into agreements with End Entities governing the provision of Certificate and Repository services and delineating the parties' respective rights and obligations.

IdenTrust will ensure that all Subscriber Agreements incorporate by reference the provisions of the TrustID CP and this CPS regarding IdenTrust's and the Subscriber's rights and obligations. In the alternative, IdenTrust may ensure that its Subscriber Agreements, by their terms, provide the respective rights and obligations of IdenTrust and the Subscribers as set forth in the TrustID CP and this CPS, including without limitation the parties' rights and responsibilities concerning the following:

- PROCEDURES, RIGHTS, AND RESPONSIBILITIES GOVERNING (I) APPLICATION FOR A TRUSTID CERTIFICATE, (II) THE ENROLLMENT PROCESS, (III) CERTIFICATE ISSUANCE, AND (IV) CERTIFICATE ACCEPTANCE;
- THE SUBSCRIBER'S DUTIES TO PROVIDE ACCURATE INFORMATION DURING THE APPLICATION PROCESS;
- THE SUBSCRIBER'S DUTIES WITH RESPECT TO GENERATING AND PROTECTING ITS KEYS;
- PROCEDURES, RIGHTS, AND RESPONSIBILITIES WITH RESPECT TO IDENTITY PROOFING;
- ANY RESTRICTIONS ON THE USE OF TRUSTID CERTIFICATES AND THE CORRESPONDING KEYS;
- PROCEDURES, RIGHTS, AND RESPONSIBILITIES GOVERNING (A) NOTIFICATION OF CHANGES IN CERTIFICATE INFORMATION, AND (B) REVOCATION OF TRUSTID CERTIFICATES;
- PROCEDURES, RIGHTS, AND RESPONSIBILITIES GOVERNING RENEWAL OF TRUSTID CERTIFICATES;



- ANY OBLIGATION OF THE SUBSCRIBER TO INDEMNIFY ANY OTHER PARTICIPANT;
- PROVISIONS REGARDING FEES;
- THE RIGHTS AND RESPONSIBILITIES OF ANY RA THAT IS PARTY TO THE AGREEMENT;
- ANY WARRANTIES MADE BY IDENTRUST AND ANY LIMITATIONS ON WARRANTIES OR LIABILITY OF IDENTRUST AND/OR AN RA;
- PROVISIONS REGARDING THE PROTECTION OF PRIVACY AND CONFIDENTIAL INFORMATION; AND
- PROVISIONS REGARDING ALTERNATIVE DISPUTE RESOLUTION.
- NOTHING IN THE CERTIFICATE SUBSCRIBER AGREEMENTS MAY WAIVE OR OTHERWISE LESSEN THE OBLIGATIONS OF THE SUBSCRIBER AS PROVIDED IN SECTION 9.6.3 OF THE TRUSTID CP.

IdenTrust will ensure that all Authorized Relying Party Agreements incorporate by reference the provisions of the TrustID CP and this CPS regarding IdenTrust's and the Authorized Relying Party's rights and obligations. Nothing in the Authorized Relying Party Agreements may waive or otherwise lessen the obligations of the Authorized Relying Party as provided in Section 9.6.4 of the TrustID CP.

#### **9.6.1.8 Protection of Private Keys**

IdenTrust must ensure that its Private Keys and Activation Data are protected in accordance with Section 4 and Section 6 of the TrustID CP and with the applicable provisions of this CPS.

#### **9.6.1.9 Restrictions on IdenTrust's Private Key Use**

IdenTrust must ensure that its CA Private Signing Key is used only to sign Certificates and CRLs. IdenTrust must ensure that Private Keys issued to its personnel to access and operate CA applications are used only for such purposes. To the extent IdenTrust personnel require or wish to use Certificates for non-CA purposes, they should be issued separate Certificates appropriate for such use.

#### **9.6.1.10 Ensuring Compliance**

IdenTrust must ensure that: (i) it only accepts information from RAs that understand and are obligated to comply with the TrustID CP; (ii) it complies with the provisions of the TrustID CP and this CPS in its certification and Repository services, Issuance and Revocation of TrustID Certificates and Issuance of CRLs; (iii) it makes reasonable efforts to ensure the RA and End Entity adherence to the TrustID CP and this CPS with regard to any TrustID Certificates issued under it; and (iv) its or any RAs' authentication and validation procedures are implemented as set forth in [Section 3](#).

#### **9.6.1.11 Consequences of Breach**

IdenTrust's liability to an End Entity will be determined in accordance with any agreement between IdenTrust and the End Entity; as such, liability may be limited by Section 9.6 of the TrustID CP, and other provisions of this CPS.

### **9.6.2 RA Representations and Warranties**

IdenTrust must ensure that all its RAs comply with all the relevant provisions of IdenTrust's CP and this 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 of the TrustID CP.

### **9.6.2.1 Notification of Certificate Issuance and Revocation**

Unless otherwise provided by contract, there are no requirements that an RA must notify a Subscriber or Authorized Relying Party of the Issuance or Revocation of a TrustID Certificate.

### **9.6.2.2 Accuracy of RA Representations**

When an RA submits End Entity or Sponsoring Organization information to IdenTrust, it certifies to IdenTrust that it has authenticated the identity of that End Entity or Sponsoring Organization in accordance with Section 3 and Section 4 of the TrustID CP and with the applicable provisions of this CPS.

### **9.6.2.3 Protection of RA Private Keys**

Each person performing RA duties online through a remote administration application with IdenTrust must ensure that his or her Private Keys are protected in accordance with Section 5 and Section 6 of the TrustID CP and this CPS.

### **9.6.2.4 Restrictions on RA Private Key Use**

Private Keys used by automated clients to access and operate IdenTrust RA Applications must not be used for any other purpose.

Private keys used by RA personnel will be used within the constraints of the Individual Certificate policies under which they are issued.

### **9.6.2.5 RA Security and Operations Manual**

Each RA will comply with the provisions of an RA Security and Operations Manual provided by IdenTrust to its RAs.

### **9.6.2.6 Consequences of Breach**

An RA's liability to an End Entity will be determined in accordance with any agreement between the RA and the End Entity; as such, liability may be limited by Section 9.6 of the TrustID CP, other provisions of this TrustID CP, and other provisions of this CPS.

### **9.6.2.7 Generation of End Entity Private Key**

An RA may generate the Key Pair associated with TrustID CIV Card Authentication Certificate and TrustID CIV Device Certificate provided the RA performs the Key Pair Generation on an approved Cryptographic Module in accordance with [Section 6.2.1](#).

## **9.6.3 Subscriber Representations and Warranties**

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 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 such as a 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 use the Certificate only on Mailbox Addresses 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:
  - a. 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
  - b. 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 and, or CPS or the CA/B Forum BR.

#### **9.6.3.1 Representations**

Provide complete and accurate responses to all requests for information made by IdenTrust (or an RA) during Applicant/PKI Sponsor registration, Certificate application, and Identity Proofing processes; and upon Issuance of a TrustID Certificate naming the Applicant/PKI Sponsor as the Subscriber, review the Certificate to ensure that all Subscriber information included in it is accurate, and to accept or reject the Certificate in accordance with Section 4.4 of the TrustID CP and with the applicable provisions of this CPS;

#### **9.6.3.2 Protection of Subscriber Private Key**

Generate a Key Pair using a Trustworthy System, and take reasonable precautions to prevent any compromise, modification, loss, disclosure, or unauthorized use of the Private Key;

#### **9.6.3.3 Restrictions on Subscriber Private Key Use**

Use the TrustID Certificate and the corresponding Private Key exclusively for purposes authorized by the TrustID CP and this CPS, and then only in a manner consistent with the TrustID CP and this CPS, including but not limited, in the case of Code Signing Certificates, to not using the Private Key to Digitally Sign hostile code, including spyware or other malicious software (malware) downloaded without user consent.

#### **9.6.3.4 Notification upon Private Key Compromise**

Instruct IdenTrust (or an RA) to revoke the TrustID Certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the Private Key, or, in the case of a TrustID Certificate issued to an Affiliated Individual under Section 3.4 and Section 4.9.12 of the TrustID CP, whenever the Affiliated Individual is no longer affiliated with the Sponsoring Organization.

#### **9.6.3.5 Consequences of Breach**

A Subscriber who is found to have acted in a manner counter to these obligations: (i) will have his, her or its TrustID Certificate revoked; (ii) forfeits all claims he, she or it may have against PKI Service Providers; (iii) must

cease all use of the Private Key corresponding to the Public Key included in the Certificate upon Revocation of that Certificate for reasons of Private Key compromise.

#### **9.6.3.6 Other Agreements**

Without forming any limitation on any provisions of the TrustID CP or this CPS, Subscriber's obligations will be governed by the Subscriber Agreement between the Subscriber and IdenTrust.

#### **9.6.4 Relying Party Representations and Warranties**

Before relying on or using a TrustID Certificate issued under the TrustID CP and this 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 the TrustID CP, this 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 of the TrustID CP and with the applicable provisions of this CPS;

##### **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 the TrustID CP or this 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**

### **9.6.5.1 Repository Obligations, Representations, and Liability**

A Repository is responsible for maintaining a secure system for storing and retrieving Certificates, a current copy, or a link to a current copy, of the TrustID CP, this CPS, and other information relevant to Certificates, and for providing information regarding the status of Certificates as valid or invalid that can be determined by an Authorized Relying Party.

### **9.6.5.2 PKI Service Provider Obligations, Representations, and Warranties**

Subject to the other provisions of this CPS, the TrustID CP, and any applicable agreement between IdenTrust and an End Entity, the provisions of Section 9.6 of the TrustID CP shall apply.

### **9.6.5.3 Representations and Warranties of Affiliated/Subscribing Organizations**

A Subscribing Organization represents and warrants that it:

- a. Authorizes the affiliation of Subscribers with the Organization for Affiliated Certificates;
- b. Verifies that any information it may provide during the Identity Proofing and/or registration processes is accurate; and
- c. Will immediately inform the CA of any severance of affiliation with any current Subscriber.

## **9.7 DISCLAIMER OF WARRANTIES**

EXCEPT FOR THOSE WARRANTIES EXPRESSLY PROVIDED IN THIS CPS OR THAT MAY BE EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT BY IDENTRUST, IDENTRUST: (I) 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 (II) 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 the TrustID CP, other provisions of this 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 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**

In addition to any other provisions of the TrustID CP, this 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 Server 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 Secure Email Certificate, TrustID CIV Card Authentication Certificate, TrustID CIV Device Certificate, TrustID Code Signing Certificate, and TrustID EV Server 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: (a) \$100,000 per transaction, and (b) \$250,000 for all transactions in which the Authorized Relying Party relies on the TrustID Certificate.

With respect to the Secure Email Certificate type of TrustID Certificate, the maximum potential liability for an Issuing CA or RA to any Authorized Relying Party with respect to any one Secure Email Certificate upon which the Authorized Relying Party relies will be limited to: (a) \$100 per transaction; and (b) \$250 for all transactions in which the Authorized Relying Party relies on the Secure Email Certificate.

With respect to the TrustID CIV Card Authentication Certificate type of TrustID Certificate, the maximum potential liability for an Issuing CA or RA to any Authorized Relying Party with respect to any one TrustID Card Authentication Certificate upon which the Authorized Relying Party relies will be limited to: (a) \$10 per transaction, and (b) \$25 for all transactions in which the Authorized Relying Party relies on the TrustID Card Authentication Certificate.

With respect to the TrustID CIV Device Certificate type of TrustID Certificate, the maximum potential liability for an Issuing CA or RA to any Authorized Relying Party with respect to anyone TrustID CIV Device Certificate upon which the Authorized Relying Party relies will be limited to: (a) \$10 per transaction, and (b) \$25 for all transactions in which the Authorized Relying Party relies on the TrustID CIV Device Certificate.

With respect to Code Signing Certificate type of TrustID Certificate, the maximum potential liability for an Issuing CA or RA to any Authorized Relying Party with respect to any Code Signing Certificate upon which the Authorized Relying Party relies will be limited to: (a) \$2,000 per transaction; and (b) \$10,000 for all transactions in which the Authorized Relying Party relies on the Code Signing Certificate.

With respect to relying on any single TrustID EV Server 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 Server 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 CPS, the TrustID CP or any agreement between IdenTrust and an End Entity: (i) 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 (ii) 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 Certificate distribution agreement in place with IdenTrust do not assume any obligation or potential liability of IdenTrust under the CA/B Forum BR 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 CPS shall remain in effect until a new CPS is approved by the IdenTrust PMA or termination of this CPS is communicated via the IdenTrust's Repository.

### **9.10.2 Termination**

The requirements of this 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 CPS are communicated via IdenTrust's Repository.

### **9.10.3 Effect of Termination and Survival**

The conditions and effects resulting from termination of this 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 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](mailto: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, 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 CPS is reviewed by IdenTrust PMA from time to time. Errors, updates, or suggested changes to this 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 CPS to become effective, it must first be approved by the IdenTrust PMA in accordance with [Section 1.5.4](#). Amendments in the CPS will most frequently reflect amendments and timing driven by the TrustID CP changes, typically once a year in accordance with the TrustID CP. 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 the TrustID Policy Authority 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 version CPS. The final and accepted copy of this 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 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 with IdenTrust within the comment period. Decisions with respect to the proposed changes are at the sole discretion of IdenTrust.

A copy of the TrustID CP and this 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 CPS if the PMA determines that a change in the CP requires a change in OIDs.

## **9.13 DISPUTE RESOLUTION PROVISIONS**

The provisions of Section 9.13 of the TrustID CP shall apply.

### **9.13.1 Specific Provisions/ Incorporation of Policy**

IdenTrust must ensure that its agreements with RAs and End Entities contain appropriate provisions that (i) incorporate the provisions of the TrustID CP, this CPS by reference, or (ii) provide to the respective contracting parties the protections established by the TrustID CP.

## **9.14 GOVERNING LAW**

The enforceability, construction, interpretation, and validity of the TrustID CP 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 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 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 CPS

### **9.16.2 Assignment**

Except where specified by other contracts, Participants may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent of IdenTrust.

### **9.16.3 Severability**

Should it be determined that one section of this CPS is incorrect or invalid, the other sections of this CPS shall remain in effect until the CPS is updated. The process for updating this CPS is described in [Section 9.12.1](#).

In the event IdenTrust becomes aware of a conflict between this 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 a detailed reference to the Law requiring a modification of this CPS under this section and the specific modification to this CPS implemented by IdenTrust. IdenTrust will also (before issuing a TrustID Certificate under the modified requirement) notify the CA/B Forum of the relevant information newly added to its CPS by sending a message to [questions@cabforum.org](mailto: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 Forum may designate), so that the CA/B Forum may consider possible revisions to this CPS accordingly.

Any modification to IdenTrust practice enabled under this section will be discontinued if and when the Law no longer applies, or this CPS is modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to this CPS, and a notice to the CA/B Forum, as outlined above, will be made within 90 days.

### **9.16.4 Enforcement (Attorney Fees and Waiver of Rights)**

Except where an express time frame is set forth in this CPS, no delay or omission by any PKI Participant to exercise any right, remedy, or power it has under this 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 CPS shall not be construed to be a waiver of any other or repeated breach of this 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 OMITTS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF: (I) ANY PROVISION OF ANY APPLICABLE LAW, REGULATION OR ORDER; (II) CIVIL, GOVERNMENTAL OR MILITARY AUTHORITY; (III) THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER SYSTEM OPERATED BY ANY OTHER PARTY OVER WHICH IDENTRUST HAS NO CONTROL; (IV) FIRE, FLOOD, OR OTHER EMERGENCY CONDITION; (V) STRIKE; (VI) ACTS OF TERRORISM OR WAR; (VII) ACT OF GOD; OR (VIII) OTHER SIMILAR CAUSES BEYOND ITS REASONABLE CONTROL.

## **9.17 OTHER PROVISIONS**

### **9.17.1 Legal Validity of Certificates**

#### **9.17.1.1 Issuance**

To be legally valid, a TrustID Certificate must be issued in accordance with the TrustID Policy and any applicable law.

### **9.17.1.2 Waivers**

No waiver by IdenTrust of any default by another entity on an obligation or duty under this CPS will operate as a waiver of any other default, or of a similar default on a future occasion. No waiver of any provision of this CPS by IdenTrust will be effective unless such waiver makes express reference to a waiver of a particular section or sections of this CPS and is made in writing and signed by an officer or director of IdenTrust.

To be legally valid, a TrustID Certificate must be issued in accordance with the TrustID CP, this CPS, and any applicable law.

### **9.17.1.3 Acceptance**

The act of Acceptance will be logged by IdenTrust and may consist of a record made when the End Entity downloads the Certificate. Such act will be recorded and maintained in an auditable trail kept by IdenTrust in a trustworthy manner that comports with industry standards and any applicable laws or provisions of the TrustID CP, this CPS, or related agreements.

### **9.17.1.4 Operational Period**

A revoked or expired TrustID Certificate may not be used for any purpose. For revoked or expired Certificates, no action taken by an Authorized Relying Party will be considered valid for purposes of this PKI unless the Digital Signature of the Authorized Relying Party verification request is able to confirm that the Digital Signature in question was created during the Operational Period of a valid TrustID Certificate. Exceptions to the Private Key Usage period may be permissible if approved by the PMA and so long as such exceptions do not conflict with documented best practices, including the [RFC 5280](#) and the BRs.

### **9.17.1.5 Rules of Repose Allowing Ultimate Termination of Certificate**

Unless otherwise specified by the Parties, reliance on a TrustID Certificate is no longer enforceable by an Authorized Relying Party against IdenTrust or RA 4 months after termination of the applicable Authorized Relying Party Agreement or 2 years after the Authorized Relying Party's validation of the TrustID Certificate with IdenTrust's Repository, whichever occurs first.

## APPENDIX A: Enterprise RAs as LRAs Auditing and Security Standards

- Trustworthy registration agent employees as specified in [Section 5.3.3.2](#) and [Section 5.3.3.3](#);
- Physically secure environment means that employees, equipment, and information are safe from physical or logical intrusion, and reasonably safe from environmental events; including guarded or restricted access to the areas where the registration information is being received and processed, and to the equipment used for connecting to us. The workstations are password protected – conforming to best-practices password standards, or better – and reasonably secure network and server equipment through which the information will pass (meaning passwords on all servers if possible and locked and restricted-access server closet/room);
- Secure network – firewalls, etc., for security protection and resistance to external attacks;
- Workstation with operating system current and under maintenance (meaning the software is covered by an in-force maintenance agreement that supplies help services and security updates, and that the updates are applied in a timely manner), with all current security updates, applied; and
- Antimalware software installed and kept up to date, cannot be bypassed or disabled by the user so long as it passes muster with industry best practices and related authorities.