TrustID®
Certification Practice Statement

IdenTrust Services LLC.
Version 4.7.7
April 26, 2021

Table of Contents

1 INTRODUCTION

1.1 OVERVIEW

This Certification Practice Statement (CPS) describes the practices employed by IdenTrust Services, LLC (IdenTrust) as a Certification Authority (CA), and by Registration Authorities (RAs), to fulfill the requirements of the IdenTrust TrustID Certificate Policy dated April 26, 2021 (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.

Appendix C documents the hierarchies for which this CPS applies including Root CA Certificates, Subordinate CA Certificates and End Entity Certificates type.

The copy of the "TrustID® Certificate Practice Statement" 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 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:

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 Copy.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the TrustID Certification Practice Statement approved for publication on April 26, 2021 by the IdenTrust Policy Management Authority (PMA). The following table contains subsequent revisions:

Table 1 - TrustID Certification Practice Statement Versions

Version	Date	Summary of Changes/Comments
2.4	May 22, 2015	Updates for TrustID CPS compliance, inclusion of FATCA Organization Certificate, inclusion of Certificate Policy OID for hardware practices, compliance with the CA/B Forum Baseline Requirement in relationship to use of CAA records for verification of Domain Name ownership/control, enhancement of Certificates definitions, and clarification on practices of unique names for Server Certificates.
3.0	September 15, 2016	Incorporate language to support Secure Email Certificates.
3.1	October 27, 2016	Updates to include the CA/B Forum Baseline Requirements v.1.4.0 and CA/B Forum Extended Validation Guidelines v.1.6.0.
3.2	April 12, 2017	Update OIDS to Support SHA-256 hash algorithm: Remove OIDs previously assigned to TrustID Business and Personal Hardware SHA-256 Support generation of Certificate non-sequential serial number from exhibiting 20 bits of entropy to exhibiting at least 64 bits of entropy.
3.3	June 1, 2017	Updates to include the CA/B Forum Baseline Requirement v 1.4.1 and enhancement for compliance with the Mozilla Root Store Policy v 2.4.1.
3.4	September 8, 2017	Additional enhancements added for compliance with the CA/B Forum Extended Validation Code Signing Requirements, Addition of TrustID Card Authentication Certificate and Device Certificate. Addition of practices for CAA check for Server Certificates. Implemented September 8, 2017 and CPS documentation approved by PMA committee on September 12, 2017.
3.5	January 30, 2018	Updates to reflect updated CA/B Forum Baseline Requirements.
4.0	May 31, 2018	1. Align with TrustID CP conversion to RFC 3647 2. Add CT Logging
4.1	August 17, 2018	1. Section 1.2.2: Add the last two OIDs for TrustID Business Certificates. 2. Section 1.6: Added definitions. 3. Section 3.2.2.4: Updates adding explicit methods supported for Domain Name Registrant validation in line with the CA/B Forum Baseline Requirements. 4. Section 4.3.1(3): update to reflect that ActiveX is not the only Certificate retrieval option.

Version	Date	Summary of Changes/Comments
		5. Section 5.2.4: Updates to some roles requiring separation of duties. 6. Section 6.2.1: Add support of non-FIPS Cryptographic Modules for TrustID Secure Email Certificates only.
4.2	October 18, 2018	1. Updates to clarify comments by Mozilla in reference to the Extended Validation Server Certificate application. 2. Updates for Certificate Problem Reporting.
4.3	January 31, 2019	1. Section 1.1; updates to reflect conformance with the version number of the CA/B Forum Baseline Requirement documents. 2. Section 1.6.1: Add definitions: • Certificate Chain. • Client-authenticated SS/TLS Encrypted Session. 3. Enable any static custom label in the OU of S/MIME Certificates: • Section 3.1.1 • Section 7.1.1.6.4 • Section 7.1.4.3 4. Section 4.7.3; update to support automatic Certificate retrieval when no modifications are required. 5. Section 4.9.1 and 4.9.5: Updates to better reflect the process in place to handle Server Certificate Revocation that is line with CA/B Forum Baseline Requirements. 6. Section 4.9.16; update to No Stipulation, instead of "Unspecified" {CA/B Forum Compliance}. 7. Section 6.1.6: Updates to remove explicit brand HSM's 8. Section 6.5.2: Updates to reflect updated CA equipment security ratings. 9. Section 7.1.2.1: Update the keyUsage description removing non-applicable statement. 10. Section 7.1.2.2: Update the nameConstraints to enable it on Subordinate CA Certificates. 11. Section 7.1.4.1: Update the CN to enable customer specific Domain Names as currently these are restricted to be prefixed with the label "TrustID…". 12. Section 9.2.3: Updates to be in line with the CP. 13. Section 9.18: Updated AIA with updated URL. 14. Section 9:20: Updates Certificate hierarchy removing expired Sub-CA.
4.4	May 31, 2019	1. Section 1.1 move text to Section 2.2.2. 2. Section 1.2.2 OID renaming and new OID. 3. Section 1.4.1.1 Added Medium Assurance Hardware Unaffiliated Certificates. 4. Section 1.6.1 Added definitions: CAA Resource Record Set; Technically Constrained Subordinate CA. 5. Section 2.2.2 Added text removed in Section 1.1. 6. Section 3.1.1 Added Medium Assurance Hardware Unaffiliated Certificates.

Version	Date	Summary of Changes/Comments
		7. Section 3.2 updates to cover in-person identity vetting for TrustID Medium Assurance Hardware Unaffiliated Certificates. 8. Section 3.2.2.4 Update to reflect that the validation method for Server Certificates is being recorded. 9. Section 4.2 Updates on how the processing for CAA Records is handled. 10. Section 4.2.1 Updates to reflect how data and documents supplied for Server Certificates vetting are used and reused. 11. Section 6.2.1 Updates enabling flexibility for FIPS 140 Cryptographic Modules. 12. Section 7.1.4.2 Updates to reflect that underscores in Server Certificate names are not allowed. 13. Section 7.1.5 Update to reflect that not fully Technically Constrained Sub-CA's are publicly disclosed. 14. Appendix C Add TrustID HID Enterprise CA 1 as non-fully Technically Constrained Subordinate CA.
4.5	September 27, 2019	1. Corrected invalid Annex A, B and C references throughout the document. 2. Updates relevant to the Network Security Controls to be line with CA/B Forum SC3 approved on August 16, 2018 to be effective on April 1, 2020: Sections 1.6; 5.2.1; 5.2.1.3.9; 5.4; 5.4.8; 6.1.5; 6.5; 6.5.1; 6.5.2 and 6.6.1. 3. Updates relevant to Extended Validation Code Signing and Time-Stamping Certificates: Sections 1.4.2.; 1.6.1; 3.1.1.; 3.1.5; 3.2; 3.2.3.8; 4.9.1; 4.10.1; 6.2.1; 6.3.2; 6.7; 8; and Appendix A. 4. Updates relevant to Card Authentication Certificates: Sections 1.6.1; 1.6.2; 4.2.2; 4.3; 4.3.1; 4.3.1.1; 4.3.1.2; 4.3.1.3; 4.3.2.
4.6	November 21, 2019	1. OID Updates to support offering of Server Certificates for Domain Validation (DV) only, Domain Validation (DV) with Organization Validation (OV) only and Extended Validation only. 2. Addition of Subordinate CAs for: Server DV Certificate only, Server EV+DV Certificate only; Server EV Certificate only, EV Code Signing only; Time-Stamping only.
4.6.1	December 11, 2019	Clarifying profile attributes for Sub CA and Server Certificates
4.7	January 31, 2020	1. Section 3.1.1 updates to allow null Subject commonName for Server Certificates as long as the subjectAltName extension is not null. 2. Section 3.1.3 updates to allow anonymous Certificates. 3. Section 3.2.2.5 updates to support Issuance of Server Certificates to IP Addresses. 4. Section 5 updates. 5. Addition of Subordinate CA A13 as replacement for Subordinate CA A12.
4.7.1	March 26, 2020	1. Align section headers with RFC-3647 format.

Version	Date	Summary of Changes/Comments
		2. Clarify CP/CPS publication schedule frequency. 3. Update http addresses. 4. Clarify language for Server Certificate types. 5. Update Certificate Profile fields.
4.7.2	May 21, 2020	1. CPS self-assessment updates. 2. Reduce the validity period on Server Certificates to 398 days maximum when issued effective September 1, 2020. 3. Incorporate requirements for supervised and unsupervised remote individuals Identity Proofing.
4.7.3	June 15, 2020	1. Removing redundant reference in Section 3.2.2.4.2. 2. Revising content order in Section 4.9 Certificate Revocation and Suspension for consistency and flow. 3. Updated Section 3.1.2 for Server Certificates. 4. Updated Section 7 Certificate profiles to clarify use of BasicConstraints. 5. Updated Appendix C to include IdenTrust Public Sector Root CA 1. 6. Incorporated various cosmetic changes.
4.7.4	August 3, 2020	1. Add language in Section 1.2.1: Alphanumeric Identifier to specify Root CAs that are currently governed by this CP. 2. Add references to IdenTrust Public Sector Root CA to Certificate Profiles in Appendix A: Certificate Profiles. 3. Add new Public Sector subordinate CA to Appendix C: Certificate Hierarchy.
4.7.5	September 28, 2020	1. Updated Reduce the validity period of Server Certificates up to 397 days maximum when issued effective September 1, 2020. 2. Added TrustID Server CA A52 back into Section 12: Appendix C Certificate as this CA is still active. 3. Updates in Sections 4.9.9, 4.9.10 and 7.3 for new OCSP requirements. 4. Updates to Section 7.1.4 Name Forms. 5. Updates to Section 7.2.2. CRLs. 6. Updates to Section 8.6 – Communication of Audit Results.
4.7.6	December 28, 2020	1. Section 4.9.1: updates to better reflect Revocation of Server and Non-Server Certificates. 2. Section 3.3.1; 4.7.3.; 4.7.3.1; 4.11.1; Reduce 90-day renewal period to 30-day on Server Certificates. 3. Section 4.9.7: Update CRL frequency to 12 months instead of 30 days. 4. Section 5.1.1; 5.1.1.1; 5.1.2.1: Systems monitoring. 5. Section 7.1.2.5; 10.1.1: Certificate field name updates. 6. Appendix C: a. Added Subordinate CA's R3 and R4. b. Removed expired subordinate CAs c. Added expiration dates to table
4.7.7	April 26, 2021	1. Section 1.6.1 and 3.2.2: Added Attestation Letter as proofing method for subject identity information 2. Section 1.6.1 updated Critical Vulnerability definition

Version	Date	Summary of Changes/Comments
		3. Section 4.2.1: Update to clarify the age of documentation for Extended Validation Code Signing Certificates 4. Section 3.2.2.4.3: Updated reference based on Updates to include the CA/B Forum Baseline Requirements v.1.7.4 5. Section 5.2.1.: Updates relevant to CA facilities surveillance 6. Appendix C, Added ISGR as subordinate of DST X3 7. Section 9.6.1.: updates relevant to Updates to the CA/B Forum Baseline Requirements v.1.7.4. 8. Updates to Trusted Roles to allow cross responsibilities between Systems Administrators and PKI Consultants. See section 5.2.1 Trusted Roles

1.2.1 Alphanumeric Identifier

The alphanumeric identifier (i.e., the title) for this CPS is the IdenTrust TrustID Certificate Practices Statement, v4.7.7 dated April 26, 2021 or "identrust_trustid_cps_v4.7.7_04262021".

The following Root CAs are governed by this CP document:

- IdenTrust Commercial Root CA 1
- IdenTrust Public Sector Root CA 1

1.2.2 Object Identifier (OID)

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 TrustID CPS are given one or more of the following OIDs:

Table 2 - TrustID Certificate Names, Types and Certificate Policy OIDs

Name	Type	Policy OID
Personal SHA-256 (S/MIME)	Signing /Encryption	2.16.840.1.113839.0.6.1.1
Personal Hardware SHA-256 (S/MIME)	Signing /Encryption	2.16.840.1.113839.0.6.12.3
Medium Assurance Unaffiliated Hardware (S/MIME)	Signing /Encryption	2.16.840.1.113839.0.6.12.1
Business (S/MIME)	Signing/Encryption/Identity	2.16.840.1.113839.0.6.10.2
	Card Authentication	2.16.840.1.113839.0.6.10.100
Business SHA-256 (S/MIME)	Signing /Encryption	2.16.840.1.113839.0.6.2.1
Business Hardware SHA-256 (S/MIME)	Signing /Encryption	2.16.840.1.113839.0.6.12.2
Server Domain Validation (DV)	SSL/TLS	2.23.140.1.2.1 2.16.840.1.113839.0.6.5
Server Organization Validation (OV)	SSL/TLS	2.23.140.1.2.2

Name	Type	Policy OID
		2.16.840.1.113839.0.6.3
Server Extended Validation (EV)	SSL/TLS	2.23.140.1.1 2.16.840.1.113839.0.6.9
Extended Validation Code Signing	Signing	2.23.140.1.3 2.16.840.1.113839.0.6.14.1
Time-Stamping	Signing	2.16.840.1.113839.0.6.13.1 2.16.840.1.113839.0.6.13.3
FATCA Organization	Signing/Encryption	2.16.840.1.113839.0.6.8
Administrative CA	Signing/Encryption	2.16.840.1.113839.0.7 (arc)
Administrators	Signing/Encryption	2.16.840.1.113839.0.7.1
Registration Authorities	Signing/Encryption	2.16.840.1.113839.0.7.2
Authorized Relying Parties	Signing/Encryption	2.16.840.1.113839.0.7.3
Secure Email Software (S/MIME)	Signing/Encryption	2.16.840.1.113839.0.6.11.1
Secure Email Hardware (S/MIME)	Signing/Encryption	2.16.840.1.113839.0.6.11.2
Card Authentication Certificate	Signing/Encryption	2.16.840.1.113839.0.6.30.1
Device Certificate	Signing/Encryption	2.16.840.1.113839.0.6.20.1

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 (CAs)

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 the 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 own 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 (RAs)

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 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 entity's own 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.

IdenTrust as an Issuing CA will remain ultimately responsible for all TrustID Certificates it issues. However, under the TrustID CP, IdenTrust may subcontract registration and Identity Proofing functions to an Organization that agrees to fulfill the functions of an RA in accordance with the terms of the TrustID CP, and who will Accept TrustID Certificate applications and locally collect and verify Applicant/PKI Sponsor identity information to be entered into a TrustID Certificate, which such and Organization is referred to as an RA. An RA operating under the TrustID CP is only responsible for those duties assigned to it by IdenTrust pursuant to an agreement with IdenTrust or as specified in the TrustID CP.

For Server Certificates, domain validation or IP Address Validation is always handled by IdenTrust as Issuing CA using one or more of the validation methods described in Section Verification of Authorization by Domain Name Registrant or in Section Authentication for an IP Address.

1.3.3 Subscribers

A Subscriber is an entity to whom or to which a Digital Certificate is issued. Subscribers may include Individuals (unaffiliated), Individuals who are affiliated (Business or VBA) or Sponsoring Organizations applying for 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 IdenTrust 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 Certificate 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.

1.4 CERTIFICATE USAGE

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 reflect the TrustID CP requirements, industry guidelines (e.g., CA/B Forum Baseline Requirements), 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 type 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

See table provided below.

Table 3 - TrustID Certificate Usages

Certificate Type	Description	Allowed Uses		
		Signature	Encryption	Client Authentication
Personal Personal Hardware Medium Assurance Unaffiliated Hardware	Certificate(s) issued to an Individual not affiliated to a Sponsoring Organization	Yes	Yes	Yes
Business Business Hardware	Certificate(s) issued to an Affiliated Individual	Yes	Yes	Yes
Administrative RA	Certificate(s) issued to an Affiliated Individual performing actions related to the LRA role in this CPS	Yes	Yes	
Secure Email	Certificate(s) issued to an email address only	Yes	Yes	Yes

1.4.1.2 Certificates Issued to Sponsoring Organizations

Certificate	Description	Allowed Uses					
		Secure Communications	Signing	Encryption	Authentication	Code Signing	Time-Stamping
Server (DV, OV, EV)	Certificate issued for use in an Electronic Device that supports server SSL/TLS Communications.	Yes	Yes	Yes	Yes		
Extended Validation Code Signing	Certificate issued for use in an Electronic Device signing code.		Yes			Yes	
Time-Stamping	Certificate issued for use in an Electronic Device time-stamping.		Yes				Yes
Administrative RA	Certificate issued to for use in an Electronic Device that supports signing of data submission by an automated Registration Authority.		Yes				
FATCA Organization	Certificate issued to for use by an Electronic Device supporting asymmetric encryption and signing of data submissions within the IRS FATCA program.		Yes	Yes			
Card Authentication Certificate	Certificate issued to an approved Cryptographic Module.				Yes		
Device Certificate	Certificate issued to an approved Cryptographic Module contained within an Electronic Device.		Yes	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 facilitates for interference with encrypted communications.

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

Questions regarding IdenTrust CA operation and/or TrustID Certificate Problem Report can be submitted via email to: problemreport@identrust.com.

See Section Certificate Problem Reporting for details on the process follow for these reports.

1.5.3 Person Determining Certification Practices Statement 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.

1.5.5 Publication and Notification Policies

1.5.5.1 Copy of Policy

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

https://secure.identrust.com/certificates/policy/ts

1.5.5.2 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 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.

1.5.5.3 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.

1.5.5.4 Final Change Notice

The PMA will determine the period for final change notice.

1.5.5.5 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.

IdenTrust review the TrustID CP and CPS at least once every year to ensure compliance with the latest approved version of the CA/B Forum Baseline Requirements as published at https://cabforum.org and/or in each browser's root store CA Policy as published on each website. Incremental version numbering and date changelog are present both on the title page of each document and in Table 1.1 of Section 1.2 as evidence of annual review, even when no other changes are made to the document.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

TERM	DEFINITION
Accept or Acceptance	An End Entity's act that triggers the End Entity's rights and obligations with respect to its TrustID Certificate under the applicable Certificate Agreement or Authorized Relying Party Agreement. Indications of Acceptance may include without limitation: • Using the TrustID Certificate (after Issuance); • Failing to notify IdenTrust of any problems with the TrustID Certificate within a reasonable time after receiving it; or • Other manifestations of assent.
Account Password	Private data, which may consist of Activation Data, used by the Applicant/PKI Sponsor for authentication and delivered to the CA securely via a 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.
Activation Data	Private data used or required to access or activate Cryptographic Modules (e.g., a personal identification number (PIN), pass phrase, or a manually-held Key share used to unlock a Private Key prior to creating a Digital Signature).

TERM	DEFINITION
Activation Code	A code generated by RAs or IdenTrust for a successful Applicant/PKI Sponsor to use to initiate the Certificate retrieval process through a secure session online.
Affiliated Individual	An Individual having an affiliation with an Organization who has been authorized by the Organization to obtain a TrustID Certificate that identifies the Organization and the fact of the Individual's affiliation with the Organization (see Sponsoring Organization).
Applicant	An Individual or Organization that submits application information to an RA or an Issuing CA for the purpose of obtaining, renewing or a request to revoke a TrustID Certificate.
Attestation Letter	A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.
Authorization Domain Name	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 left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.
Authorized Port	One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).
Application Software Supplier	A supplier of Internet browser software or other Relying Party application Software that displays or uses Certificates and incorporates Root Certificates.
Authorizing Official (AO)	An Individual who is an official approved by and listed within IdenTrust's databases as affiliated with a specific Organization. The AO is able to sign the authorizing form for other Individuals or PKI Sponsors for the approval of a RA Administrative Certificate for use within that Organization. This role is exclusive only to the RA Administrative Certificate process.
Authority Revocation List (ARL)	A list of revoked CA Certificates. An ARL is a CRL for CA Certificates.
Authorized Relying Party	An Individual or Organization that has entered into an Authorized Relying Party Agreement.
Authorized Relying Party Agreement	A contract between an Individual or an Organization and IdenTrust allowing the party to rely on TrustID Certificates in accordance with the TrustID CP and this CPS.
Base Domain Name	The portion of an applied-for FQDN that is the first Domain Name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

TERM	DEFINITION
CAA	A Certification Authority Authorization (CAA) record is used to specify which Certificate authorities (CAs) are allowed to issue Certificates for a domain.
CAA Resource Record Set	Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended Certificate mis-issuance.
CA Private Signing Key	The Private Key that corresponds to IdenTrust's Public Key listed in its CA Certificate and used to sign TrustID Certificates.
CA Private Root Key	The Private Key used to sign CA Certificates.
Certificate	A computer-based record or electronic message that: • Identifies the Certification Authority issuing it • Names or identifies a Subscriber, Authorized Relying Party or Electronic Device • Contains the Public Key of the Subscriber, Authorized Relying Party or Electronic Device • Identifies the Certificate's Validity Period • Is Digitally Signed by a Certification Authority and • Has the meaning ascribed to it in accordance with applicable standards A Certificate includes not only its actual content but also all documents expressly referenced or incorporated in it.
Certificate Chain	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 CP, a self-signed Root Certificate is issued in compliance with this Policy.
Certificate Agreement	The contract between a Subscriber and IdenTrust and/or RA that details the procedures, rights and obligations of each party with respect to a TrustID Certificate issued to the Subscriber.
Certificate Holder	An Individual or Sponsoring Organization that: • Is named or identified in a TrustID Certificate, or is responsible for the Electronic Device named, as the Subject of the TrustID Certificate; and; • Holds a Private Key that corresponds to the Public Key listed in that TrustID Certificate. However, for purposes of interpreting the TrustID CP and this CPS, persons holding Secure Email Certificates (S/MIME) or Certificates for administrative purposes (e.g., the Subject of an Authorized Relying Party Certificate used to access a Repository to verify Certificate status) will not be considered "Certificate Holders" with respect to Certificates issued under this Policy.
Certificate Manufacturing Authority (CMA)	An Organization that manufactures or creates TrustID Certificates for IdenTrust.

TERM	DEFINITION
Certificate Management Center (CMC)	An online interface available for Subscribers to manage their Certificate information.
Certificate Policy (CP)	A named set of rules that indicates the applicability of Certificates to particular communities and classes of applications and specifies the Identity Proofing processes performed prior to Certificate Issuance, the Certificate Profile and other allowed uses of Certificates.
Certificate Problem Report	Complaint of suspected Private Key compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to IdenTrust issued Certificates.
Certificate Profile	The protocol used in Section 7, Appendix A of this CPS, and the TrustID Certificate Profile document to establish the allowed format and contents of data fields within TrustID Certificates, which identify IdenTrust as the Issuing CA, the End Entity, the Certificate's Validity Period, and other information that identifies the End Entity.
Certificate Revocation List (CRL)	A database or other list of Certificates that have been revoked prior to the expiration of their Validity Period.
Certificate Transparency (CT)	Open standard (see RFC 6962 in Section 1.6) and open source framework for monitoring and auditing digital Certificates. Through a system of Certificate logs, monitors, and auditors, Certificate Transparency allows website users and domain owners to identify mistakenly or maliciously issued Certificates and to identify Certificate authorities (CAs) that have gone rogue.
Certification Authority (CA)	An entity that creates, issues, manages and revokes Certificates.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in creating, issuing, managing and revoking Certificates.
Common Vulnerability Scoring System (CVSS)	A quantitative model used to measure the base level severity of a vulnerability (see https://nvd.nist.gov/home).
Client-authenticated SSL/TLS-Encrypted Session	A Client-authenticated SSL/TLS-Encrypted Session is a session securely communicated through use of the Secure Sockets Layer and Transport Layer cryptographic protocols. For Client-authenticated SSL/TLS-Encrypted Sessions discussed in this CP, 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.
Critical Vulnerability	A system vulnerability that has a CVSS v2.0 score of 7.0 or higher according to the NVD or an equivalent to such CVSS rating (see https://nvd.nist.gov/vuln-metrics/cvss), or as otherwise designated as a Critical Vulnerability by the CA or the CA/B Forum.

TERM	DEFINITION
Cross-Certificate	A Certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [NIST FIPS 140-3].
Datacenter	A building within which the IdenTrust CA system resides in a high-security area involving both physical and technological protection.
Digital Signature / Digitally Sign	The transformation of an electronic record by one person using a Private Key and Public Key Cryptography so that another person having the transformed record and the corresponding Public Key can accurately determine: • Whether the transformation was created using the Private Key that corresponds to the Public Key; and • Whether the record has been altered since the transformation was made.
Distinguished Name (DN)	The unique identifier for a Subscriber so that he, she or it can be located in a directory (e.g., the DN for a Subscriber might contain the following attributes: common name (CN), email address (mail), Organization name (o), Organizational unit (ou), locality (l), state (st) and country (c)).
Domain Contact	The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.
Domain Name	The label assigned to a node in the Domain Name system (see Fully-Qualified Domain Name).
Domain Namespace	The set of all possible Domain Names that are subordinate to a single node in the Domain Name system.
Domain Name Registrant	Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
Domain Name Registrar	A person or entity that registers Domain Names under the auspices of or by agreement with: • The Internet Corporation for Assigned Names and Numbers (ICANN) • A national Domain Name authority/registry or • A Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).
Electronic Device	Computer software, hardware or other electronic or automated means (including email) configured and enabled by a person to act as its agent and to initiate or respond to electronic records or performances, in whole or in part, without review or intervention by such person.

TERM	DEFINITION
End Entity(ies)	Subscribers and Authorized Relying Parties.
Enrollment Work Station (EWS)	An Enrollment Work Station is the customer side computer application that interfaces with the CMS to accomplish Certificate registration.
Enterprise RA	An employee or agent of a Sponsoring Organization unaffiliated with IdenTrust, as the Issuing CA, who authorizes Issuance of Certificates to that Organization. Enterprise RAs sign an agreement with IdenTrust, which sets forth their obligations, which include selective equivalent obligations to an LRA.
External CA	An independent entity that is not affiliated to the Issuing CA that issues Certificates from a Subordinate CA Certificate. Such 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 are 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.
Extended Validation Code Signing (EV Code) Certificate	A Certificate that contains Subject information specified in the CA/B Forum Extended Validation Code Signing Guidelines and that are validated in accordance with those guidelines. EV Code Signing Certificates focus only on assuring the identity of the Subscriber and that the signed code has not been modified from its original form. EV Code Signing Certificates are not intended to provide any other assurances, representations, or warranties. Specifically, EV Code Signing Certificates do not warrant that code is free from vulnerabilities, malware, bugs, or other problems.
Extended Validation (EV SSL) Server Certificate	A Certificate that contains Subject information specified in the CA/B Forum Extended Validation Guidelines 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.
FATCA Foreign Financial Institution (FFI) List Search and Download Tool	An online application provided by the IRS to enable the creation and download 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 https://www.irs.gov/businesses/corporations/fatca-foreign-financial-institution-list-search-and-download-tool
Fully-Qualified Domain Name (FQDN)	A Domain Name that includes the labels of all superior nodes in the Internet Domain Name system.

TERM	DEFINITION
GET Method	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.
Government Entity	A Legal Entity, the existence of which was established by the government of a nation or a political subdivision thereof and is owned or controlled by such government or political subdivision.
Identification Proofing	To ascertain and confirm through appropriate inquiry and investigation the identity of an Individual, End Entity or Sponsoring Organization.
Individual(s)	A natural person and not a juridical person or Legal Entity.
Internal Name	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.
Internet	The Internet is a global system of interconnected computer networks that uses multiple protocols to communicate data.
Internet Protocol (IP)	The primary protocol in the Internet Layer defined by the Request for Comment 1122 (RFC 1122) - *Requirements for Internet Hosts -- Communication Layers*, Internet Engineering Task Force, R. Braden, October 1989. The IP has the task of delivering datagrams from the source host to the destination host solely based on the addresses.
IP Address or IP Addresses	A 32-bit or 128-bit label assigned to a device that uses the Internet Protocol for communication.
Issue Certificates / Issuance	The act performed by a CA in creating a Certificate, listing itself as "Issuer," and notifying the Applicant or PKI Sponsor of its contents and that the Certificate is ready and available for Acceptance.
Issuing Certification Authority (Issuing CA)	An entity authorized by the PMA to issue and sign Certificates in accordance with the TrustID CP and this CPS.
Key	A general term used throughout this Policy to encompass any one of the defined Keys mentioned in these general definitions section.
Key Escrow Database (KED)	A database that contains an escrowed copy of the encryption Certificate for each TrustID Certificate generated.
Key Generation	The process of creating a Key Pair.
Key Pair	Two 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

TERM	DEFINITION
	decrypted using the other Key; and (ii) even knowing one Key, it is computationally infeasible to discover the other Key.
Legal Entity	An association, corporation, partnership, proprietorship, trust, Government Entity or other entity with legal standing in a country's legal system.
Local Registration Agent (LRA)	An employee of an Issuing CA or Registration Authority (RA) who is responsible for confirming the correctness and accuracy of Applicant identity, either through direct contact or via review and approval of documents submitted by a licensed notary or Trusted Agent, executing the requests from Applicants in the system, and approving the Issuance of a Certificate based on that information.
National Vulnerability Database (NVD)	A database that includes the Common Vulnerability Scoring System (CVSS) scores of security-related software flaws, misconfigurations, and vulnerabilities associated with systems (see https://nvd.nist.gov/home).
Online Certificate Status Protocol (OCSP)	An online Certificate-checking protocol that enables Relying Party application software to determine the status of an identified Certificate (see also Online Status Check).
Object Identifier (OID)	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 TrustID CP and this CPS and the cryptographic algorithms supported.
Online Status Check	An online, real-time status check of the validity of a TrustID Certificate. An Online Status Check involving a CRL consists of checking the most recently issued CRL (e.g., not involving a cached CRL).
OWASP Top Ten	A list of application vulnerabilities published by the Open Web Application Security Project. See: https://owasp.org/www-project-top-ten/
Operational Period	A Certificate's actual term of validity, beginning with the start of the Validity Period and ending on the earlier of: • The end of the Validity Period disclosed in the Certificate; or • The Revocation of the Certificate.
Organization(s)	An entity that is legally recognized in its jurisdiction of origin (e.g., a corporation, partnership, sole proprietorship, government department, non-government Organization, university, trust, special interest group or non-profit corporation).
Participants	All PKI Service Providers and End Entities authorized to participate in the PKI defined by the CP and this CPS.
Penetration Test	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

TERM	DEFINITION
	types of exploits, with a goal of breaking through layers of defenses and reporting on unpatched vulnerabilities and system weaknesses.
PKI Service Providers	The PMA, IdenTrust, RAs, CMAs, and Repositories participating in the PKI defined by the CP and this CPS.
PKI Sponsor	An Individual who is employed by the Sponsoring Organization or an authorized agent who has express authority to represent the Organization but is not the Subscriber. The Sponsoring Organization verifies the PKI Sponsor is an Individual that: • Signs and submits, or approves a request for a Certificate issued to an Electronic Device on behalf of the Organization, and/or • Signs and submits a Certificate Agreement on behalf of the Organization, and/or • Acknowledges and agrees to the Certificate Terms of Use on behalf of the Organization when the Organization is an affiliate of the CA (see Section 1.3.5.4).
PMA Charter	The document adopted by the PMA that identifies the policies and procedures for administering the CP and this CPS.
Policy	The governing document that dictates the parties involved and requirements for these practices listed in this Certification Practicing Statement.
Policy Management Authority (PMA)	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).
Private Key	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.
Public Key	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.
Public Key Cryptography	A type of cryptography also known as asymmetric cryptography that uses a Key Pair to securely encrypt and decrypt messages.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based Public Key Cryptography system.
Public Suffix	The right-most concatenated portion of a Domain Name which appears in a database of information used by the CA as part of the verification process specified in Section 3.2.2.3.1.
Random Value	A value specified by a CA to the Domain Registrant that exhibits at least 112 bits of entropy.
Reasonable Reliance	For purposes of 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: • 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;

TERM	DEFINITION
	• Verified that the Digital Signature in question (if any) was created by the Private Key corresponding to the Public Key in the TrustID Certificate during the time that the TrustID Certificate was valid, and that the communication signed with the Digital Signature had not been altered; • Verified that the TrustID Certificate in question was valid at the time of the Authorized Relying Party's reliance, by conducting a status check of the Certificate's then-current validity as required by IdenTrust; and Used the TrustID Certificate for purposes appropriate under 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 prior to reliance (an Authorized Relying Party bears all risk of relying on a TrustID Certificate while knowing or having reason to know of any facts that would cause a person of ordinary business prudence to refrain from relying on the Certificate).
Registration Authority (RA)	A Legal Entity that is not a CA, contractually delegated by IdenTrust to Accept and process Certificate applications, and to verify the identity of potential End Entities and authenticate information contained in Certificate applications, in conformity with the provisions of this Policy and related agreements. RA's do not sign or issue Certificates.
Registration Authority Agreement	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.
Registration Number	The unique number assigned to a private organization by the incorporating agency in such entity's jurisdiction of incorporation.
Registration Reference	The unique number assigned to a private organization by the incorporating agency in such entity's jurisdiction of incorporation.
Registry-Controlled Label	A Public Suffix registered with a Domain Name Registrar.
Reliable Data Source	An identification document or source of data used to verify Subject identity information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.
Relying Party	A person or Legal Entity who has received information that includes a Certificate and a Digital Signature verifiable with reference to a Public Key listed in the Certificate, and is in a position to rely on them (see Section 1.3.4).
Remote Identity Proofing	Remote Identity Proofing allows an authorized individual to perform Identity Proofing via a video conferencing session, in lieu of conducting in-person Identity Proofing. NIST SP 800-63A Section 5.3.3 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.

TERM	DEFINITION
	See definitions for Supervised Remote Identity Proofing and Unsupervised Remote Identity Proofing for addition information regarding each Identity Proofing model. Refer to Section 3.2.3.2 In-Person Identification for further definitions regarding Supervised versus Unsupervised Identity Proofing.
Reserved IP Address	An IPv4 or IPv6 address that the IANA has marked as reserved: https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml https://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
Repository	An online system maintained by IdenTrust for storing and retrieving Certificates and other information relevant to Certificates, including information relating to Certificate validity or Revocation.
Request Token	A value, derived in a method specified by the Issuing CA which binds this demonstration of control to the Certificate request.
Required Website Content	Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the Issuing CA.
Revocation	The act of making a Certificate permanently ineffective from a specified time forward. Revocation is effected by notation or inclusion in a set of revoked Certificates or other directory or database of revoked Certificates (e.g., inclusion in a CRL).
Root CA Certificate	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 in order to establish a certification chain (see also Subordinate CA Certificate).
Root Certificate	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
SANS Top 25	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 https://www.sans.org/top25-software-errors/
Secure Room	The room within the Datacenter that houses 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.
Secure Email Certificate	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 prior to 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.

TERM	DEFINITION
Security and Operations Manual	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.
Shared Secret	Activation Data used to assist parties with Identity Proofing and establishing a reliable channel of communication. For purposes of establishing identity between an RA and a Subscriber, a Shared Secret may consist of an account PIN or online banking 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.
Signing Authority	An Organization that signs code on behalf of a Subscriber.
Split-Knowledge Technique	A security procedure where no single Individual possesses the equipment, knowledge or expertise to view, alter or otherwise have access to sensitive or confidential information in a particular PKI.
Sponsoring Organization	An Organization that has an affiliation with an Individual and has permitted the Individual to hold a TrustID Certificate that identifies the Sponsoring Organization and the fact of the Individual's affiliation with the Sponsoring Organization (see Affiliated Individual). In the case of Certificates issued to Electronic Devices, the Sponsoring Organization owns or controls the Electronic Device or the information asserted in the Certificate such as the Domain Name for a Certificate issued for a server. In the context of the CP, they are also called Applicant but from hereon they are referred to as Sponsoring Organizations.
Sponsoring Organization Authorization Form	The form used to provide information about an Affiliated Individual who will be authorized by an Organization to hold a TrustID Certificate.
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
Subject Distinguished Name	The specific field in a Certificate containing the unique name-identifier for the Subscriber.
Subordinate CA	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
Subordinate CA Certificate	A Certificate that is signed by the IdenTrust Root CA or other Subordinate CA's within the IdenTrust Root chain. Subordinate CA Certificates and their corresponding Public Keys may be embedded into software obtained or downloaded by the affirmative act of an Authorized Relying Party in order to establish a certification chain within the TrustID PKI hierarchy.
Subscriber	See Certificate Holder.

TERM	DEFINITION
Supervised Remote Identity Proofing	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 which 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. 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 identity and act as a witness to the proceedings. Supervised Remote Identity Proofing is used for high assurance Certificate issuance. Refer to Remote Identity Proofing and Unsupervised Remote Identity Proofing for related information. Refer to Section 3.2.3.2 In-Person Identification for further definitions regarding Supervised versus Unsupervised Identity Proofing.
Technically Constrained Subordinate CA	A Subordinate CA Certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates. The anyExtendedKeyUsage keyPurposeID shall not appear in the EKU extension of any publicly trusted Certificates.
Time-Stamping Authority	An Organization that time-stamps data, thereby asserting that the data existed at the specified time.
Time-Stamping Certificate	A Certificate used by a Time-Stamping Authority to time-stamp data, thereby asserting that the data existed at the specified time.
Token	A Cryptographic Module consisting of a hardware object (e.g., a “smart card”), often with memory and a microchip.
Trusted Agent(s)	Entity authorized to act as a representative of a Sponsoring Organization in verifying Applicant or PKI Sponsor identification during the registration process. Trusted Agents do not have automated interfaces with CAs (see Section 1.3.5.5).
Trusted Platform Module (TPM)	An international standard for a secure crypto-processor, which is a dedicated microprocessor designed to secure hardware by integrating cryptographic keys into devices.
Trusted Role(s)	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.
TrustID Certificate	A Certificate issued pursuant to the TrustID CP and this CPS.
Trustworthy System	Computer hardware and software that: • Are reasonably secure from intrusion and misuse; • Provide a reasonable level of availability; and • Are reasonably suited to perform their intended functions.

TERM	DEFINITION
Unaffiliated Individual	An Individual not attached or associated with an Organization and wishes to obtain a TrustID Certificate to verify his/her identity and/or an email address.
Unsupervised Remote Identity Proofing	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 which 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 Section 3.2.3.2.1 Remote Identity Proofing for additional details.
Validity Period	The intended term of validity of a Certificate, beginning with the date of Issuance ("Valid From" or "Activation" date), and ending on the expiration date indicated in the Certificate ("Valid To" or "Expiry" date).
Vulnerability Scan	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.
WHOIS	Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.
Wildcard Certificate	A Certificate containing an asterisk (*) in the left-most position of any of the Fully Qualified Domain Names contained in the Certificate.

1.6.2 Acronyms

ACRONYM	DEFINITION
AO	Authorizing Official
ARL	Authority Revocation List
CA	Certification Authority
CAA	Certification Authority Authorization
CMA	Certificate Manufacturing Authority

CMC	Certificate Management Center
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
DBA	Doing Business As
DoS/DDoS	Denial of Service/Distributed Denial of Service
DN	Distinguished Name
DSA	Digital Signature Algorithm
EV	Extended Validation
EWS	Enrollment Workstation
FATCA	Foreign Account Tax Compliance Act
FIPS	Federal Information Processing Standard (US Government)
gTLD	General Top-Level Domain
KED	Key Escrow Database
ICANN	Internet Corporation for Assigned Names and Numbers
IRS	Internal Revenue Service of the United States of America
ISO	International Standards Organization
LRA	Local Registration Agent
OCC	Office of the Comptroller of the Currency
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PED	PIN Entry Device
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure

PMA	Policy Management Authority
PPP	Policy Practices and Procedures
QGIS	Qualified Government Information Source
QGTIS	Qualified Government Tax Information Source
RA	Registration Authority
RFC 6962	Document on Certificate Transparency by the Internet Engineering Task Force (IETF) Organization: https://tools.ietf.org/html/rfc6962
RFPS	Registration Practices Statements
RSA	Rivest-Shamir-Adleman cryptosystem
SSP	System Security Plan
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VBA	Visual Basic Application
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

2.1 REPOSITORIES

IdenTrust operates and maintains a Repository in order 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 both its regular HTTP website (http://identrust.com and subdomains of it) and on its SSL/TLS secured web site HTTPS (https:// identrust.com and subdomains of it). The information is documented in this Section and in the Certificate Profiles Section.

2.1.1 Repository Obligations

IdenTrust maintains a secure system for storing and retrieving currently valid TrustID Certificates, this CPS, the current copy of the TrustID CP, and other information relevant to TrustID Certificates. Information about the status of TrustID Certificates is also maintained in this Repository.

IdenTrust operates the Repository and implements access controls to prevent unauthorized modification or deletion of information.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 Publication of Certificates and Certificate Status

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 are available only for Subordinate CA Certificates and Root CA Certificates issued prior to March 1, 2014

CRLs are also available at: http://crl.identrust.com/ or http://validation.identrust.com/crl/. The specific location depends on the Issuance of the Certificate signing the CRL. For Subordinate CA Certificates issued after March 1, 2014, the second URL is used.

Additional online Certificate status information is available through IdenTrust's TrustID validation services through OCSP. The validation services can be found at: http://ocsp.identrust.com, or commercial.ocsp.identrust.com. For Root CA Certificates issued after March 1, 2014, the second URL is used.

IdenTrust operates and maintains CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less. IdenTrust Root CA Certificates, CRLs, and online TrustID Certificate status information are available for retrieval 24 hours a day, seven days a week, with a minimum of 99% availability overall per year and scheduled downtime does not exceed 0.5% annually, excluding network outages.

2.2.2 Publication of CA Information

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

- Copy of the TrustID CP;
- This TrustID CPS; and
- Other information related to IdenTrust (e.g., notary forms, instruction for bulk loading, etc.).

These web pages are found:

- Within each Certificate Policy field: https://secure.identrust.com/certificates/policy/ts/; or
- At IdenTrust webpage: https://www.identrust.com/support/documents/trustid

The following webpage is available for testing Subscriber Certificates chaining up to IdenTrust publicly trusted root:

https://testssl.identrust.com/

This CPS conforms to the current versions of:

1. The "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published at https://www.cabforum.org
2. The "CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates" published at https://cabforum.org/
3. The "CA/B Forum Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates" published at https://cabforum.org/
4. The "Mozilla Root Store Policy" published at:

   https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/

With regard to Server Certificates or Code Signing Certificates, if any inconsistency exists between this CPS and the guidelines and requirements referenced above, then those guidelines and requirements take precedence.

2.2.3 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 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 PMA also reviews and updates this CPS on an annual basis or more frequently when required, to include the most recent CA/B Forum Baseline Requirements, CA/B Forum Extended Validation SSL Guidelines requirements, CA/B Forum Extended Validation Code Signing Guidelines, 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 authentication of Subscribers with respect to their own 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, RFC 5280 and the CA/B Forum Baseline Requirements 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 flagged as critical.

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

Table 4 - TrustID Certificates Identity Authentication Requirements

TrustID Certificate Type	Identification Requirements
Personal and Medium Assurance Hardware Unaffiliated	Identity shall be established by: Verification of the identity of the Unaffiliated Applicant based on Section 3.2.3 Identification and Authentication of Individual Identity.
Business	Identity shall be established by: Verification of the identity of the affiliated Applicant based on Section: 3.2.3 Identification and Authentication of Individual Identity. Verification of the Organization based on Section 3.2.2 Authentication of Organization Identity.
Administrative CA for Administrators and Registration Authorities	Identity shall be established by: Verification of the identity of the affiliated Applicant based on Section 3.2.3 Identification and Authentication of Individual Identity. Verification of the Organization based on Section 3.2.2 Authentication of Organization Identity.
Administrative CA for Authorized Relying Parties	Identity shall be established by: Verification of the identity of the Relying Party based on Section 3.2.3.12 Authorized Relying Parties.
FATCA Organization	Identity shall be established by: Verification of the Organization based on Section 3.2.2 Authentication of Organization Identity.
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 Section 3.2.3.9 Secure Email Certificate.

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 CA/Browser Forum Guidelines for the Issuance and Management of Publicly-Trusted Certificates" published at https://cabforum.org. When the Subject Distinguished Name is present, it must contain a single IP address or a FQDN that is one 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), authenticity of the Certificate Request, verification of individual 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 CA/Browser Forum Guidelines for the Issuance and Management of Publicly-Trusted Certificates" published at https://cabforum.org.
Server Extended Validation (EV)	Identity for Extended Validation (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 Section 9.2 of the "CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates" published at https://cabforum.org.
Extended Validation Code Signing	Identity shall be established by: Verification of the Applicant's Organization in accordance with Extended Validation Code Signing and Time-Stamping Certificates as set forth in the "CA/Browser Guidelines for the Issuance and Management Of Extended Validation Code Signing Certificates" published at https://cabforum.org.
Time-Stamping	Identity shall be established by: Verification of the Applicant's Organization in accordance with Section 3.2.3.8 Extended Validation Code Signing and Time-Stamping Certificates.
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.

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, within that extension there is a Common Name field, Organization name field, Organization unit, Country, and Locality field and each field 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 Card Authentication Certificate or TrustID Device Certificate will not contain an FQDN as the dNSName, or Common Name.

TrustID Certificate Type	Naming Requirements
Personal and **TrustID Medium Assurance Hardware Unaffiliated**	The DN must include an authenticated commonName must be a combination of first name, surname, and optional initials.
Business; **Administrative CA for Administrators and Registration Authorities;** **Administrative CA for Authorized Relying Parties;** **TrustID FATCA Organization**	In addition to the authenticated commonName (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.
Secure Email	The DN must include a validated email address provided in emailAddress. There is no commonName included in the DN for this type of Certificate.
Device	The DN for a must include a unique name populated in commonName that identifies the electronic Device that will contain the associated Cryptographic Module.
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 flagged 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 flagged as critical. The Subject Distinguished Name must be as set forth in the CA/Browser Forum Guidelines for the Issuance and Management of Publicly-Trusted Certificates" published at https://cabforum.org. 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 Section 9.2 of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates. Wildcard Certificates are not allowed for Server EV Certificates except as permitted under Appendix F of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates. 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.
Extended Validation Code Signing	The DN must include the authenticated legal Subscribing Organization name in commonName. The DN must also include the authenticated legal Subscribing Organization name in organizationName.

TrustID Certificate Type	Naming Requirements
	Optionally, the organizationUnitName may be used to name the Subscribing Organization unit/department that is associated with the Subscriber, if provided by the Subscriber.
Time-Stamping Authority	Time-Stamping Authority Certificates are issued to IdenTrust and used in conjunction with the Time-Stamping Authority Server service. The DN must include the commonName, with a value of "TrustID Timestamp Authority <m>" where <m> is the Iteration of the TrustID Timestamp (e.g. 1, 2) The DN must include organizationName, with a value of "IdenTrust". The DN must also include countryName, with a value of "US".
Card Authentication	TrustID 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, CA Certificates do not contain anonymous or pseudonymous 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 Subject Alternative Name (SAN) extension are interpreted using RFC 5322, formerly 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 RFC 5280 describe how character sets and strings are to be interpreted in Issuer and Subject fields, and Subject Alternative Name (SAN) extension. RFC 2253 explains how an X.500 distinguished name in ASN.1 is translated into a UTF-8 human-readable string representation, and RFC 2616 explains how to interpret Uniform Resource Identifiers (URIs) for HTTP references.

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 name space 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 made possible through the use of an additional naming attribute as part the Subscriber's Subject DN. This attribute is 0.9.2342.19200300.100.1.1, which is an OID for the attribute UID. Whenever IdenTrust issues a Certificate, it calculates a 128-bit Globally Unique ID (GUID) or Universal Unique Identifier (UUID). The GUID/UUID consists of three variables:

- The IP Address of the generator— "the CA system" (4 bytes);
- Time (8 bytes); and
- Sequence number (4 bytes).

The GUID/UUID value, along with the common name of the Subscriber, guarantee uniqueness of the Certificate in the Repository. In the case of TrustID FATCA Organization Certificates, the GUID/UUID along with the

Sponsoring Organization and country guarantee uniqueness of the Certificate in the Repository. The GUID/UUID is converted to a string of hexadecimal numbers, e.g., D01E411A000000E1A341CAC00000001.

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 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, IdenTrust may implement these as well; in order to increase application interoperability of Certificates.

3.1.5.1 Human 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.

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

3.1.5.3 Device Certificates

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

3.1.5.4 Server Certificates

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

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

3.1.5.5 Extended Validation Code Signing Certificates

For Extended Validation Code Signing Certificates, the uniqueness of the Subject DN is ensured by inclusion of 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-stamp 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 in order 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 prior to the Issuance of TrustID Certificates. IdenTrust performs Identity Proofing itself, aided by its own 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:

Table 5 - TrustID Certificates Initial Identity Validation Requirements

Certificate Type	Identification Requirements
Personal	Verification of the identity of the unaffiliated Applicant based on Section 3.2.3 and the performance of an Electronic Identification based on Section 3.2.3.4 or the performance of in-person or Unsupervised Remote Identity Proofing based on Section 3.2.3.2; and Verification of email based on Section 3.2.8.
Medium Assurance Hardware Unaffiliated	Verification of the affiliated Applicant based on Section 3.2.3 and performance of in-person or Unsupervised Remote Identity Proofing based on Section 3.2.3.2; and Verification of email based on Section 3.2.8.
Business	Verification of the affiliated Applicant based on Section 3.2.3 and performance of in-person or Unsupervised Remote Identity Proofing based on Section 3.2.3.2; Verification of the Organization based on Sections 3.2.2; Verification of Individual-Organization affiliation based on Section 3.2.2.1; Verification of email based on Section 3.2.8; and Verification of a Certificate request based on Section 3.2.9.
Server *	Verification of the Organization based on Sections 3.2.2; Verification of the PKI Sponsor's Organization affiliation based on Section 3.2.2.3;

Certificate Type	Identification Requirements
	Verification of a Certificate request based on Section 3.2.9; Authentication of a Device identity based on Section 3.2.2.6; Verification against high risk and denied request lists based on Section 4.2.2.2; Verification of the authorization by Domain Name Registrant based on Section 3.2.2.5. Verification of DBA/tradename based on Section 3.2.2.3.1; Verification of country code based on Section 3.2.2.3.2; Verification of control over entire namespace delimited by the FQDN of wildcard Certificate on Section 3.2.2.3.4; Verification of email based on Section 3.2.8**; and Verification of IP address based on Section 3.2.2.5. In addition to the applicable requirements above, adherence to the applicable requirements listed in the in "The CA/Browser Forum Guidelines for the Issuance and Management of Publicly-Trusted Certificates" published at https://cabforum.org.
Server Extended Validation (EV)	In addition to the applicable verification requirements for Server Certificate listed above, adherence to the requirements listed in the CA/B Forum EV SSL Guidelines, available at https://cabforum.org/
Extended Validation Code Signing and Time-Stamping	A TrustID Extended Validation 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 Extended Validation Code Signing Certificate or TrustID Time-Stamping Certificate, the Issuing CA shall conform with the applicable provisions set forth in the "CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates" published at https://cabforum.org/.
FATCA Organization	Verification of the Organization based on Section 3.2.2 and 3.2.2.1; Verification of PKI Sponsor-Organization affiliation based on Section 3.2.2.3; Verification of email based on Section 3.2.8; and Verification of a Certificate request based on Section 3.2.9.
Administrative RA Certificates	The Subscriber 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.
Secure Email	Demonstration of the Applicant's control of the email address at the time of email verification, based on Section 3.2.8 Verification of Email Address.
Card Authentication Certificate	Demonstration that the associated RA, or the CA has assigned a unique name for identifying the Cryptographic Module.
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.

Certificate Type	Identification Requirements
Authorized Relying Parties	Identification and of 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 27 or more months prior to the Issuance of the Certificate or in the case of Server Extended Validation and Extended Vallidation Code Signing Certificates, the age of all data used to support renewals will not exceed the period specified in Section 11.14.3 of the the CA/B Forum Guidelines for the Issuance and Mangement of Extended Validation Certificates, available at https://cabforum.org/. For TrustID Server Domain Validation Certificates, the validation is limited to the FQDN.

**This check is only performed when necessary for Server Certificates. It will be performed when the profile of the requested Server Certificate specifies an e-mail 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 4.3. 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 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 Certificate 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 ensure 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 IdenTrust of the 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;
- Type of entity;
- Year of formation;
- Names of directors and officers;
- Address;
- Telephone number; and
- Proof of good standing in the jurisdiction where the Applicant is incorporated or otherwise organized.

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, and by calling the Sponsoring Organization's telephone number. IdenTrust and 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 Certificate 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 Certificate 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 an independently verified point of contact, i.e., IdenTrust or the RA obtains telephone numbers for the Sponsoring Organization from a trusted source unrelated to the prospective Sponsoring Organization. The contact actually 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.

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.

3.2.2.2 Authentication of Subscribing Organization Identity

Prior to 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, and the telephone number 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, and telephone number of the Organization, which are verified through a telephone call with a representative of the Organization made to the telephone number independently obtained by LRA or Trusted Agent;

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), telephone number, and, when deemed necessary, Domain Name registration, 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 the CA/B Forum EV SSL Guidelines and CA/B Forum EV Code Signing Guidelines, available at https://cabforum.org/.

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 prior to 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 an independently verified point of contact, i.e., IdenTrust or the RA obtains telephone numbers for the Sponsoring Organization from a trusted source unrelated to the prospective Sponsoring Organization. The contact actually 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 Server Extended Validation 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 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. In order 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 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 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 Sections 3.2.2 and 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 two-letter country code (ccTLD) (e.g., www.identrust.uk as opposed to www.identrust.com), this confirmation will be sought from the Domain Name level to which the ccTLD applies. This means that the LRA cannot obtain verification from www.identrust.com if the PKI Sponsor is applying for a Domain Name from www.identrust.uk.

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

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 has never issued a Server Certificate 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

Prior to 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 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 Verification of Authorization by Domain Name Registrant

Prior to Server Certificate Issuance, IdenTrust verifies that the PKI Sponsor has the right to use or has control of the FQDN (s) listed in the Server Certificate application by following one or more of the validation methods listed below, maintaining a record of which of the Domain Name validation or IP Address validation methods described below and in Section 4.2 Certificate Application Processing, including the relevant CA/B Forum Baseline Requirements version number used.

Additional checks and verification will be made for Server EV Certificate applications based on the requirements within the CA/B Forum Extended Validation Guidelines, available at https://cabforum.org/.

3.2.2.4.1 Email to Domain Contact

The LRA confirms the Domain Registrant's control over the FQDN by doing the following:

1. The Domain(s) supplied by the PKI Sponsor is placed into a search engine (e.g., WHOIS) and the LRA records the contact information for the Domain Name Registrant.
2. Once the Domain Name Registrant is identified from a database record, he or she is contacted via email sending a Random Value unique to the email. In this email the Domain Name Registrant will be asked:
    a. to confirm response utilizing the Random Value;
    b. to confirm or deny the right of the PKI Sponsor to be issued a Server Certificate for the Domain Name(s) for which the PKI Sponsor has applied;
    c. with respect only to applications for wildcard Certificates, to confirm or deny control over the entire Domain Namespace of the FQDN provided and that such control is rightful.

After confirmation has been received, the LRA will check the email string from the domain administrator for accuracy to confirm or deny the PKI Sponsor's right to apply for a Server Certificate for the specified FQDN(s).

In cases where the registered domain holder cannot be contacted, the LRA will reject the Server Certificate application.

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

This validation method is in line with CA/B Forum Baseline Requirements Section 3.2.2.4.2.

3.2.2.4.2 Constructed Email to Domain Contact

The LRA confirms the Domain Registrant'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, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

After confirmation has been received, the LRA will check the email string from the domain administrator for accuracy to confirm or deny the PKI Sponsor's right to apply for a Server Certificate for the specified FQDN(s).

In cases where the registered domain holder cannot be contacted, the LRA will reject the Server Certificate application.

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

This validation method is in line with CA/B Forum Baseline Requirements Section 3.2.2.4.4.

3.2.2.4.3 DNS Change

The LRA confirms the Domain Registrant's control over the FQDN by confirming the presence of a Random Value 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 label that begins with an underscore character.

The Random Value used is unique to the Server Certificate request and shall not be used after (i) 30 days or (ii) if the Domain Registrant submitted the Server Certificate request, the timeframe permitted for reuse of validated information relevant to the Server Certificate as described in Section 4.1.1 or Section 11.14.3 of the CA/B Forum Extended Validation Guidelines.

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

This validation method is in line with CA/B Forum Baseline Requirements Section 3.2.2.4.7.

3.2.2.4.4 Agreed-Upon Change to Website

The LRA confirming the Applicant's control over the FQDN by verifying that the Random Value is contained in the contents of a file.

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

The file containing the Random Number:

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 the CA follows redirects the following apply:

1. Redirects must be initiated at the HTTP protocol layer (e.g. using a 3xx status code).
2. Redirects must be the result of an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4.3.
3. Redirects must be to resource URLs with either via the "http" or "https" scheme.
4. Redirects must be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:

1. The IdenTrust CA 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. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS

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

This validation method is in line with CA/B Forum Baseline Requirements Section 3.2.2.4.18.

3.2.2.5 Authentication for an IP Address

IdenTrust as Issuing CA shall confirm that prior to 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 time period specified in the relevant requirement such as those in Section 4.2.1 for Server Certificates, prior to 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 CA/B Forum Baseline Requirements version number that was used to validate every IP Address.

IP Addresses verified in accordance with this section may be listed in Server Certificates as defined in Section 7.1.4.2.

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 such as those in Section 4.2.1 for Server Certificates.

This validation method is in line with CA/B Forum Baseline Requirements Section 3.2.2.5.1.

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 mail 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 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.

This validation method is in line with CA/B Forum Baseline Requirements Section 3.2.2.5.2.

3.2.2.6 Authentication of 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, Table 5. 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.

3.2.2.6.1 Extended Validation Code Signing Certificates

Likewise, checks and verifications will be made for EV Code Signing Certificate applications based on the requirements within the CA/B Forum EV Code Signing Guidelines available at https://cabforum.org/.

3.2.2.6.2 Card Authentication Certificate and Device Certificates

For TrustID Card Authentication Certificates and TrustID 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 Device Certificate, the assigned unique identifier may identify an Electronic Device.

3.2.2.7 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. In order 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 will be based upon IdenTrust authenticating the identity of the Applicant as explained in this and 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. 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 it appears in the Certificate's Common Name attribute;
- Method of application (e.g., online, in-person, remote);
- For each data element accepted for verification, including electronic forms:
  - Name of 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
- 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 Issuance of a TrustID Certificate who apply in person must present satisfactory proof of identity.

1. The following are considered by the TrustID Policy to be acceptable “Government-issued photo IDs” 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 the identity verification is performed in-person, the Applicant/PKI Sponsor meets with an Individual authorized to collect the appropriate information and verify the Applicant’s/PKI Sponsor’s identity. See conditions for remote Identity Proofing provided later in this section.

In-person identification may be 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.).

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.

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 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 to the RA. The complete paper forms need to be reviewed by the LRA prior to 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 two 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 only 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 are eligible for automated, 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 a 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 which addresses at least the following topics:
3. Scheduling a Remote Identity Proofing session.
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 TrustID 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 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.

3.2.3.4 Electronic Identification

When the authentication is performed through an automated/online 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 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 valid state-issued driver's license number or state-issued identification card number.

In addition to the requirements above, the Applicant must also provide two or more of "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 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 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 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 Authentication of Subscribers for Role-based Certificates

Role-based Certificates are currently not issued under this CPS.

3.2.3.7 Authentication of Subscribers for Group Certificates

Group Certificates are currently not issued under this CPS.

3.2.3.8 Extended Validation Code Signing and Time-Stamping Certificates

A TrustID Extended Validation 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 Extended Validation Code Signing Certificate or TrustID Time-Stamping Certificate, IdenTrust as Issuing CA conforms with the provisions of the current version of "CA/B Forum Guidelines for Issuance and Management of Extended Validation Certificates" published at https://cabforum.org/. In the event of any conflict between the provisions of this CPS and the provisions of the above referenced document, then the provisions of above referenced document, as applicable, shall govern. A TrustID Extended Validation 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.

3.2.3.9 Secure Email Certificate

For Secure Email Certificates, at the time of email address verification during authentication prior to 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. Email addresses are interpreted using RFC 5322, formerly RFC 822, specifying the format of Internet email messages.

For Certificates supporting the secure/multipurpose internet mail extensions (S/MIME) protocol, email address validation is always handled by IdenTrust as Issuing CA using the validation methods described in the Verification of Email Address or section.

3.2.3.10 TrustID Card Authentication Certificate

For TrustID 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 Subject Name of the TrustID Card Authentication Certificate issued to the Cryptographic Module.

3.2.3.11 TrustID Device Certificate

For a TrustID 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 Device Certificate issued to the Electronic Device containing the Cryptographic Module storing the corresponding Key Pair.

3.2.3.12 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 document on Appendix A of this CPS, which only allow certain information to be included in Certificates. The processes described in Sections 3.0 and 4.0 of this CPS 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 on 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.

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 of this CPS;
- Issue Certificates compliant with the profiles described in the TrustID CP 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.

3.2.7 Verification and Validation of Information

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

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

3.2.7.1 Verification and Validation of Personal, Business, and VBA 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 two acceptable forms of ID, one of which shall be a Government-issued photo ID as described and required in Sections 3.2.3, 3.2.3.1, 3.2.3.2 dependent on the type of application and Certificate that is requested as listed in Table 5 of Section 3.2.

3.2.7.2 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 two additional verifications of information may be conducted prior to Issuance in order 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 4.2.2.4; and
- High-risk denials, as documented in Section 4.2.2.3, 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.

Should a third party vendor be utilized to confirm 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.

3.2.7.3 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 information available through the tool only to resolve exceptions during an application. The absence from the list

will not result on 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.

3.2.8 Verification of Email Address

Email verification when required can be done in two 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.

3.2.8.1 Electronic Verification of Email

When an Applicant/PKI Sponsor submits an application through a secure online form, an automated email is sent to the email address provided in the application. Within that automated email message there is a link that guides the Applicant/PKI Sponsor to a server-authenticated SSL/TLS secured web site and instructions to provide a one-time email verification code and the Account Password. This Account Password was created during the application by the Applicant/PKI Sponsor and it is known only to the Applicant/PKI Sponsor. When the Applicant/PKI Sponsor provides and submits the Account Password created during the application the verification of the email address is completed and the verification status is automatically updated within the Applicant/PKI Sponsor's application record.

3.2.8.2 Manual Verification of Email

When a Trusted Agent provides the list of authorized Applicants/PKI Sponsors, the email address is validated by the Trusted Agent based on the internal knowledge of the Sponsoring Organization. The Trusted Agent may use internal databases and directories to ensure the email accuracy.

3.2.8.3 Demonstration of Control of an Email Address for a Secure Email Certificate

Control of the email address at the time of email verification is demonstrated via an automated process, the steps of which are set forth below:

- Upon submission of a Certificate application, a system-generated email is sent to the Applicant provided email address that will be included in the Certificate.
- The automated email contains a unique, system generated code to be used for email validation and a link to a website that is used for email verification.
- Upon receipt of the automated email, the recipient will visit the email verification website, via the link provided, and will provide the unique, system-generated code and the password selected by the Applicant during initial registration.
- Both the unique code and the Applicant selected password must be successfully validated against the CA database before the Certificate application can be approved.

Successful submission of the unique, system generated code in combination with the Applicant provided password, by the email recipient, constitutes demonstration of control of the email address by the initial Applicant at the time of email verification.

3.2.9 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 contact the phone number provided during the application process and ask for verification of the request from the Applicant.

To verify the authenticity of a Server or FATCA Organization Certificate's request, the LRA contacts the PKI Sponsor via the company/Organization telephone number independently verified through a third party database. The LRA will request to speak to the PKI Sponsor at the Organization telephone number and upon confirming identity, will ask the PKI Sponsor to verify the validity of the request.

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 Server EV Certificate applications based on the requirements within the CA/B Forum Extended Validation Guidelines, available at https://cabforum.org/.

Likewise, checks and verifications will be made for EV Code Signing Certificate applications based on the requirements within the CA/B Forum EV Code Signing Guidelines available at https://cabforum.org/.

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 three months prior to 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 Table 5 of 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 prior to 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 Table 5 of 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 is Section 4.9.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

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 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 Certificate Agreement.
- An Individual who is already a Subscriber of this type of Certificate.

4.1.1.2 Business Certificates, Organization/Business VBA Certificates

- An Individual who is affiliated with a Sponsoring Organization, through an employment, contractual or agency relationship, and agrees to the terms of the Certificate 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 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 Server EV Certificates Subjects are made in accordance with the CA/B Forum Extended Validation Guidelines available at https://cabforum.org/.
- Likewise, checks and verifications will be made for EV Code Signing Certificate applications based on the requirements within the CA/B Forum EV Code Signing Guidelines available at https://cabforum.org/.

4.1.1.4 FATCA Organization Certificates

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

4.1.1.5 RA Systems Certificates

- 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 in a Certificate of incumbency.

4.1.2 Enrollment Process and Responsibilities

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 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.

4.1.3 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 own 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 Sections 3 and 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 web site 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 4.1.2.3; 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.

4.1.3.1 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.

4.1.3.1.1 Bulk-Loading by Trusted Agents

The Sponsoring Organization in conjunction with IdenTrust or the RA appoints Trusted Agent(s) to assist with processing of requests for the Issuance of Certificates. Trusted Agents undergo Identity Proofing in accordance with Sections 3.2.2, 3.2.3, and 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 Sections 3.2.2 and 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.

4.1.3.1.2 Bulk Loading by Enterprise RAs

The Sponsoring Organization in conjunction with IdenTrust appoints Enterprise RAs to assist with processing of requests for the Issuance of Server Certificates. An Enterprise RA, who is current with requirements of 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.

4.1.3.2 Data Collected during Enrollment Process

All Applicants and PKI Sponsors must provide the following as described in the following subsections based on Certificate type:

4.1.3.2.1 Data Collection by Certificate Type

4.1.3.2.1.1 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.

4.1.3.2.1.2 Business Certificates, Business/Organization VBA 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.

4.1.3.2.1.3 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 for Business Entities in the CA/B Forum Extended Validation Guidelines; and
- Additional checks will be in place based on requirements listed in the CA/B Forum EV Code Signing Guidelines

4.1.3.2.1.4 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.

4.1.3.2.1.5 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.

4.1.3.2.2 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 are able to 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 in order 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.

4.1.3.2.3 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 enable access to the TrustID CP and this CPS; and the Certificate Agreement that is provided during the enrollment process.

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 TrustID CPS and CP.

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 RFC 8659.
Issuewild property tags are ignored, unless the request is for a wildcard Certificate. See Verification of Control over Entire Namespace Delimited by FQDN of a Wildcard Certificate.

To prevent resource exhaustion attacks, IdenTrust limits the length of CNAME chains that are accepted and process 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 the Section Time to Process Certificate Applications.

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 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, the that extension must be marked critical

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 825 days prior to issuing the Certificate. For Server Extended Validation and Extended Validation Code Signing Certificates, the age of all data used to support renewals shall not exceed more than thirteen months as specified in Section 11.14.3 of the CA/B Forum Guidelines For the Issuance and Management of Extended Validation Certificates. . Effective September 1, 2020, re-use of previous validations is limited to no more than 397 days for all Server Certificates.

4.2.2 Approval or Rejection of Certificate Applications

For Non-Server Certificates or EV Code Signing Certificate applications, IdenTrust and RAs appoints 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 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 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' is 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 Identity Proofing process; and
- Informing the Applicant/PKI Sponsor of the process necessary to resume 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 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

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" was 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" was 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 Certificates are properly verified, IdenTrust and RAs conduct two 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 prior to 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 for Business Entities in the CA/B Forum Extended Validation SSL Guidelines; and
- Additional requirements as specific for Business Entities in the CA/B Forum Extended Validation Code Signing Guidelines.

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 in order to commit fraudulent or phishing activities (e.g., www.g00gle.com, www.1dentrust.com, etc.) and specific filters that are established at the system level to deny initial applications (e.g., non-US ASCII characters);
- Manual review of all documents and information provided; and/or
- Other verifiable proof as deemed necessary by RA or IdenTrust management.

4.2.2.4 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 human sponsored Certificate and its Issuance. However, the Issuing CA should respond promptly to all such applications.

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

4.3 CERTIFICATE ISSUANCE

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 has published the Subscriber's Certificates to IdenTrust's Repository.

4.3.1 CA Actions during Certificate Issuance

Both 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.

4.3.1.1 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 application process described in Section 4.1. This two-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 prior to 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 are 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 IdenTrust's or the RA's Retrieval URL, and the Subscriber's client platform. The now 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.

4.3.1.2 Issuance via Secure Website for Server Certificates

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 3.2;
6. The PKI Sponsor has signed and is bound by the Certificate 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.

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

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

4.3.1.3 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 store 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 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
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 biometric (if collected) are securely transferred into the smart card.
5. The TA or LRA different then 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 prior to Certificate Issuance explained in Section 4.3.; IdenTrust, Enterprise RA or the RA notifies the Applicant/PKI Sponsor about the approval of the Certificate. Notifications 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 that is associated to 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 (as specified in Section 4.3.1).

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 Certificate Agreement. The Certificate 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 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 Certificate 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 Certificate Agreement, this CPS, the TrustID CP and any other obligations that the Subscriber may otherwise have;
- 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 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 Certificate Agreement online or in paper copy; or, by undergoing a full registration process prior to receiving the Certificate. Additional information concerning the rights and obligations of Subscribers may be found in Sections 9.6.1.2 of this CPS.

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 4.9.

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 further renewed.

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 an

825-day lifetime[1] Re-key period with an initial issue and two annual renewals before Re-Rey 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 in the Repository, which is disclosed in the End Entity and Subordinate CA Certificates themselves.

The subjectName 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.

[1] Effective September 1, 2020 must not exceed 397 days.

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 Sections 3.3 and.3.3.1).

4.7.3 Processing Certificate Re-Keying Requests

For human Subscribers, three months prior to the expiration period, the IdenTrust or the RA's system will 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 prior to the expiration period, the IdenTrust or the RA's system will 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 Definitions.)

IdenTrust offers re-key services through subscription renewal rekey. Beginning ninety (90) days prior to the expiration of a human Certificate and thirty (30) days for Server Certificates, e-mail 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 if the following criteria is met:

- The maximum Validity Period for Key Pair Usage as defined in Section 6.3.2 Certificate Operational Periods and Key Pair Usage Periods, 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 Server EV Certificates, EV Code Signing Certificates, in accordance with the CA/B Forum Extended Validation SSL Guidelines and the CA/B Forum EV Code Signing Guidelines available at https://cabforum.org/

IdenTrust will authenticate the Subscriber by using the Identity Proofing processes required for the corresponding Certificate in Table 5 of Section 3.2. Once the Subscriber is authenticated, IdenTrust will then follow the TrustID Certificate Issuance process described in Section 4.3.

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.

4.7.6 Publication of the Re-Keyed Certificate by the CA

See Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8 CERTIFICATE MODIFICATION

Certificate modification consists of creating new Certificates with Subject information that may differ from the old Certificate. IdenTrust provides two 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., 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 Subject Alternative Name (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 in order for 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 (Identification of Individual Identity) and Section 4.1.1 (Who can submit a Certificate application) for specific details.

IdenTrust may request a modification of its own 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 provided in written 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.

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 4.4.3.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

4.9.1.1 Non-Server Certificates

Prior to 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 or Applicant with whom a Certificate application is affiliated may request written Revocation of his or her TrustID Certificate at any time for any reason;
- The Applicant of an approved Secure Email Certificate notifies IdenTrust that the Domain Name email address associated with the individual holding the Certificate is no longer affiliated with the Organization.
- 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 is compromised.
- 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 (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);
- 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.
- A Sponsoring Organization requests IdenTrust Revocation of a TrustID Certificate issued to its Affiliated Individual or a Device at any time for any reason.
- IdenTrust may revoke any Certificate deemed out of compliance.
- For Extended Validation Code Signing Certificates, the Certificate has been used to sign, publish or distribute malware, downloaded without user consent or other malicious purpose.
- For Certificates used to sign Adobe documents, Adobe has requested Revocation.

4.9.1.2 Server Certificates

IdenTrust shall revoke a Certificate within 24 hours and must revoke a Certificate within 5 days if one or more of the following events take place:

- The Certificate no longer complies with the requirements in the relevant section of the CA/B Forum Baseline Requirements.
- IdenTrust obtains evidence that the Certificate was misused.
- The Subscriber or the cross-certified CA breached a material obligation under this CPS, the TrustID CP, or the relevant agreement.
- IdenTrust confirms any circumstance indicating that use of a FQDN or IP Address in the Server Certificate is no longer legally permitted.
- IdenTrust confirms that a wildcard Server Certificate has been used to authenticate a fraudulently misleading subordinate FQDN.

- IdenTrust confirms a material change in the information contained in the Certificate.
- IdenTrust confirms that the Certificate was not issued in accordance with the CA/B Forum Baseline Requirements, this CP or IdenTrust TrustID CPS.
- IdenTrust determines or confirms that any of the information appearing in the Certificate is inaccurate.
- IdenTrust's right to issue Certificates under the CA/B Forum Baseline Requirements expires or is revoked or terminated, unless the IdenTrust has made arrangements to continue maintaining the CRL/OCSP Repository.
- IdenTrust confirms a demonstrated or proven method that exposes the Subscriber's Private Key to compromised methods or if there is clear evidence that the specific method used to generate the Private Key was flawed.

The Issuing CA may revoke any Certificate in its sole discretion, even if the Issuing CA believes that:

- Either the Subscriber's or the Issuing CA's obligations under this CP or the CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised.
- The Issuing CA received a lawful and binding order from a government or regulatory body to revoke the Certificate.
- The Issuing CA ceased operations and did not arrange for another Certificate authority to provide Revocation support for the Certificates.
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Providers, Relying Parties, or others.
- The Subscriber was added as a denied party or prohibited person to a blacklist or is operating from a destination prohibited under the laws of the United States.

The Issuing CA shall revoke a Certificate if the binding between the Subject and the Subject's Public Key in the Certificate is no longer valid or if an associated Private Key is compromised.

IdenTrust shall revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

- The Subordinate CA requests Revocation in writing.
- The Subordinate CA notifies IdenTrust that the original Certificate request was not authorized and does not retroactively grant authorization.
- 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 in the relevant sections of the CA/B Forum Baseline Requirements.
- IdenTrust obtains evidence that the CA Certificate was misused.
- IdenTrust confirms that the CA Certificate was not issued in accordance with or that Subordinate CA has not complied with the applicable Certificate Policy or Certification Practice Statement.
- IdenTrust determines that any of the information appearing in the CA Certificate is inaccurate or misleading.
- 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.
- IdenTrust or the Subordinate CA's right to issue Certificates under the CA/B Forum Baseline Requirements expires or is revoked or terminated, unless IdenTrust has made arrangements to continue maintaining the CRL/OCSP Repository.
- The technical content or format of the CA Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

4.9.1.3 Certificate Problem Reporting

IdenTrust provides Certificate Holders, 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 support section 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.

Once a report is received either by email or telephone call, a Customer Support Representatives 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. Certificate Holder, 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 Certificate Holder;
3. The entity making the complaint (for example, a complaint from a law enforcement official that a web site 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 evening, weekend or holiday hours.

4.9.2 Who Can Request Revocation

The only persons permitted to request Revocation or suspension of a TrustID Certificate issued pursuant to the TrustID CP are the Applicant in the case of a Server or a Secure Email Certificate, the Subscriber, the PKI Sponsor on behalf of the Sponsoring Organization, IdenTrust, the RA, an Enterprise RA or Trusted Agent who performed the Identity Proofing process.

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 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 in order 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.

The Subscriber or the PKI Sponsor is required to indicate the reason for the Revocation request. 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. Reason codes are included in the CRLs issued by IdenTrust, including the reason code of Revocation because of Private Key compromise.

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 following 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

Prior to 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 is 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 Sections 4.9.7 and 4.9.8. The Certificate information (i.e., serial number) remains in the CRL until after the Certificate expiration date.

4.9.3.3 Procedure for Revocation by IdenTrust

4.9.3.3.1 End-Entity Certificates

IdenTrust may revoke a Certificate within 24 hours and will revoke a Certificate within 5 days if one or more of the following events take place:

- The Certificate no longer complies with the requirements of the CA/B Forum Baseline Requirements.
- IdenTrust obtains evidence that the Certificate was misused.
- The Subscriber or the cross-certified CA breached a material obligation under the CP, this CPS, or the relevant agreement.
- For Server Certificates IdenTrust confirms any circumstance indicating that use of a FQDN or IP Address in the Certificate is no longer legally permitted.
- For Server Certificates IdenTrust confirms that a wildcard Certificate has been used to authenticate a fraudulently misleading Subordinate CA FQDN.

- For Extended Validation Code Signing Certificates, the Certificate has been used to sign, publish or distribute malware, downloaded without user consent or other malicious purpose.
- IdenTrust confirms a material change in the information contained in the Certificate.
- IdenTrust confirms that the Certificate was not issued in accordance with the CA/B Forum Baseline Requirements or the IdenTrust TrustID CP or this CPS.
- IdenTrust determines or confirms that any of the information appearing in the Certificate is inaccurate.
- IdenTrust's right to issue Certificates under the CA/B Forum Baseline Requirements expires or is revoked or terminated, unless IdenTrust has made arrangements to continue maintaining the CRL/OCSP repository.
- Revocation is required by the IdenTrust TrustID CP and/or this CPS.
- IdenTrust confirms a demonstrated or proven method that exposes the Subscriber's Private Key to compromised methods or if there is clear evidence that the specific method used to generate the Private Key was flawed.

At its own discretion, IdenTrust may revoke any Certificate if it believes that:

- Either the Subscriber's or IdenTrust's obligations under the CP or this CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised.
- IdenTrust received a lawful and binding order from a government or regulatory body to revoke the Certificate.
- IdenTrust ceased operations and did not arrange for another Certificate authority to provide Revocation support for the Certificates.
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Providers, Relying Parties, or others.
- The Subscriber was added as a denied party or prohibited person to a blacklist or is operating from a destination prohibited under the laws of the United States.
- For Certificates used to sign Adobe documents, Adobe has requested Revocation.
- For Extended Validation Code Signing Certificates, the Certificate was used to sign, publish, or distribute malware, code that is downloaded without user consent, or other harmful content.

IdenTrust always revokes a Certificate if the binding between the Subject and the Subject's Public Key in the Certificate is no longer valid or if an associated Private Key is compromised.

IdenTrust will revoke the Certificate:

- If the Private Key is suspected of compromise;
- If the Subscriber can be shown to have violated the stipulations of the Certificate Agreement;
- If IdenTrust learns, or reasonably suspects, that the Subscriber's Private Key has been compromised;
- If IdenTrust determines that the TrustID Certificate was not properly issued in accordance with the TrustID CP or the TrustID CPS;
- Other circumstances requiring Revocation exist within the TrustID CP or this CPS (e.g., the binding in the Certificate between Subject attributes and the Subject's Public Key are no longer considered valid).

IdenTrust may also revoke a Certificate:

- Upon failure of the Subscriber (or the Sponsoring Organization, where applicable) to meet its obligations under the TrustID CP, this CPS, or an applicable agreement, regulation, or law;

- Upon a determination that the Certificate has become unreliable or that material information in the application for a Certificate or in the Certificate itself has changed or has become false or misleading (e.g., the Subscriber changes his or her name);
- A governmental authority has lawfully ordered IdenTrust to revoke the Certificate; or there are any other grounds for Revocation. An agreement with a Sponsoring Organization or participating agency may limit or extend these circumstances for Revocation;
- If IdenTrust ceases operations for any reason and has not made arrangements for another CA to provide Revocation support for the Certificate; and/or
- IdenTrust's right to issue Certificates under the Policy OID for Subject identity validated type Certificates (see Section1.2.2) expired, revoked or terminated, unless IdenTrust has made arrangements to continue maintaining the CRL/OCSP Repository.

4.9.3.3.2 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, prior to 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.

4.9.3.3.3 Subordinate CA Certificates

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

- The Subordinate CA requests Revocation in writing.
- The Subordinate CA notifies IdenTrust that the original Certificate request was not authorized and does not retroactively grant authorization.
- 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 the CA/B Forum Baseline Requirements.
- IdenTrust obtains evidence that the CA Certificate was misused.
- IdenTrust confirms that the CA Certificate was not issued in accordance with or that Subordinate CA has not complied with this CPS or the applicable Certificate Policy or Certification Practice Statement.
- IdenTrust determines that any of the information appearing in the CA Certificate is inaccurate or misleading.
- IdenTrust or the Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide Revocation support for the CA Certificate.
- IdenTrust or the Subordinate CA's right to issue Certificates under the CA/B Forum Baseline Requirements expires or is revoked or terminated, unless IdenTrust has made arrangements to continue maintaining the CRL/OCSP Repository.
- Revocation is required by IdenTrust's Certificate Policy and/or Certification Practice Statement.
- The technical content or format of the CA Certificate presents an unacceptable risk to Application Software suppliers or Relying Parties.

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 Sections 3.2.2 and 3.2.3.

4.9.3.5 Procedure for Revocation by Non-Authorized Requestors

Any Certificate Revocation requests from other, non-authorized requesters must be submitted to IdenTrust. If IdenTrust determines that Revocation is appropriate, it will be revoked it 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 prevents an LRA or Enterprise RA from requesting or approving the Revocation of Certificates of Subscribers who are not within their own 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 is 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 brief explanation of the reasons for Revocation and to archive such notice. The CA 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.

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 will revoke a CA Certificate within one hour after receiving clear instructions from the PMA.

Within 24 hours after receiving a Certificate Problem Report, IdenTrust investigates the facts and circumstances related to a Certificate Problem Report and will 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 works 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 in 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. The date selected by IdenTrust will consider the following criteria:

- The nature of the alleged problem (scope, context, severity, magnitude, risk of harm).
- The consequences of Revocation (direct and collateral impacts to Subscribers and Relying Parties).
- The number of Certificate problem reports received about a particular Certificate or Subscriber.
- The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered).
- Relevant legislation.

Under normal operating circumstances, IdenTrust will revoke Certificates as quickly as practical after validating the Revocation request following the guidelines of this section and Section 4.9.1, generally within the following time frames:

- Certificate Revocation requests for publicly-trusted Certificates are processed within 18 hours after their receipt.
- Revocation requests received two or more hours before CRL Issuance are processed before the next CRL is published.
- Revocation requests received within two hours of CRL Issuance are processed before the following CRL is published.

4.9.6 Revocation Checking Requirements for Relying Parties

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. 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 updates and reissues CRLs at least (i) once every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field is not more than twelve months beyond the value of the thisUpdate field.

When CRLs are used to distribute status information:

- They are issued periodically, even if there are no changes to be made, to ensure timeliness of information; and
- Superseded Certificate status information is removed from the Repository system upon posting of the latest Certificate status information.

4.9.7.1 CRL Checking Requirements

Authorized Relying Parties who rely on a CRL must in their validation requests check a current, valid CRL for the Issuing CA in the Certificate path and obtain a current CRL.

4.9.8 Maximum Latency for CRLs

IdenTrust publishes a CRL within one hour of 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

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

4.9.10 Online Revocation Checking Requirements

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.

IdenTrust supports an OCSP capability using the GET Method for retrieval of validation information for Certificates issued in accordance with the CA/B Forum Baseline Requirements.

For the status of Subscriber Certificates:

Prior to September 30, 2020: The IdenTrust CA shall update information provided via an Online Certificate Status Protocol at least every four days. OCSP responses from this service have a maximum expiration time of ten days.

Effective September 30, 2020:

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

For the status of Subordinate CA Certificates:

OCSP responses issued for the Root Certificate last 7 days and the next update is available at 3.5 days. OCSP responses issued for Subordinate CA Certificates last for 24 hours and the next update is available at 12 hours.

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, the responder will not respond with a “good” status for such requests.

The IdenTrust CA monitors the OCSP responder for requests for “unused” serial numbers as part of its security response procedures.

The OCSP responder may provide definitive responses about "reserved" Certificate serial numbers, as if there was a corresponding Certificate that matches the Precertificate as described in the RFC6962.

A Certificate serial number within an OCSP request is one of the following three options:

1. "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
2. "reserved" if a Precertificate as described in the RFC6962 with that serial number has been issued by (a) the Issuing CA; or (b) a Precertificate Signing Certificate as described in the RFC6962 associated with the Issuing CA; or
3. "unused" if neither of the previous conditions are met

4.9.11 Other Forms of Revocation Advertisements Available

IdenTrust does not support any other method for obtaining Certificate status information than those described in Sections 4.9.7 and 4.9.9. 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. 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 Server or FATCA Organization Certificates and the Repository must not include these Certificate types in suspended state

4.9.14 Who Can Request Suspension

See Section 4.9.2.

4.9.15 Procedures for Suspension Request

A suspension may be requested at any time for any reason. In order 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 three 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 two 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 the 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 in the IdenTrust support webpage.

In order 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 two 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 the 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 Sections 7.2 and 7.3 mainly.

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 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 Extended Validation Code Signing Certificates which remain on the CRL or OCSP for at least 10 years after revoked or expired.

4.10.2 Service Availability

See Section 2.2.1.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

4.11.1 End of Subscription for Subscribers

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.

Prior to the end of 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 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).

4.12.1.3 Procedure for Private Key Recovery Request

4.12.1.4 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 Certificate Agreement and the Certificate Policy for the corresponding product.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

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

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

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 three 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 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.

5.1.1 Site Location and Construction

The construction and location of the building housing the IdenTrust's CA system has 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 damages, 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 own 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 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 two-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 own 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 protections 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 two-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 two-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 that still allows for enough personnel to cover the needs of IdenTrust's diverse customer base. Two-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. Two 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 two 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 two 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. Prior to 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 two-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 two-factor authentication including biometrics. The secure cage is physically secured by an IdenTrust-owned system that requires two-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 on Section 5.1.1.1.

5.1.5 Fire Prevention and Protection

The facility housing the IdenTrust CA, RAs and Repositories equipment provides 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 proper. 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 two-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 two 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 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 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 prior to 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 so 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 two 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 ten minutes of inactivity. This configuration cannot be changed by the employee.

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

Lockout account access to Certificate systems after no more than five 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 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.

Table 6 – TrustID Trusted Roles Matrix

	IdenTrust Defined Roles									
CP Defined Roles	**CA Administrator**	**Operations Manager**	**System Administrator**	**Security Officer**	**Network Administrator**	**PKI Consultant**	**LRA**	**External RA Administrator**	**Trusted Agent**	**Help Desk Representative**
CA Administrator	X									
CA Agent							X			
CA Auditor				X						
CA Operator			X							
CSA Administrator	X									
CSA Agent							X			
CSA Auditor				X						
CSA Operator			X							
CMS Administrator	X									
CMS Operator			X							
CMS Auditor				X						
RA Administrator	X					X		X		
Other Trusted Role		X			X					
Other Non-Trusted Role									X	X

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

5.2.1.1 Certificate Authority 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-Certificate, Root CA Certificate, and Subordinate CA Certificate Key management (performed under two-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 two 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 responsibilities are performed by an LRA. See Section 5.2.4.4 for further detail. CA Certificates generation responsibility is also shared by Customer Support Representatives. See Section 4.1.2.3 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 5.2.4.7 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 5.2.1.4.7 for details on CA Operator's tasks performed by the System Administrator.

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 two-person control);
- Management of CSA Key and Certificate lifecycle, including renewal of OCSP Responder Certificates (performed under two-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 5.2.1.4.7 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 by the IdenTrust Security Office with oversight by the IdenTrust Security Officer. See Section 5.2.1.4.9 Security Officer for details.

5.2.1.2.5 CSA Operator

Within IdenTrust the CA Operator and the CSA Operator are equivalent and interchangeable. See Section 5.2.1.1.4 CA Operator.

5.2.1.3 Card Management System ("CMS") Roles

CMS services are not offered currently offered under the TrustID program; 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 the 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;
- 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 with the exception of Key Management that would be performed by the CA Administrator. See Section 5.2.4.5 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 5.2.4.4 for further detail.

Within IdenTrust, the RA Officer responsibilities are 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 5.2.4.7 for details

5.2.1.4.4 Local Registration Agent (LRA)

An LRA is a Trusted Role. The responsibilities of 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-Certificate, the Root CA Certificate and Subordinate CA Certificates, re-keying and Revocation (performed under two-person control).

5.2.1.4.5 Trusted Agent

A Trusted Agent is an entity is 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 trustworthy manner. A Trusted Agent is confirmed through the Issuance of a business Certificate held on hardware Cryptographic Module that validate 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 referenced mapping of CP defined Trusted Roles to internal IdenTrust Trusted Roles Matrix.

5.2.1.5.1 System Administrator

IdenTrust's System Administrators are Trusted Roles and 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, 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 and 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 Sections 5.4 and 5.5 of this CPS;
- Administrative functions such as compromise reporting; and
- For Server and Extended Validation Code Signing Certificates, performing quarterly self-audits to monitor Certificate Issuance quality described in Sections 8, 8.5.1 and 8.6.1 of this CPS.

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 two-person control).

5.2.1.5.5 PKI Consultant

PKI Consultants are IdenTrust employees who coordinate the processes needed to securely on-board 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 Sections 5.1.2.1 and 6.2.2). Generation, backup, or activation of the Certificate signing Private Keys require the actions of at least two 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 Sections 5.3.1 and 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.

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 of 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 5.3.1), 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 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 with respect to 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 of this CPS;
- 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 that the person is competent, reliable and trustworthy;
- High schools, colleges and universities are contacted to verify the highest or most relevant degree;
- Residence checks are performed to determine that 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 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 five years for employment, education, criminal, and references, and the last three 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 be 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

Personnel performing CA, CSA, RA and LRA duties receive comprehensive training in security principles and procedures, PKI hardware and software used, and disaster recovery and business continuity procedures. Security awareness and training programs are developed and implemented in accordance with federal laws, regulations, and guidelines and supporting security guidelines IdenTrust maintains records of the training received by persons in Trusted Roles.

RAs are obligated by contract, this CPS and the TrustID CP to train its personnel and maintain a record of 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 Server 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 Management Personnel

- Operating systems 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 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 the ones 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 security audit, events related to 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

All security auditing capabilities of IdenTrust's systems required by the TrustID CP are enabled.

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, 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).

Table 7 - TrustID Auditable Events

Auditable Event	CA	CSA	RA
SECURITY AUDIT	**CA**	**CSA**	**RA**
Any changes to the audit parameters, e.g., audit frequency, type of event audited – 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 modification.	X	X	X
Any attempt to delete or modify the audit logs – 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 modification.	X	X	X
Obtaining a third party time-stamp	N/A	N/A	N/A
IDENTITY AND AUTHENTICATION	**CA**	**CSA**	**RA**
Successful and unsuccessful attempts to assume a role – The operating system and applications automatically record: date and time of attempted login, username asserted at time of attempted login, and success or failure indication, are automatically logged.	X	X	X

Auditable Event	CA	CSA	RA
The value of maximum authentication attempts is changed – The operating system logging facility automatically logs date and time, type of event, and identification of the user 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.	X	X	X
Maximum number of authentication attempts occurring during user login – Date and time of attempted login, username asserted at time of attempted login, and failures are recorded automatically by the operating system and application audit logs.	X	X	X
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts – Date and time of event and identification of account holder and administrator are logged automatically by the operating system.	X	X	X
An administrator changes the type of authenticator, e.g., from a password to a biometric – 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
LOCAL DATA ENTRY	**CA**	**CSA**	**RA**
All security-relevant data that is entered in the system – 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
REMOTE DATA ENTRY	**CA**	**CSA**	**RA**
All security-relevant messages that are received by the system – Date and time, Digital Signature/authentication mechanism, and message are automatically logged by the application.	X	X	X
DATA EXPORT AND OUTPUT	**CA**	**CSA**	**RA**
All successful and unsuccessful requests for confidential and security-relevant information – Date and time of attempted access, username or identity asserted at time of 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 person reporting the event and the resolution.	X	X	X
KEY GENERATION	**CA**	**CSA**	**RA**
Whenever a CA generates a Key (not mandatory for 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	-
PRIVATE KEY LOAD AND STORAGE	**CA**	**CSA**	**RA**
The loading of Component Private Keys – A manual log of all physical access to production CA and CSA Cryptographic Modules is maintained by IdenTrust, and the log records each action taken, the date and time the action was taken and the name of person who performed each action. A separate record of authorization to access Cryptographic Modules is also maintained that specifies date, time, reason for access and name of authorizing person.	X	X	N/A

Auditable Event	CA	CSA	RA
All access to Certificate Subject Private Keys retained within the CA for Key recovery purposes – 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
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE	**CA**	**CSA**	**RA**
All changes to the trusted Public Keys, including additions and deletions are automatically logged through the applications and manually through IdenTrust's change management process and access authorization forms.	X	X	X
SECRET KEY STORAGE	**CA**	**CSA**	**RA**
The manual entry of secret Keys used for authentication – 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 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 date, time, reason for access, and name(s) of authorizing person(s).	X	X	N/A
PRIVATE AND SECRET KEY EXPORT	**CA**	**CSA**	**RA**
The export of private and secret Keys (Keys used for a single session or message are excluded) – 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 Section 5.2.4. At the time of export, a manual log records the action taken, date and time the action was taken, and the name(s) of 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 authorizing person(s).	X	X	N/A
CERTIFICATE REGISTRATION	**CA**	**CSA**	**RA**
All Certificate requests – Date and time of 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 request (online, in-person, remote), source of verification, name of 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 interaction and identity provided.	X	N/A	X
CERTIFICATE REVOCATION	**CA**	**CSA**	**RA**
All Certificate Revocation requests – 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
CERTIFICATE STATUS CHANGE APPROVAL	**CA**	**CSA**	**RA**
The approval or rejection of a Certificate status change request – Identity of equipment operator who initiated the request, message contents, message source, destination, and success or failure indication are automatically logged by the application.	X	N/A	N/A

Auditable Event	CA	CSA	RA
COMPONENT CONFIGURATION	**CA**	**CSA**	**RA**
Any security-relevant changes to the configuration of a component – Date and time of modification, name of modifier, description of 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
ACCOUNT ADMINISTRATION	**CA**	**CSA**	**RA**
Roles and users are added or deleted – 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 date and time and type of change, reason for change of role, and authorization and approval records.	X	X	-
The access control privileges of a user account or a role are modified – 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 date and time and type of change, reason for modification and authorization and approval records.	X	X	-
CERTIFICATE PROFILE MANAGEMENT	**CA**	**CSA**	**RA**
All changes to the Certificate profile – Change management records capture date and time and type of change, reason for modification and authorization and approval records.	X	N/A	N/A
REVOCATION PROFILE MANAGEMENT	**CA**	**CSA**	**RA**
All changes to the Revocation profile – Change management records capture date and time and type of change, reason for modification and authorization and approval records.	X	N/A	N/A
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT	**CA**	**CSA**	**RA**
All changes to the Certificate Revocation list profile – Change management records capture date and time and type of change, reason for modification and authorization and approval records.	X	N/A	N/A
MISCELLANEOUS	**CA**	**CSA**	**RA**
Appointment of an Individual to a Trusted Role – Date of the appointment, type of Trusted Role, name of the appointee, and authorizing signature are manually logged.	X	X	X
Designation of personnel for multi-=party control – Date of the appointment, name of the appointee and authorizing signature are manually logged.	X	-	N/A
Installation of the Operating System – Date and time of server installation, name of installer, and details of installation process are manually recorded during installation. The automatic security auditing capabilities of the underlying operating system hosting the software are enabled during installation. All changes are also manually logged through change management procedures.	X	X	X
Installation of the PKI application – Date and time of installation, name of installer, and details of installation process are recorded during installation. All changes are also logged through change management procedures.	X	X	X
Installation of hardware Cryptographic Modules – 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 person who performed the action.	X	X	X

Auditable Event	CA	CSA	RA
Removal of hardware Cryptographic Modules – 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 action.	X	X	X
Destruction of Cryptographic Modules – 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
System Startup – Date and time of system startup is automatically logged in the system's event log.	X	X	X
Logon attempts to PKI Applications – For CA, RA and CSA application access – the date and time of the event, type of event, identity of user accessing the system, and success or failure indication are automatically logged by the application.	X	X	X
Receipt of hardware / software – Kept manually in a database that records the hardware and software possessed, licensed or owned.	X	X	X
Attempts to set passwords – Date and time, identity of user, and success or failure indication of attempt to set password is kept automatically by the operating system/application or manually in a password change log.	X	X	X
Attempts to modify passwords – Date and time, identity of user, and success or failure indication of attempt to modify password is kept by the operating system/application or manually in a password change log.	X	X	X
Back up of the internal CA database – Date and time of the backup event and location of backup are kept manually in a backup log.	X	-	-
Restoration from back up of the internal CA database – Dates and times of restoration tests are kept in a disaster recovery log.	X	-	-
File manipulation (e.g., creation, renaming, moving**)** – for 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	-	-
Posting of any material to a Repository – 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	-	-
Access to the internal CA database – 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	-	-
All Certificate compromise notification requests – Date and time of notification, identity of person making the notification, identification of entity compromised, and a description of the compromise are logged manually by the personnel who receive the notification (e.g., Customer Support, RA Operators, etc.) and by RA/RA Operators' system processing logs.	X	N/A	X
Loading Cryptographic Modules with Certificates – 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 date, time, reason for access, and name of authorizing person.	X	X	N/A
Shipment of Cryptographic Modules – 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	X	X	N/A

Auditable Event	CA	CSA	RA
taken, (e.g., return, receipt), date and time action was taken, name of person performing action and reason for action.			
Zeroizing Cryptographic Modules – A manual list of modules is maintained, and the list records action taken, date and time action were taken, name of person who performed action, name and role of person authorizing the action.	X	X	N/A
Re-key of the CA – 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
CONFIGURATION CHANGES TO THE PKI SERVERS INVOLVING:	**CA**	**CSA**	**RA**
Hardware – All changes are manually logged through change management procedures.	X	X	X
Software – All changes are manually logged through change management procedures.	X	X	X
Operating System – All changes are manually logged through change management procedures.	X	X	X
Patches – All changes are manually logged through change management procedures.	X	X	X
Security Profiles – All changes are manually logged through change management procedures.	X	X	X
PHYSICAL ACCESS / SITE SECURITY	**CA**	**CSA**	**RA**
Personnel Access to room housing component – A manual recording of physical access to 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	-	-
Physical access to System Components – Logged through a combination of automatic and manual logs based upon the type of component and type of access.	X	X	-
Known or suspected violations of physical security – For any known or suspected violations of physical security - date/time, description of suspected event, name of person reporting the event and resolution are manually logged by the Security Office.	X	X	X
ANOMALIES	**CA**	**CSA**	**RA**
Software error conditions – Date and time of event, and description of event are automatically logged by the application reporting the event or by the operating system.	X	X	X
Software check integrity failures – Date and time of event, and description of event are automatically logged by the application reporting the event or by the operating system.	X	X	X
Receipt of improper messages – Date and time of event, and description of event are automatically logged by the application reporting the event or by the operating system.	X	X	X
Misrouted messages – Date and time of event, and description of event are automatically logged by the application reporting the event or by the operating system.	X	X	X
Network attacks (suspected or confirmed) – Date and time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	X

Auditable Event	CA	CSA	RA
Equipment failure – Date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	-
Electrical power outages – Date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	-
Uninterruptible Power Supply (UPS) failure – Date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	-
Obvious and significant network service or access failures – Date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	-
Violations of Certificate Policy – Date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	X
Violations of Certification Practice Statement – Date/time, description of suspected event, name of person reporting the event and resolution are manually logged by a Security Officer.	X	X	X
Resetting Operating System clock – Date/time, description of suspected event, name of person is automatically logged by the operating systems logging facility.	X	X	X

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 of 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 date, name of reviewer, description of 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 in order to prevent overflow conditions. Alerts are sent to a Security Officer if space available becomes inadequate.

The security audit logs are moved monthly to 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 review logs in consistency 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

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 4.1.2.3 IdenTrust Secure Registration Messaging Protocol. 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 in consistency 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 has the rights to modify or delete files in all three locations. Log storage capability is monitored by the operating systems at each location to ensure that sufficient space exists in order to prevent overflow conditions. Logs for the current and two 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 Sections 5.5.3 and 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 in consistency 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 RAs 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 (1) 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 three (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 Compliance Audit and Other Assessments for additional details.

IdenTrust does one of the following within 96 hours of 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.

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 OF 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 three months and archived offsite for at least ten years and six 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 as per Section 3.2.3;
- Documentation of receipt and Acceptance of Certificates;
- Export of Private Keys;
- Certificate 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 date 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 as per Section 3.2.3;
- Documentation of receipt and Acceptance of Certificates;
- Certificate 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 three months and archived offsite for at least ten years and six 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 application that can read those files for ten years and six months.

5.5.3 Protection of Archive

Archived data is stored in a separate, offsite storage facility identified in Section 5.1.68. Records are uniquely identified. The media used for retaining the archived data is specifically chosen and tested to insure 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. IdenTrust's 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 three 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 Sections 9.3 and 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 two 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 prior to 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 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 prior to 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 (CA) 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 either 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 seventy-two 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.

5.7.5 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 own 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 is able to provide help to users when a security incident occurs in the system and to 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.

5.7.6 Entity Public Key is Revoked

In the event of the need for Revocation of an Issuing CA's CA Certificate, IdenTrust will immediately notify: (i) the PMA; (ii) all CAs to whom it has issued cross-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-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, it will follow the procedure described on 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 prior to 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 reason, 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 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 a Contractual Relationship with a Sponsoring Organization with Enterprise RAs

- Archival of all paper records, if any, prior to 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 reason, and provisions have been made to continue compromise recovery, compliance and security audit, archive, and Revocation, then the Certificates approved by the Enterprise RA 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 prior to 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 twenty-four 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

6.1.1.1 Hardware/Software Key Generation

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

6.1.1.2 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 ceremony is scripted, video-recorded and witnessed. The 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 recording are made available to independent third party auditors during the annual audit for examination.

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 is 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 in Section 6.1.2.1.

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 KeyPurposeIds id-kp-serverAuth or anyExtendedKeyUsage.

For delivery of an encryption Private Key, two methods are available as described in the following sub-sections:

6.1.2.1 IdenTrust 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 Generation

When the encryption Keys and Certificate 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 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. Two 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 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 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 back 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.

1. Prior to 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 prior to 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 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 web site. 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

Minimum Key length for other than elliptic curve base algorithm is 2048 bits and divisible by 8. Minimum Key length for elliptic curve group algorithm is 224 bits.

Table 8 - TrustID Key Sizes

	Certificate Signature Algorithm	CRL Signature Algorithm	OCSP Response Signature Algorithm	OIDs Asserted in CA Certificate	OIDs and Certificates Signed by the CA
Root CA (Signed before December 31, 2010)	SHA-1	SHA-1 (Note 1) SHA-256 (Note 1)	SHA-1 (Note 1) SHA-256	None	OCSP Subordinate CA
Root CA (Signed on or after January 1, 2011)	SHA-1 SHA-256	SHA-256	SHA-1 (Note1) SHA-256	None	OCSP Subordinate CA
Subordinate CAs Humans and others	SHA-256	SHA-256 (Note 1)	SHA-256 (Note 1)	SHA-256	Personal, Business Certificates, VBA for Organization, VBA for Business, Admin. RA, FATCA Organization, Secure Email
Subordinate CA Server Certificates	SHA-256	SHA-256 (Note 1)	SHA-256 (Note 1)	SHA-256	Server
TrustID End Entity Certificates					
Personal	SHA-256	SHA-256	SHA-256	SHA-256	Software and Hardware
Business	SHA-256	SHA-256	SHA-256	SHA-256	Software and Hardware

	Certificate Signature Algorithm	CRL Signature Algorithm	OCSP Response Signature Algorithm	OIDs Asserted in CA Certificate	OIDs and Certificates Signed by the CA
FATCA Organization	SHA-256	SHA-256	SHA-256	SHA-256	FATCA Organization
Secure Email	SHA-256	SHA-256	SHA-256	SHA-256	Software and Hardware
Server	SHA-256	SHA-256	SHA-256	SHA-256	Server DV, OV and EV
EV Code Signing	SHA-256	SHA-256	SHA-256	SHA-256	EV Code Signing
Time-Stamping	SHA-256	SHA-256	SHA-256	SHA-256	Time-Stamping
Device and Card Authentication	SHA-256	SHA-256	SHA-256	SHA-256	Device and Card Authentication

Note 1: IdenTrust PMA will make the SHA-2 algorithms mandatory when the browser/Cryptographic Module technology and Relying Party applications is widely available and security threats make it prudent to require it.

All valid Certificates that expire on or after December 31, 2011 shall contain Public Keys of at least 2048 bits and divisible by 8 for RSA or at least P-256 bits for ECDSA.

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 on-board 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 have 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 Cryptomodules 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 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 OCSP 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 for TrustID. For further details see the TrustID Certificate Profile document or Appendix A of this CPS which addresses all Certificate profiles.

6.1.7.1 CA and Cross-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 customers 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) CRL Signature; (ii) Key Certificate Signature, (iii) Digital Signature; and (iv) Non-Repudiation.

6.1.7.3 Signing Certificates (including Personal and Business)

The following Key Usage values are present in the Subscribers Signing Certificates: (i) Digital Signature; and (ii) non-repudiation, which will be marked as critical.

The following Key Usage value is present in the Subscriber Encryption Certificates: Key encipherment and data encipherment which will be marked as critical.

The following extended Key Usage value is present: (i) client authentication and (ii) Secure Email.

The following Key Usage value is present in the Subscriber Encryption Certificates: Key encipherment and data encipherment which will be marked as critical.

The following extended Key Usage value is present: Secure Email.

6.1.7.4 VPN IPSec and OCSP Signing Certificates

The following Key Usage values are present in the VPN IPSec, OCSP Signing, and Digital Signature, which will be marked as critical.

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}.

6.1.7.5 Server Certificates

The following Key Usage values are present in the Server Certificates. (i) Digital Signature and (ii) Key encipherment, which will be marked as critical.

The following extended Key Usage values are present: (i) server authentication (ip-kp-serverAuth); and (ii) client authentication (ip-kp-clientAuth).

6.1.7.6 FATCA Organization Certificates

The following Key Usage values are present in the FATCA Organization Certificates. (i) Digital Signature and (ii) Key encipherment, which will be marked as critical.

6.1.7.7 Server EV Certificates

The following Key Usage values are present in the Server Certificates. (i) Digital Signature and (ii) Key encipherment, which will be marked as critical.

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 and this CPS.

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 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, for 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 plain 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 Certificates.

For TrustID EV Code Signing Subscriber, TrustID Time-Stamping and Signing Authority Certificates, the corresponding Key Pairs are generated and stored in hardware Cryptographic Modules that are validated at minimum of FIPS 140-2 Level-2 or equivalent standard. For TrustID Card Authentication Certificates and TrustID Device Certificates, the corresponding Key Pairs are generated and stored in hardware Cryptographic Modules that are validated at 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 two-person control and are stored in the Secure Room and in a secure off-site facility where two-person controls are implemented as explained in Sections 5.1.6, 5.1.8 and 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 two-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 two-person control, IdenTrust backs up CA Private Keys on cloned Cryptographic Modules in order to obviate the need to re-key in the case of hardware failure.

Two copies of the Root CA Certificate are created in separate Cryptographic Modules. Two 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 two-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 CAs 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 plain text outside of the module.

6.2.4.4 Backup of CSA Private Key

Under two-person control, IdenTrust backs up CSA Private Keys on cloned Cryptographic Modules in order to obviate the need to re-key in the case of hardware failure.

Two 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 two-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

IdenTrust's CA and CSA Private Keys are stored in FIPS 140-1/2 level 3 Modules.

For 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.

6.2.8 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 two-person control. The Private Key is activated by use of the PED Key during a ceremony.

Subscribers must protect their Private Key from unauthorized use with a strong password, whose constrains 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 that requires two-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 be 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 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 in accordance with the following table:

Table 9 - TrustID Operational Periods and Key Usage Periods

Periods / Key Type	Private Key Usage Period	Certificate Lifetime
Root CA	20 years	20 years
Subordinate CA	Up to 15 years	Up to 15 years
CSA (OCSP)	3 years	Up to 12 months
Subscriber (Signature)	Up to 3 years	Up to 3 years
Subscriber (Encryption)	Unrestricted	Up to 3 years
LRA (Signature)	Up to 3 years	Up to 3 years
LRA (Encryption)	Unrestricted	Up to 3 years
End Entity Server Certificates	Up to 39 months when issued after July 1, 2016 but prior to March 1, 2018	Up to 39 months when issued after July 1, 2016 but prior to March 1, 2018
	No greater than 825 days when issued after March 1, 2018, no greater than 815 days when issued after April 20, 2018 and no greater than 397 days when issued on or after September 1, 2020	No greater than 825 days when issued after March 1, 2018, no greater than 815 days when issued after April 20, 2018, and no greater than 397 days when issued on or after September 1, 2020.
Extended Validation Code Signing	Up to 39 months	Up to 39 months
Time-Stamping	End Entity: Up to 15 months	Subordinate CA: Up to 135 months

Periods / Key Type	Private Key Usage Period	Certificate Lifetime
FATCA Organization	Up to 39 months	Up to 39 months
Secure Email	Up to 3 years	Up to 3 years
End Entity Certificates - Other Devices	Up to 7 years	Up to 7 years

Subscriber Key Pair must be replaced in accordance with the provisions of Section 3.3.1.

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 two-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 two 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, 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 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 is able to 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., three 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 least privilege.

IdenTrust provides technical access controls designed to provide 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 or unsuccessful authentication attempts. User IDs are revoked if a password attempt threshold failed login attempts is exceeded.

IdenTrust's systems are able to 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 have 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 quality product, and 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 in order to confirm the content when it is received. Other major PKI components (i.e., servers) are shipped under standard conditions. At reception, 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 is 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.

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, 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 functioning. 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 evaluate 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.

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

7.1.1 Version Number(s)

This CPS is applicable to X.509 v.3 Certificates.

The specific Certificate Profiles and values contained in Certificates issued pursuant to this CPS may be found in the TrustID Certificate Profile document or Appendix A of this CPS. However, the following sections provide generally applicable Certificate profile information for Certificates issued to Subscriber in accordance with this CPS.

7.1.1.1 Version

Version of X.509 Certificate, version 3 (i.e., populated with the integer "2")

7.1.1.2 Serial Number

Unique serial number for a Certificate

For all Certificates, IdenTrust generates a non-sequential serial number that exhibits at least 64 bits of entropy.

For all TrustID Server Certificates, IdenTrust shall generate Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a cryptographically secure pseudorandom number generator.

7.1.1.3 Signature

Issuer's Digital Signature on the Certificate

The Issuer Digital Certificates will also be signed with the same algorithms.

Certificates issued under the TrustID CP and this CPS may use the following OIDs for signatures:

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

7.1.1.4 Issuer

Name of the Issuing CA specified as the following:

Issuer's Distinguished Name:

cn =	<Issuer CA type>
ou =	<Issuer CA designation>
o =	<Issuer>
c =	<country of Issuer>

See the TrustID Certificate Profile document or Appendix A of this CPS for variations to this Issuer DN.

7.1.1.5 Validity Period

Validity periods are provided in Section 6.3.2 for each Certificate.

7.1.1.6 Subject

Based on the type of Certificate and the user, the subject profiles are listed as follows:

7.1.1.6.1 Human Subscribers

Subscriber's Distinguished Name, which may contain a unique identifier to ensure name uniqueness:

cn =	<subject name> (firstname MI lastname)
ou =	< department/division of Organization >
o =	<Sponsoring Organization name >
c =	<country of Subscriber>

7.1.1.6.2 Server Certificates

Subscriber's Distinguished Name, which may contain a unique identifier to ensure name uniqueness:

7.1.1.6.2.1 Server Domain Validation (DV):

Subscriber's Distinguished Name, which may contain a unique identifier to ensure name uniqueness:

cn =	<subject Fully Qualified Domain Name> *If present, it will contain a single IP address or FQDN that is one of the values contained in the Certificate's subjectAltName extension.*

7.1.1.6.2.2 Server Organization Validation (OV):

cn =	<subject Fully Qualified Domain Name> *If present, it will contain a single IP address or FQDN that is one of the values contained in the Certificate's subjectAltName extension.*
ou =	<department/division of Organization>
o =	<Sponsoring Organization name>
LocalityName =	<verified city of the Sponsoring Organization>
StateOrProvinceName =	<verified state>
c =	<country of Sponsoring Organization>

7.1.1.6.2.3 Server Extended Validation (EV):

Subscriber's Distinguished Name, which may contain a unique identifier to ensure name uniqueness:

cn =	<subject Fully Qualified Domain Name> *If present, it will contain a single IP address or FQDN that is one of the values contained in the Certificate's subjectAltName extension.*
(optional) ou =	<department/division of Organization>
o =	<Sponsoring Organization name>
LocalityName =	<verified city of the Sponsoring Organization>
StateOrProvinceName =	<verified state of the Sponsoring Organization>
(optional) streetAddress =	< verified street and number of the Sponsoring Organization >

(optional) postalCode =	< verified postal code of the Sponsoring Organization >
c =	<country of Sponsoring Organization>
Business Category {2.5.4.15}	One of the following strings: • Private Organization, • Government Entity, • Business Entity, or • Non-Commercial Entity
Jurisdiction of Incorporation Locality {1.3.6.1.4.1.311.60.2.1.1 }	<verified city of incorporation>
Jurisdiction of Incorporation State / Province {1.3.6.1.4.1.311.60.2.1.2 }	<verified state or province of incorporation>
Jurisdiction of Incorporation Country {1.3.6.1.4.1.311.60.2.1.3 }	<verified country of incorporation>
Registration Number {2.5.4.5}	<verified Registration Number of similar assigned to the Sponsoring Organization>
(optional) Organization Identifier {2.5.4.97}	<verified Registration Reference assigned to the Sponsoring Organization>

7.1.1.6.3 FATCA Organization Certificates

o =	<Sponsoring Organization name >
c =	<country of Sponsoring Organization>

7.1.1.6.4 Secure Email Certificates

GUID	Unique Certificate identifier
ou =	"{any static custom label}: <email address>"
e =	<email address>

7.1.1.6.5 Extended Validation Code Signing Certificates

cn =	<verified legal name of Sponsoring Organization>
(optional) ou =	<department/division of Organization>
o =	<Sponsoring Organization name>
LocalityName =	<verified city of the Sponsoring Organization>
StateOrProvinceName =	<verified state of the Sponsoring Organization>
(optional) streetAddress =	< verified street and number of the Sponsoring Organization >
(optional) postalCode =	< verified postal code of the Sponsoring Organization >
c =	<country of Sponsoring Organization>

Business Category {2.5.4.15}	One of the following strings: • Private Organization, • Government Entity, • Business Entity, or • Non-Commercial Entity
Jurisdiction of Incorporation Locality {1.3.6.1.4.1.311.60.2.1.1}	<verified city of incorporation>
Jurisdiction of Incorporation State / Province {1.3.6.1.4.1.311.60.2.1.2}	<verified state or province of incorporation>
Jurisdiction of Incorporation Country {1.3.6.1.4.1.311.60.2.1.3}	<verified country of incorporation>
Registration Number {2.5.4.5}	<verified Registration Number of similar assigned to the Sponsoring Organization>

7.1.1.6.6 Time-Stamping Certificates

cn =	TrustID Time-Stamping Authority *[m]*
(optional) ou =	<department/division of Organization>
o =	IdenTrust
LocalityName =	<verified city of the Sponsoring Organization>
StateOrProvinceName =	<verified state of the Sponsoring Organization>
(optional) streetAddress =	< verified street and number of the Sponsoring Organization >
(optional) postalCode =	< verified postal code of the Sponsoring Organization >
c =	US
Business Category {2.5.4.15}	One of the following strings: • Private Organization, • Government Entity, • Business Entity, or • Non-Commercial Entity
Registration Number {2.5.4.5}	<verified Registration Number of similar assigned to the Sponsoring Organization>

7.1.1.7 Subject Public Key Information

Algorithm ID, the Subscriber's Public Key, and Public Key parameters.

7.1.2 Certificate Extensions

This section shows all the extension supported in each of the Certificates issued under this Policy following the specification off the RFC 5280.

7.1.2.1 Root CA Certificate

basicConstraints	This extension is present and marked critical. The cA flag value is set to true. The pathLenConstraint field is not present.
keyUsage	This extension is present and marked critical. Bit positions for keyCertSign and cRLSign are set.
subjectKeyIdentifier	This extension is present and is marked non-critical. It contains the SHA-1 hash of the subjectPublicKey.

7.1.2.2 Subordinate CA Server Certificates

authorityKeyIdentifier	This extension is present and is marked non-critical. It contains the identifier defined in the subjectKeyIdentifier extension of the issuer CA Certificate.
subjectKeyIdentifier	This extension is present and is marked non-critical. It contains the SHA-1 hash of the subjectPublicKey
keyUsage	This extension is present and marked critical. Bit positions for keyCertSign and cRLSign are set. When the Subordinate CA Private Key is used for signing OCSP responses, the digitalSignature bit is also set.
extkeyUsage	This extension is present and marked as non-critical. Subordinate CA Certificates issuing Server Certificates are technically constrained by including the values id-kp-serverAuth and id-kp-clientAuth at a minimum. Subordinate CA Certificates for Certificates issued to Individuals are populated with the values Client Authentication and Secure Email.
certificatePolicies	This extension is present and marked non-critical. It includes the at least one policy Identifier, a cPSuri and a userNotice.
basicConstraints	This extension is present and marked critical. The cA flag value is set to true. The pathLenConstraint field is present and has a value of zero (0)
nameConstraints	This extension may be present and marked critical.
authorityInfoAccess	This extension is optional. If present: C = No. [1]accessMethod ::={1.3.6.1.5.5.7.48.1} accessLocation::= { http://commercial.ocsp.identrust.com} [2] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= { URL = "http://validation.identrust.com/roots/commercialrootca1.p7c" }
cRLDistributionPoints	This extension is present and marked non-critical.

	It contains the HTTP URL of the CA's CRL service

7.1.2.3 OCSP Certificates

authorityKeyIdentifier	This extension is present and is marked non-critical. It contains the identifier defined in the subjectKeyIdentifier extension of the issuer CA Certificate
subjectKeyIdentifier	This extension is present and is marked non-critical. It contains the SHA-1 hash of the subjectPublicKey.
keyUsage	This extension is present and marked critical. Bit position for digitalSignature is set.
extkeyUsage	This extension is present and marked non-critical. It includes the value id-kp-OCSPSigning.
subjectAltName	This extension is present and marked non-critical. It includes the dNSName entry containing the Fully-Qualified Domain Name of the HTTP URL
id-pkix-ocsp-nocheck	This extension is present and marked non-critical. The value is null.
authorityInfoAccess	This extension may be present and marked non-critical. It contains the HTTP URL of the CA's Certificate (accessMethod = 1.3.6.1.5.5.7.48.2).
cRLDistributionPoints	This extension may be present and marked non-critical. It contains the HTTP URL of the CA's CRL service.

7.1.2.4 Personal, Personal Hardware, Business and Business Hardware Certificates

authorityKeyIdentifier	This extension is present and is marked non-critical. It contains the identifier defined in the subjectKeyIdentifier extension of the issuer CA Certificate.
subjectKeyIdentifier	This extension is present and is marked non-critical. It contains the SHA-1 hash of the subjectPublicKey.
keyUsage	This extension is present and marked critical. Bit positions for digitalSignature, nonrepudiation, keyEncipherment and dataEncipherment are set.
extkeyUsage	This extension is present and marked non-critical. It includes the values Client Authentication, Secure Email and Smart Card Logon.
certificatePolicies	This extension is present and marked non-critical. It includes one policyIdentifier, a cPSuri and a userNotice.
basicConstraints	This extension may be present. If present:

	Marked as critical The cA flag value set to false. The pathLenConstraint field is none
subjectAltName	This extension is present and marked non-critical. It includes the RFC5322Name containing the email address of the Subscriber. It may also include the otherName: userPrincipalName.
authorityInfoAccess	This extension is present and marked critical. It contains the HTTP URL of the CA's OCSP responder (accessMethod= 1.3.6.1.5.5.7.48.1). It also contains the HTTP URL of the CA's Certificate (accessMethod = 1.3.6.1.5.5.7.48.2).
cRLDistributionPoints	This extension may be present and marked non-critical. It contains the HTTP URL of the CA's CRL service.

7.1.2.5 Server Certificates

authorityKeyIdentifier	This extension is present and is marked non-critical. It contains the identifier defined in the subjectKeyIdentifier extension of the issuer CA Certificate.
subjectKeyIdentifier	This extension is present and is marked non-critical. It contains the SHA-256 hash of the subjectPublicKey.
1.3.6.1.4.1.11129.2.4.2 (SCT List)	This extension is present and includes one or more RFC 6962 signed Certificate time-stamps.
keyUsage	This extension is present and marked critical. Bit positions for digitalSignature and keyEncipherment are set.
extkeyUsage	This extension is present and marked non-critical. It includes the values id-kp-serverAuth and id-kp-clientAuth.
certificatePolicies	This extension is present and marked non-critical. It includes the at least one policyIdentifier, a cPSuri and a userNotice.
basicConstraints	This extension is optional. If present: - Marked as critical - The cA flag value set to false - The pathLenConstraint is none
subjectAltName	This extension is present and marked non-critical, unless the Subject Distinguished Name is empty, in which case this extension must be present and marked as critical It includes at least one dNSName entry containing the Fully-Qualified Domain Name. No iPAddress entries are included.
authorityInfoAccess	This extension is present and marked non-critical.

	It contains the HTTP URL of the CA's OCSP responder (accessMethod= 1.3.6.1.5.5.7.48.1). It also contains the HTTP URL of the CA's Certificate (accessMethod = 1.3.6.1.5.5.7.48.2).
cRLDistributionPoints	This extension may be present and marked non-critical. It contains the HTTP URL of the CA's CRL service.

7.1.2.6 Administrative RA Certificates (Individual)

authorityKeyIdentifier	This extension is present and is marked non-critical. It contains the identifier defined in the subjectKeyIdentifier extension of the issuer CA Certificate.
subjectKeyIdentifier	This extension is present and is marked non-critical. It contains the SHA-1 hash of the subjectPublicKey.
keyUsage	This extension is present and marked critical. Bit positions for digitalSignature, nonrepudiation, keyEncipherment and dataEncipherment are set.
certificatePolicies	This extension is present and marked non-critical. It includes one policyIdentifier, a cPSuri and a userNotice.
subjectAltName	This extension is present and marked non-critical. It includes the RFC5322Name containing the email address of the Subscriber.
authorityInfoAccess	This extension is present and marked critical. It contains the HTTP URL of the CA's OCSP responder (accessMethod= 1.3.6.1.5.5.7.48.1). It also contains the HTTP URL of the CA's Certificate (accessMethod = 1.3.6.1.5.5.7.48.2).
cRLDistributionPoints	This extension may be present and marked non-critical. It contains the HTTP URL of the CA's CRL service.

7.1.2.7 Administrative RA Certificates (Electronic Device)

authorityKeyIdentifier	This extension is present and is marked non-critical. It contains the identifier defined in the subjectKeyIdentifier extension of the issuer CA Certificate.
subjectKeyIdentifier	This extension is present and is marked non-critical. It contains the SHA-1 hash of the subjectPublicKey.
keyUsage	This extension is present and marked critical. Bit positions for digitalSignature and nonrepudiation.
certificatePolicies	This extension is present and marked non-critical. It includes the at least one policyIdentifier, a cPSuri and a userNotice.
authorityInfoAccess	This extension is present and marked critical.

	It contains the HTTP URL of the CA's OCSP responder (accessMethod= 1.3.6.1.5.5.7.48.1). It also contains the HTTP URL of the CA's Certificate (accessMethod = 1.3.6.1.5.5.7.48.2)
cRLDistributionPoints	This extension may be present and marked non-critical. It contains the HTTP URL of the CA's CRL service.

7.1.2.8 FATCA Organization Certificates

authorityKeyIdentifier	This extension is present and is marked non-critical. It contains the identifier defined in the subjectKeyIdentifier extension of the issuer CA Certificate.
subjectKeyIdentifier	This extension is present and is marked non-critical. It contains the SHA-1 hash of the subjectPublicKey.
keyUsage	This extension is present and marked critical. Bit positions for digitalSignature and keyEncipherment are set.
certificatePolicies	This extension is present and marked non-critical. It includes one policyIdentifier, a cPSuri and a userNotice.
subjectAltName	This extension is present and marked non-critical. It includes the RFC5322Name containing the email address of the Subscriber.
authorityInfoAccess	This extension is present and marked critical. It contains the HTTP URL of the CA's OCSP responder (accessMethod= 1.3.6.1.5.5.7.48.1). It also contains the HTTP URL of the CA's Certificate (accessMethod = 1.3.6.1.5.5.7.48.2).
cRLDistributionPoints	This extension is present and marked non-critical. It contains the HTTP URL of the CA's CRL service.

7.1.2.9 Secure Email Certificates

authorityKeyIdentifier	This extension is present and is marked non-critical. It contains the identifier defined in the subjectKeyIdentifier extension of the issuer CA Certificate.
subjectKeyIdentifier	This extension is present and is marked non-critical. It contains the SHA-1 hash of the subjectPublicKey.
keyUsage	This extension is present and marked critical. Bit positions for digitalSignature and keyEncipherment are set.
extkeyUsage	This extension is present and marked non-critical. It includes the values Client Authentication, Secure Email and for Hardware based Certificates includes Smart Card Logon.
certificatePolicies	This extension is present and marked non-critical. It includes one policyIdentifier, a cPSuri and a userNotice.

basicConstraints	This extension is present. The cA flag value set to false. The pathLenConstraint field is none
subjectAltName	This extension is present and marked non-critical. It includes the RFC5322Name containing the email address of the Subscriber.
authorityInfoAccess	This extension is present and marked critical. It contains the HTTP URL of the CA's OCSP responder (accessMethod= 1.3.6.1.5.5.7.48.1). It also contains the HTTP URL of the CA's Certificate (accessMethod = 1.3.6.1.5.5.7.48.2).
cRLDistributionPoints	This extension is present and marked non-critical. It contains the HTTP URL of the CA's CRL service.

7.1.2.10 Extended Validation Code Signing Subordinate CA Certificates

authorityKeyIdentifier	This extension is present and is marked non-critical. It contains the identifier defined in the subjectKeyIdentifier extension of the issuer CA Certificate.
subjectKeyIdentifier	This extension is present and is marked non-critical. It contains the SHA-256 hash of the subjectPublicKey.
keyUsage	This extension is present and marked critical. Bit positions for digitalSignature are set.
extkeyUsage	This extension is present and marked non-critical. It includes the values id-kp-codeSigning.
certificatePolicies	This extension is present and marked non-critical. It includes the at least one policyIdentifier, a cPSuri and a userNotice.
basicConstraints	This extension is present and not marked as critical. The cA flag value set to true. The pathLenConstraint field is optional.
authorityInfoAccess	This extension is present and marked non-critical. It contains the HTTP URL of the CA's OCSP responder (accessMethod= 1.3.6.1.5.5.7.48.1). It also contains the HTTP URL of the CA's Certificate (accessMethod = 1.3.6.1.5.5.7.48.2).
cRLDistributionPoints	This extension may be present and marked non-critical. It contains the HTTP URL of the CA's CRL service.

7.1.2.11 Time-Stamping Certificates

authorityKeyIdentifier	This extension is present and is marked non-critical.

	It contains the identifier defined in the subjectKeyIdentifier extension of the issuer CA Certificate.
subjectKeyIdentifier	This extension is present and is marked non-critical. It contains the SHA-256 hash of the subjectPublicKey.
keyUsage	This extension is present and marked critical. Bit positions for digitalSignature and nonRepudiation are set.
extkeyUsage	This extension is present and marked non-critical. It includes the values id-kp-timeStamping.
certificatePolicies	This extension is present and marked non-critical. It includes the at least one policyIdentifier, a cPSuri and a userNotice.
basicConstraints	This extension is present and marked critical. The cA flag value set to false. The pathLenConstraint field is none
authorityInformationAccess	This extension is present and marked non-critical. It contains the HTTP URL of the CA's OCSP responder (accessMethod= 1.3.6.1.5.5.7.48.1). It also contains the HTTP URL of the CA's Certificate (accessMethod = 1.3.6.1.5.5.7.48.2).
cRLDistributionPoints	This extension may be present and marked non-critical. It contains the HTTP URL of the CA's CRL service.

7.1.2.12 Certificate Policies

The Certificate Policies extension is populated in all Certificates issued by the Root CA with the OIDs in Section 1.2.2.

One of these OIDs is included in the Certificate Policies extension of Certificates issued to Subscribers. The Certificate Policies extension is set to non-critical.

7.1.2.13 Policy Constraints

The Policy constraints extension in Certificates issued by the Root CA Certificates to Subordinate CA Certificates is not populated.

7.1.2.14 Critical Extensions

When present, the following Certificate extensions are marked as critical in a Certificate issued by IdenTrust: Key Usage, Basic Constraints, and Name Constraints.

When Name Constraint extension is present in a Subordinate CA Certificate that issues Server Certificates, it may be market as not-critical. This Policy allows this exception until such extension is supported by all Application Software Suppliers for which IdenTrust is Participant of their Root CA Certificate programs.

7.1.3 Algorithm Object Identifiers

Certificates are issued with the following Certificate attributes, associated algorithms and OIDs, including but not limited to:

signature, sha256WithRSAEncryption	OID = 1.2.840.113549.1.1.11
subjectPublicKeyInfo, RSAEncryption	OID = 1.2.840.113549.1.1.1

7.1.4 Name Forms

Every DN is defined according to the form of an X.501 PrintableString.

IdenTrust does not issue Server Certificates with a Reserved IP Address or Internal Names.

Prior to September 30, 2020, the content of the Certificate Issuer Distinguished Name field must match the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280, section 4.1.2.4.

Effective September 30, 2020 the following requirements should be met by all newly-issued Subordinate CA Certificates that are not used to issue Server Certificates, as defined Section 7.1.2.2 of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published at https://www.cabforum.org, and must be met for all other Certificates, regardless of whether the Certificate is a CA Certificate or a Subscriber Certificate.

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.

7.1.4.1 Name Form for CAs

Identifier type:	With data content of:	Indicates:
Subject: **countryName (C)**	**Root CA** N/A The letters "US" **Subordinate CA** The letters "US"	**Root CA** That the Root Certificate is managed by a CA operated in the United States of America. **Subordinate CA** That the Certificate is sponsored by a CA in the country represented by the two-letter code.
Subject: **organizationName (O)**	**Root CA** IdenTrust **Subordinate CA** IdenTrust	**Root CA** That the Root CA is owned and operated by IdenTrust. **Subordinate CA** The name of Organization sponsoring the CA.
Subject: **organizationalUnitName (OU)**	**Root CA** N/A **Subordinate CA** TrustID	**Root CA** Designation by IdenTrust for this Root to be the IdenTrust Use Root **Subordinate CA** Signing CA designation.

Identifier type:	With data content of:	Indicates:
Subject: **commonName (CN)**	**Root CA** DST Root CA X3 IdenTrust Commercial Root CA [n] or IdenTrust Public Sector Root CA [n] **Subordinate CA** TrustID CA A1[n] Enterprise CA Name TrustID EV Code Signing CA[n] TrustID Time-Stamping CA[n] [n] Iteration of the TrustID CA	**Root CA** The name of the Root CA followed by a number starting in one (1) and progressively increasing with each new instance of the Root Certificate **Subordinate CA** The name of the Subordinate CA. A number could be appended to indicate the instance of the Subordinate CA Enterprise CA Name may be constrained. See Section 7.1.4.2

7.1.4.2 Name Form for End Entity Certificates

Identifier type:	With data content of:	Indicates:
Subject: **countryName (C)**	A two-letter code	The two-letter code indicating the country where the Sponsoring Organization is located
Subject: **organizationName (O)**	Alphanumeric text	The unique name of Sponsoring Organization composed by the original Sponsoring Organization name.
Subject: **organizationalUnitName (OU)**	Alphanumeric text	The affiliation between the Subscriber and a Sponsoring Organization
Subject: **commonName (CN)**	Alphanumeric text	**For Human Subscribers Certificates** The Subscriber's name vetted in accordance with Section 3.2.3 Name format consist of first name, middle initial and last name each separated from the next by a space. If the last name consists of last name and a name indicating generation such as "Jr." or "III" they will be separated by a space character (ASCII 32) **For Server Certificates** The FQDN of the component or device being certified. If the component is a web server or IP Address, the URI or IP Address is always listed in subjectAltName Underscore characters ("_") must not be present in dNSName entries. Subject attributes which contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable are not accepted. The CN must contain the Subject's full legal organization name as verified per Section

Identifier type:	With data content of:	Indicates:
		3.2 and when using the DBA/Tradename, as verified per Section 3.2.2.3.1. In addition, for Server EV Certificates, an assumed name or DBA/Tradename 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. **For OCSP Certificates** The URI for the OCSP responder **For EV Code Signing Certificates:** The full legal Organization name. **For Time-Stamping Certificates** The name of the Signing Authority
Subject: serialNumber	Hexadecimal Characters for a Universally Unique Identifier (UUID) 0.9.2342.19200300.100.1.1	**For Human Certificates** A unique Subject identifier explained in Section 3.1.5
Subject: streetAddress (OID: 2.5.4.9)	Alphanumeric text	**For Server EV Certificates, and EV Code Signing.** The street and number of the physical location of the Subscribing Organization
Subject: localityName (OID: 2.5.4.7)	Alphanumeric text	**For Server EV Certificates, and EV Code Signing.** The city of the physical location of the Subscribing Organization
Subject: stateOrProvinceName (OID: 2.5.4.8)	Alphanumeric text	**For Server EV Certificates, and EV Code Signing.** The state or province of the physical location of the Subscribing Organization
Subject: countryName (OID: 2.5.4.6)	Alphanumeric text	**For Server EV Certificates, and EV Code Signing.** The country of the physical location of the Subscribing Organization
Subject: postalCode (OID: 2.5.4.17)	Alphanumeric text	**For Server EV Certificates, and EV Code Signing.** The postal code of the physical location of the Subscribing Organization
Subject: jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1)	Alphanumeric text	**For Server EV Certificates, and EV Code Signing.** The city of incorporation confirmed with the incorporating agency or registration agency conformant to the specification in RFC 5280 for ASN.1 - X520LocalityName
Subject: jurisdictionStateOrProvinceName	Alphanumeric text	**For Server EV Certificates, and EV Code Signing.**

Identifier type:	With data content of:	Indicates:
(OID: .3.6.1.4.1.311.60.2.1.2)		The state or province of incorporation confirmed with the incorporating agency or registration agency conformant to the specification in RFC 5280 for ASN.1 - X520StateOrProvinceName
Subject: jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)	Alphanumeric text	**For Server EV Certificates, and EV Code Signing.** The country of incorporation confirmed with the incorporating agency or registration agency conformant to the specification in RFC 5280 for ASN.1 - X520countryName
Subject: businessCategory (OID: 2.5.4.15)	Text String	**For Server EV Certificates, and EV Code Signing.** One of the following pre-determining text strings: • Private Organization, • Government Entity, • Business Entity, or • Non-Commercial Entity
Registration Number Subject: serialNumber (OID: 2.5.4.5)	Alphanumeric text in common format	**For Server EV Certificates, EV Code Signing, and Time-Stamping.** 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.
Organization Identifier Subject: organzationIdentifier (OID: 2.5.4.97)	Alphanumeric text encoded as a PrintableString or UTF8String	**For Server EV Certificates, EV Code Signing, and Time-Stamping.** The Registration reference for a Legal Entity assigned in accordance to an identified registration scheme.
subjectAltName: rfc5322name (in a Certificate issued to an Individual Subscriber) and the extension required for Server Certificates	For Individuals, the email address in the form prescribed by [IETF RFC 822] (now superseded; see [IETF RFC 5322]). For Server Certificates, the dNSName containing the FQDN or an iPAddress containing the IP of the Server. IdenTrust does not issue Certificates with a	**For Human Certificates** An email address at which the Subscriber can receive messages via SMTP. An RFC5322name appears in Certificates issued to Individuals; however, the email address may be for that Subscriber or one or more other persons in the Sponsoring Organization. **For Server Certificates**

Identifier type:	With data content of:	Indicates:
	subjectAltName extension or Subject commonName field containing a Reserved IP Address or Internal Name. Entries in the dNSName must be in the "preferred name syntax", as specified in RFC 5280, and thus must not contain underscore characters ("_").	The FQDN after it if fully verified or an iPAddress containing the IP address of a server. **For FATCA Organization Certificates** An email address at which the Subscriber can receive messages via SMTP. An RFC5322name is for that Subscribing Organization and may correspond to one or more Individuals.
Subject: **localityName, state or provinceName**		**For Server Certificates** This extension will be included when the Organization Name (O) is included.

When multiple values exist for an attribute in a DN, the DN is encoded so that each attribute value is encoded in a separate relative distinguished name.

7.1.4.3 Name Form for Secure Email Certificates

Identifier type:	With data content of:	Indicates:
Subject: **organizationUnitName (OU)**	Alphanumeric text	"{any static custom label}: [email address]"
email (E)	The email address in the form prescribed by [IETF RFC 822] now superseded; see [IETF RFC 5322]	Email address
Subject: **serialNumber**	Hexadecimal Characters for a Universally Unique Identifier (UUID) 0.9.2342.19200300.100.1.1	A unique Subject identifier explained in Section 3.1.5
subjectAltName (SAN): RFC5322name (in a Certificate issued to an Individual Subscriber) and the extension required for Server Certificates	The email address in the form prescribed by [IETF RFC 822] now superseded; see [IETF RFC 5322]	Email address

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.

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 ceremony which encompasses all procedures set forth in the TrustID CP and this CPS. The 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 prior to the Subordinate CA Certificate Issuance.

The Certificate's Extended Key Usage extension will, at a minimum, contain the id-kp-serverAuth and may contain the id-kp-clientAuth.

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 will be 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.

IdenTrust publicly disclose not fully Technically Constrained Subordinate CA's per Mozilla Root Store Policy 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 one or more of the OIDs listed in Section 1.2.2.

7.1.7 Usage of Policy Constraints Extension

CAs are required to adhere to the Certificate formats described in this CPS.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates with a Policy qualifier in the Certificate Policies extensions 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

Policy qualifiers will be populated as follows:

[1,1] **Policy Qualifier Info:**	Policy Qualifier Id=CPS Qualifier: https://secure.identrust.com/certificates/policy/ts/index.html
[1,2] **Policy Qualifier Info:**	Policy Qualifier Id=User Notice Qualifier: Notice Text=This TrustID Certificate has been issued in accordance with IdenTrust's TrustID Certificate Policy found at: https://secure.identrust.com/certificates/policy/ts/index.html

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 marked noncritical*, to support legacy applications that cannot process InhibitAnyPolicy.

7.2 CRL PROFILES

7.2.1 Version Number(s)

IdenTrust issues X.509 version two (2) CRLs (i.e., populated with integer "1"). CRLs conform to RFC 5280 and 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.

Issuer	DN of issuer of CRL
Effective Date	Issue date of the CRL
Next Update	Date by which next CRL will be issued
Revoked Certificates	CRL of revoked Certificates, Serial Number, Revocation Date and Reason Code

7.2.2 CRL and CRL Entry Extensions

IdenTrust CRLs comply with Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile (see Appendix A of this CPS or the TrustID Certificate Profile document).

7.2.2.1 reasonCode (OID 2.5.29.21)

Effective September 30, 2020, IdenTrust has implemented the following requirements pertaining to extension reasonCode:

- If present, this extension is not marked critical.
- If a CRL entry is for a Root CA or Subordinate CA Certificate, including Cross Certificates, this CRL entry extension must be present.
- If a CRL entry is for a Certificate not technically capable of causing issuance, this CRL entry extension should be present, but may be omitted, subject to the following requirements:
    - The CRLReason indicated must not be unspecified (0).
    - If the reason for revocation is unspecified, CAs must omit reasonCode entry extension, if allowed by the previous requirements.
    - If a CRL entry is for a Certificate not subject to the CA/B Forum Baseline Requirements and was either issued on-or-after September 30, 2020 or has a notBeforeon-or-after September 30, 2020, the CRLReason must not be certificateHold (6).

    - If a CRL entry is for a Certificate subject to the CA/B Forum Baseline Requirements, the CRLReason must not be certificateHold (6).
- If a reasonCodeCRL entry extension is present, the CRLReason must indicate the most appropriate reason for revocation of the Certificate, as defined in Section 4.9 of this CPS.

7.3 OCSP PROFILE

Effective September 30, 2020, 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.

Effective September 30, 2020, the CRLReason indicated must contain a value permitted for CRLs, as specified in Section 7.2.2 of the CA/B Forum Baseline Requirements.

7.3.1 Version Number(s)

The version number for request and responses shall be version one.

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 *singleExtension*s 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 and CPS 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.C. § 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 result 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, Extended Validation Code Signing and Time-Stamping Certificates are adhering to requirements of the TrustID CP 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 8.2.

IdenTrust will conduct a separate audit using the standards listed in Appendix B when assessing Enterprise RAs. Sponsoring Organization's with Enterprise RAs will produce the records necessary for a quarterly assessment of their Server Certificates by the IdenTrust security office.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

IdenTrust has passed previous audits that have demonstrated compliance with the TrustID CP and 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 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 Baseline Requirements. A Certificate is deemed as 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 B when assessing Server Certificates issues for Sponsoring Organizations with Enterprise RAs.

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[2], 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.
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

[2] 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.

ensure that IdenTrust conforms to its TrustID CP and CPS and familiarity with those documents is necessary for performing the audit for either IdenTrust or for 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 RAs will do the same.

8.3 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 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.

8.4 TOPICS COVERED BY ASSESSMENT

IdenTrust's engagement of its auditors 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 WebTrust for CAs v2.0 or newer and WebTrust for CAs SSL Baseline with Network Security v2.2 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.

Sponsoring Organizations with Enterprise RAs will comply with the TrustID CP, this CPS, and their contracts with IdenTrust.

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 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 thirty 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 web site 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 make its Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three 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-labelled 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 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.

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 customer agreements. Any fees collected for Certificate applications that are not approved will be refunded.

9.1.6 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, 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.

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 personal 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 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 purposes of the TrustID CP and this CPS. Access to this information will be restricted to those with an official need-to-know in order 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

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. 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 request, 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 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 public Certificate Transparency logs created for this purpose.

9.4.4 Responsibility to Protect Private Information

See Section 9.3.2.

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 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 Identity Proofing process as described in Section 3.2;
- Verification of authorization by Domain Name Registrant as described in Section 3.2.2.4.
- 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 2.2.1;
- 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 and this CPS, 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 CERTIFICATE AGREEMENT (AND IN ACCORDANCE WITH THE TRUSTID CP , IF THE TRUSTID CP HAS BEEN INCORPORATED BY REFERENCE IN THE CERTIFICATE AGREEMENT; AND IN ACCORDANCE WITH THIS CPS, IF THIS CPS HAS BEEN INCORPORATED BY REFERENCE IN THE CERTIFICATE AGREEMENT); AND
- The TrustID Certificate meets all requirements of the applicable Certificate Agreement (and the TrustID CP, if the TrustID CP has been incorporated by reference in the Certificate Agreement; and this CPS, if this CPS has been incorporated by reference in the Certificate 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., Certificate 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 Certificate 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 Certificate 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 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 it is Private Keys and Activation Data are protected in accordance with Sections 4 and 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) it's 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, other provisions of this 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 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 Sections 3 and 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 Sections 5 and 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 Card Authentication Certificate and TrustID Device Certificate provided the RA perform the Key Pair generation on an approved Cryptographic Module in accordance with Section 6.2.1.

9.6.3 Subscriber Representations and Warranties

The responsibilities of each Applicant/PKI Sponsor/Subscriber are to:

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 EV 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 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, a Subscriber's obligations will be governed by the Certificate Agreement between the Subscriber and IdenTrust.

9.6.4 Relying Party Representations and Warranties

Prior to 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 of this CPS;

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, liability of IdenTrust shall be limited as described below in this Section 9.8.

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 9.8 of the TrustID CP shall apply.

UNLESS OTHERWISE SPECIFIED IN SECTION 9.8 OF THE TRUSTID CP, 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 Certificate 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 Baseline Requirements or that otherwise might exist because of the Issuance or maintenance of TrustID Certificates or reliance thereon by Authorized Relying Parties or others. IdenTrust will defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a TrustID Certificate issued by IdenTrust, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a TrustID Certificate issued by IdenTrust where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a TrustID Certificate that is still valid, or displaying as trustworthy: (1) a TrustID Certificate that has expired, or (2) a TrustID Certificate that has been revoked (but only in cases where the Revocation status is currently available from IdenTrust online, and the application software either failed to check such status or ignored an indication of revoked status).

9.10 TERM AND TERMINATION

9.10.1 Term

This CPS shall remain in effect until a new CPS is approved by the IdenTrust PMA or a 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 effect resulting from a termination of this CPS are communicated via IdenTrust's Repository.

9.10.3 Effect of Termination and Survival

The conditions and effect 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, 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:

1. 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
2. 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 of this CPS. 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 prior to 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 change. Comments may be filed with IdenTrust within the comment period. Decisions with respect to the proposed changes are at the sole discretion of IdenTrust.

A copy of the TrustID CP and this CPS is available in electronic form on the Internet at https://secure.identrust.com/certificates/policy/ts/

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 2.9.13 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 CP 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 event, IdenTrust will immediately (and prior to 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 (prior to 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 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 OMITS 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 TrustID 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 TrustID CPS by IdenTrust will be effective unless such waiver makes express reference to a waiver of a particular section or sections of this TrustID 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 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 RFC 5280 and Baseline Requirement.

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 four months after termination of the applicable Authorized Relying Party Agreement or two years after the Authorized Relying Party's validation of the TrustID Certificate with IdenTrust's Repository, whichever occurs first.

10 APPENDIX A: Certificate Profiles

See the TrustID Certificate Profile document to view profiles that are not provided in this abbreviated list.

10.1 SERVER CERTIFICATES:

10.1.1 TrustID Server Subordinate CA Certificate Profile

Field	Value
version	V3 (2)
serialNumber	Must be unique. At least 64 bits of entropy.
Issuer signatureAlgorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer distinguishedName	cn = IdenTrust Commercial Root CA x*[n]* or IdenTrust Public Sector Root CA x*[n]* o = IdenTrust c = US The content of the Issuer Distinguished Name field must match the Subject DN of the Issuing CA *[x]:**D**(Domain validation; **O**(organization validation **E(**Extended validation)* *[n]:* Iteration of the IdenTrust Commercial Root CA (e.g., IdenTrust Commercial Root CA 1, IdenTrust Commercial Root CA 2, etc.) or IdenTrust Public Sector Root CA (e.g., IdenTrust Public Sector Root CA 1, IdenTrust Public Sector Root CA 2, etc.)
validity	Up to 15 years expressed in UTC format
subjectDistinguishedName	cn = *[d]* CA *[n]* ou = TrustID Server o = IdenTrust c = US *[d]:* Optional pre-descriptor *[n]* iteration of the named CA e.g.; TrustID Server CA 01 TrustID Server CA E1 TrustID Server CA D1 In the case of an Enterprise Server CA: [Enterprise Name] Server CA1; [Enterprise Name] Server CA2; Etc.
subjectPublicKeyInfo	2048 bit RSA Key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Extension	Value
authorityKeyIdentifier	C = no; KeyIdentifier is the identifier defined in the subjectKeyIdentifier extension of the Issuer CA Certificate

Field	Value
subjectKeyIdentifier	C = no; KeyIdentifier is SHA-1 hash of subjectPublicKey
keyUsage	C = yes; KeyCertSign cRLSign digitalSignature
extKeyUsage	C = no; Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
certificatePolicies	C = no; anyPolicy {2.5.29.32.0} [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://secure.identrust.com/certificates/policy/ts/index.html [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=This TrustID Server Certificate has been issued in accordance with IdenTrust's TrustID Certificate Policy found at https://secure.identrust.com/certificates/policy/ts/index.html
basicConstraints	C = yes; cA=True pathLenConstraint = 0
nameConstraints	This extension may be present and marked critical.
authorityInfoAccess	This extension is optional If present: C = No; [1]accessMethod ::={1.3.6.1.5.5.7.48.1} accessLocation::= { http://commercial.ocsp.identrust.com} [2] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= { URL = “http://validation.identrust.com/roots/commercialrootca1.p7c” }
cRLDistributionPoints	C = no; [1] CRL HTTP URL = http://validation.identrust.com//crl/commercialrootca1.crl

10.1.2 End-Entity Server Certificate Profile

Field	Value
version	V3 (2)
serialNumber	Must be unique. At least 64 bits of entropy
Issuer signatureAlgorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer distinguishedName	Derived from issuing CA
validity	Up to 815 days when issued after April 20, 2018 and up to 397 days when issued after August 31, 2020.
subjectDistinguishedName	Unique X.500 subject DN cn* = <Fully Qualified Domain Name> ou = <Optionally, the Organization Department when collected and verified. > o = <unique Organization Name> LocalityName = <Verified City of the Organization> StateOrProvinceName = <Verified state of the Organization. State name is spelled out. E.g., Nebraska, Utah> c = <country of Organization. Country expressed as a two-letter ISO 3166-1 country code> Additional fields for Server EV Certificates: <Business Category> 2.5.4.15 = <pre-determined string> <Jurisdiction of Incorporation> 1.3.6.1.4.1.311.60.2.1.1 = <Incorporation Locality> 1.3.6.1.4.1.311.60.2.1.2 = <Incorporation State/Province> 1.3.6.1.4.1.311.60.2.1.3 = <Incorporation Country> <Registration Number> 2.5.4.5 = <Registration Number from incorporation agency, date of incorporation, or the string “Government Entity”> 2.5.4.97 <Organizational Identifier> {Optional} If present, The Organization Identifier must be encoded as a PrintableString or UTF8String and with the structure defined in Section 9.2.8 of the latest version of the CA/B Guidelines for The Issuance and Management Of Extended Validation Certificates. ** If the CN is present, it will contain a single IP address or FQDN that is one of the values contained in the Certificate’s subjectAltName extension.*
subjectPublicKey Information	2048 bit RSA Key modulus, rsaEncryption
Extension	**Value**

Field	Value
authorityKeyIdentifier	C = no; Octet String (same as Subject Key identifier in Issuing CA Certificate)
basicConstraints	This extension is optional. If present: - Marked as critical - The cA flag value set to false - The pathLenConstraint is none
subjectKeyIdentifier	C = no; Octet String (same as in PKCS-10 request from the Subject or calculated by the CA)
keyUsage	C = yes; Optional; digitalSignature keyEncipherment
extKeyUsage	C = no; Required; id-kp-serverAuth id-kp-clientAuth
certificatePolicies	C = no; Required **For Server DV Certificates** {2.16.840.1.113839.0.6.5} {2.23.140.1.2.1}[3] **For Server OV Certificates** {2.16.840.1.113839.0.6.3} {2.23.140.1.2.2} **For Server EV Certificates** {2.16.840.1.113839.0.6.9} {2.23.140.1.1} [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://secure.identrust.com/certificates/policy/ts/ [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: This TrustID Server Certificate has been issued in accordance with IdenTrust's TrustID Certificate Policy found at https://secure.identrust.com/certificates/policy/ts/
subjectAltName	C = no; Required, OR; C= yes; Required if the Subject Distinguished Name field is empty DNSName=<Fully Qualified Domain Name or Names> or an IP Address containing the IP address of a server

[3] When this policy identifier is asserted, the Server DV Certificate does NOT include organizationName, givenName, surname, streetAddress, localityName, stateOrProvinceName, or postalCode in the Subject field.

Field	Value
authorityInfoAccess	C = no; [1]accessMethod ::={1.3.6.1.5.5.7.48.1} accessLocation ::= { URL = http://commercial.ocsp.identrust.com} [2] accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= {URL = http://validation.IdenTrust.com/certs/trustidcax*[m]*.p7c} *[m]:* Iteration of the TrustID Server CA xn (e.g., TrustID Server CA D1, TrustID Server CA O1, TrustID Server CA E1, etc.)
cRLDistributionPoints	C = no; Required [1]CRL HTTP URL=http://validation.identrust.com/crl/trustidcaa5*[m]*.crl *[m]:* Iteration of the TrustID Server CA xnx (e.g., TrustID Server CA D1, , TrustID Server CA O1, TrustID Server CA E1, etc.)

For all other Certificates, Certificate Profiles are addressed in a separate document available to major customers, regulators and auditors under Non-Disclosure Agreement.

11 APPENDIX B: Enterprise RAs as LRAs Auditing and Security Standards

- Trustworthy registration agent employees as specified in Section 5.3.1;
- Physically secure environment meaning 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.

12 APPENDIX C: Certificate Hierarchy

The table below depicts IdenTrust Certificate hierarchy associated to this TrustID CPS. This hierarchy includes all CA certificates for which associated certificates are still active at the time of this CPS publication. This hierarchy includes Root CA Certificates, Subordinate CA Certificates and the eligible End Entity Certificate types. Root CA and Subordinate CA Certificates are documented by their common name. End entity Certificates are documented by their use.

Until such time that all certificates issued under a CA certificate have expired, the CA is subject to audit review. All private keys are archived per the requirements stated in Section 5.5.1.

Certificate Level in Hierarchy	Common Name or Use
Root CA:	**DST Root CA X3 Expiration 09/30/2021**
Subordinate CA	**Let's Encrypt Authority X3 Expiration 03/17/2021**
End Entity Certificate Type	• Server DV Certificates
Applicable Practices	• This CPS for the Subordinate CAs • External CPS for end entities
Subordinate CA	**Let's Encrypt Authority X4 Expiration 03/17/2021**
End Entity Certificate Type	• Server DV Certificates
Applicable Practices	• This CPS for the Subordinate CAs • External CPS for end entities
Subordinate CA	**R3 Expiration 09/29/2021**
End Entity Certificate Type	Server DV Certificates
Applicable Practices	• This CPS for the Subordinate CAs • External CPS for end entities
Subordinate CA	**R4 Expiration 09/29/2021**
End Entity Certificate Type	Server Certificates
Applicable Practices	• This CPS for the Subordinate CAs • External CPS for end entities
Subordinate CA	**ISRG Root X1 Expiration 09/30/2024**
End Entity Certificate Type	Server Certificates
Applicable Practices	• This CPS for the Subordinate CAs • External CPS for end entities
Root CA	**IdenTrust Commercial Root CA 1 Expiration 01/16/2034**
Subordinate CA	**TrustID CA A12 Expiration 02/18/2023**
End Entity Certificate Type	• TrustID Secure Email (Client Auth, S/MIME) • TrustID Personal (ClientAuth, Digital Signature, Encryption, S/MIME) • TrustID Business (Client Auth, Digital Signature, Encryption, S/MIME) • TrustID FATCA Organization (Client Auth, Digital Signature, Encryption, S/MIME)

Applicable Practices	• This CPS for the Subordinate CAs • This CPS for end entities
Subordinate CA	**TrustID CA A13 Expiration 02/12/2030**
End Entity Certificate Type	• TrustID Secure Email (Client Authentication, S/MIME) • TrustID Personal (Client Auth, Digital Signature, Encryption, S/MIME) • TrustID Business (Client Auth, Digital Signature, Encryption, S/MIME) • TrustID FATCA Organization (Client, Digital Signature, Encryption, S/MIME)
Applicable Practices	• This CPS for the Subordinate CAs • This CPS for end entities
Subordinate CA	**TrustID Server CA A52 Expiration 03/20/2022**
End Entity Certificate Type	• Server Certificates • TrustID Extended Validation Time-Stamping • TrustID Extended Validation Code Signing
Applicable Practices	• This CPS for the Subordinate CAs • This CPS for end entities
Subordinate CA	**TrustID Server CA O1 Expiration 12/12/2029**
End Entity Certificate Type	• Server DV+OV Certificates
Applicable Practices	• This CPS for the Subordinate CAs • This CPS for end entities
Subordinate CA	**TrustID Server CA E1 Expiration 12/12/2029**
End Entity Certificate Type	• Server DV+OV+EV Certificates
Applicable Practices	• This CPS for the Subordinate CAs • This CPS for end entities
Subordinate CA	**TrustID Code Signing CA 1 Expiration 09/18/2027**
End Entity Certificate Type	• EV Code Signing Certificates
Applicable Practices	• This CPS for the Subordinate CAs • This CPS for end entities
Subordinate CA	**TrustID Time-Stamping CA 1 Expiration 12/21/2030**
End Entity Certificate Type	• Time-Stamping Certificates
Applicable Practices	• This CPS for the Subordinate CAs • This CPS for end entities
Subordinate CA	**Booz Allen Hamilton BA CA 01 Expiration 08/28/2025**
End Entity Certificate Type	• TrustID Business (Client Authentication, Digital Signature, Encryption, S/MIME)
Applicable Practices	• This CPS for Subordinate CAs • External RPS for end entities
Subordinate CA	**TrustID SAIC Public Email Issuing CA Expiration 10/13/2026**

End Entity Certificate Type	• TrustID Business (Client Authentication, Digital Signature, Encryption, S/MIME)
Applicable Practices	• This CPS for Subordinate CAs • External RPS for end entities
Subordinate CA	**TrustID HID Enterprise CA 1 Expiration 04/27/2027**
End Entity Certificate Type	• Document Signing, Smart Card Logon, Client Authentication, Secure Email (S/MIME), Card Authentication, Digital Signature, Encryption, Content Signing
Applicable Practices	• This CPS • External CPS for end entities
Subordinate CA	**HydrantID Server CA O1 Expiration 12/12/2029**
End Entity Certificate Type	• Server DV+OV+EV Certificates
Applicable Practices	• This CPS • External CPS for end entities
Root CA	**IdenTrust Public Sector Root CA 1 Expiration 01/16/2034**
Subordinate CA	**IdenTrust Public Sector Server CA 1 Expiration 01/16/2034**
End Entity Certificate Type	• Server DV+OV+EV Certificates
Applicable Practices	• This CPS • External CPS for end entities

