IdenTrust
part of HID Global

TrustID®
Certificate Policy

IdenTrust Services LLC.
Version 4.8.6
September 1, 2023

TABLE OF CONTENTS

1 INTRODUCTION

1.1 OVERVIEW

This IdenTrust TrustID Certificate Policy (CP) is the Policy under which IdenTrust Services, LLC (IdenTrust) establishes and operates a Public Key Infrastructure ("PKI") for issuing Certificates that can be used in an interoperable manner with other X.509 PKIs. It does not define a particular implementation practice of the TrustID PKI, nor the plans for future implementations or future Certificate policies. This document will be reviewed and updated as described in Section 9.12, based on criteria that include but are not limited to the current and expected use of the TrustID PKI, operational experience, changing threats, and further analysis.

This Policy describes the roles, responsibilities, and relationships of the PKI Service Providers and End Entities (collectively "Participants"), and the rules and requirements for the Issuance, acquisition, management, and use of TrustID Certificates to verify Digital Signatures and to encrypt and authenticate electronic communications.

This document defines the creation and management of X.509 Version 3 Public Key Certificates for use in applications requiring authentication of an End Entity, digital signing of content by an End Entity, digital signing of content by a content signer, and data or message confidentiality between networked computer-based systems and/or Individuals. Such applications include, but are not limited to, electronic mail, the transmission of confidential information, signature of electronic documents, and authentication of infrastructure components such as web servers, firewalls, and directories.

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

NOTICES:

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

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

C. PKI Participants (see Section 1.32 of the Policy Copy) must not, as PKI Participants, rely on 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 a repository is 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 CP was approved for publication on August 31, 2023 by the IdenTrust Policy Management Authority (PMA). The following table contains subsequent revisions:

Table 1 - CP Versions

Version	Date	Summary of Changes/Comments
1.7	May 22, 2015	Updates CP compliance, the inclusion of FATCA Organization Certificate, inclusion of Certificate Policy OID for hardware practices, compliance with the TLS BR. 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.
2.0	September 15, 2016	Incorporated language to support Secure Email Certificates. Updated format for ease of use.
2.1	October 27, 2016	Updated the document to include updates for the TLS BR v1.4.0 and EV TLS BR v1.6.0.
2.2	April 12, 2017	Add SHA-256 hash algorithm support with its OID for TrustID Personal, TrustID Personal Hardware, and TrustID Business Certificates.
2.3	September 8, 2017	Updated the document to include updates for the CS v1.4.1, EV TLS BR v1.6.1 , Device Certificates, and Card Authentication Certificates. Implemented September 8, 2017, and CP documentation approved by the PMA committee on September 12, 2017.
2.4	January 30, 2018	Updates to reflect updated TLS BR v1.4.4.
4.0	May 31, 2018	1. Conversion to RFC 3647 format. 2. Add CT Logging.
4.1	August 17, 2018	Section 1.2.2: Add the last 2 OIDs for TrustID Business Certificates.
4.2	October 18, 2018	Updates to clarify comments by Mozilla in reference to the EV Server Certificate application.
4.3	January 31, 2019	1. Section 1.1: Updates to reflect conformance with the TLS BR v1.6.4. 2. Section 1.6.1: Add definitions: • Certificate Chain. • Subordinate CA Certificate. 3. Section 4.9.1 and 4.9.5: Updates to better reflect the process in place to handle Server Certificate Revocation that is in line with the BR. 4. Section 9.8: Update liability language for Extended Validation Certificates.
4.4	May 31, 2019	1. Section 1.1 move text to Section 2.2. 2. Section 1.2.2 OID renaming and new OID. 3. Section 1.6.1 Added definitions: CAA Resource Record Set; Technically Constrained Subordinate CA. 4. Section 2.2 Added text removed in Section 1.1. 5. Section 3.1.1 Added Medium Assurance Hardware Unaffiliated. 6. Section 3.2.3 Added TrustID Medium Assurance Hardware Unaffiliated. 7. Section 3.2.6.1 Added Cross-Certification. 8. Section 3.2.2.4 Update to reflect that the validation method for Server Certificates is being recorded.

Version	Date	Summary of Changes/Comments
		9. Section 4.2 Updates on how the processing of 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 pointing to the PMA approved list of FIPS 140 Cryptographic Modules in Appendix A. 12. Section 7.1.5 Update to reflect that not fully Technically Constrained Subordinate CA's are publicly disclosed. 13. Appendix A: List of PMA approved list of FIPS 140 Cryptographic Modules.
4.5	September 27, 2019	1. Updates relevant to the NetSec BR v1.7 to be in line with the BR SC3 approved on 8/16/18 to be effective April 1, 2020: Sections 1.6.1; 5.4 and 5.4.8. 2. Updates relevant to EV Code Signing and Time-Stamping Certificates: Sections 3.1.1; 3.2.12.1; 4.9.1; 4.10.1; 6.2.1; 6.3.2 and 9.8.
4.6	November 21, 2019	OID Updates to support the offering of Server Certificates for Domain Validation (DV) only, Domain Validation (DV) with Organization Validation (OV) only, and EV Server only.
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. Updates to support Issuance of Server Certificates to IP Addresses. 4. Section 5 updates. 5. Addition of Subordinate CA A13 as a replacement for Subordinate CA A12.
4.7.1	March 26, 2020	1. Align section headers with RFC 3647 format. 2. Clarify CP/CPS publication schedule frequency. 3. Update http addresses. 4. Clarify Language for Server Certificate types.
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. Updates to Section 3.1.2 for Sever Certificates. 2. Adding matrix to Section 5.4.1 Types of Events Recorded. 3. Correcting reference in Section 5.5.1 Types of Records Archived.
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.
4.7.5	September 28, 2020	1. Updated validity period of Server Certificates for up to 397 days effective September 1, 2020. 2. Updates in Sections 4.9.9, 4.9.10, and 7.3 for new OCSP requirements. 3. Updates to Section 7.1.4 Name Forms. 4. Updates to Section 7.2.2. CRLs. 5. Updates to Section 8.6 – Communication of Audit Results.
4.7.6	December 28, 2020	1. Section 4.9.1: Allow Applicants to revoke Secure Email Certificates. 2. Section 3.3.1; 4.7.3.; Reduce the 90-day renewal period to 30-days on Server Certificates. 3. Section 5.1.2: Systems monitoring.

Version	Date	Summary of Changes/Comments
		4. Cosmetic changes to standardize references. 5. Add language to address special situations for extended use of Private Keys for CAs. 6. Clarified language regarding liability re: revoked Certificates
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. 3. Section 4.2.1: Update to clarify the age of documentation for EV Code Signing Certificates.
4.7.8	June 4, 2021	1. Updates for Code Signing: • Minimum key size 3072 bit for RSA. • Add Code Signing Certificates (Non-EV).
4.7.9	August 6, 2021	1. Section 4.7.3: Renewal notification updates. 2. Addition of Code Signing Subordinate CAs. 3. Remove optional OU from Server Certificates. 4. Section 4.9.12: Updates to reflect methods demonstrating private key-compromise. 5. Support of ECDSA for Code Signing Certificates.
4.8.0	January 27, 2022	1. Update Section 3.2.2. adding extended validation sources. 2. Updates to Section 6.3.2 for validity periods on human Certificates to be a maximum of 825 days effective April 1, 2022. 3. Appendix A: Add SafeNet® eToken® 5110 CC.
4.8.1	April 11, 2022	1. Update Key Sizes in Section 6.1.5. 2. Update Operational and Key Usage Validity Periods in Section 6.3.2.
4.8.2	May 12, 2022	1. Add BR OID for Timestamping Certificates on Section 1.2.2. 2. Updates in Retention Period for Archive on Section 5.5.2 .
4.8.3	May 27, 2022	1. Updates to Section 4.10.1 to better reflect compliance 2. Section 6.3.2 update table.
4.8.4	December 2, 2022	1. Addition of new definitions to Section 1.6.1. 2. Cosmetic updates in Sections 1.2, 1.2.1, 1.2.2, 1.6.1, 1.6.2, 3.1.1, 3.2, 3.2.2, 3.2.2.6, 3.2.3.8, 4.2.1, 4.9.1.1, 6.3.2. 3. Cleanup update in Sections 2.2. 4. Updates for verification of FATCA Certificates in Section 3.2. 5. Updates to CSA OCSP Responder Certificate Operational Period in Section 6.3.2. 6. Removal of SHA-1 signatures in Section 7.1.3.1. 7. Add Section 8.7, self-audits. 8. Update Insurance Coverage details in Section 9.2.1. 9. Update Section 9.8 to be in line with the TrustID CPS.
4.8.5	January 26, 2023	1. Add a reference to the NetSec BR v1.7 in Section 2.2.2
4.8.6	September 1, 2023	Updates based on the TLS BR v2.0.0 and S/MIME BR v1.0.0, 1.0.1 1. 1.2.2 Updated names and added S/MIME OIDs 2. 1.3.2.1 Added section 3. 1.5.2 Moved reference to Section 4.10.2 4. 1.6.1, 1.6.2 Added/Updated definitions/acronyms 5. 2, 2.1,2,2, 2.3 Updates for repositories 6. 2.3 Updates for Time or Frequency of Publication

Version	Date	Summary of Changes/Comments
		7. 2.3 Access Updated Access Controls on Repositories 8. 3.1.3.1, 3.2.3.2 Added sections 9. 3.2.2, 3.2.2.1 Updates for Organization validation 10. 3.2.2.6, 3.2.2.7, 3.2.2.8, 3.2.2.10, 3.2.2.10.1 added sections 11. 3.2.3, Updates for Individual identity 12. 3.2.3.3.1 Added section 13. 3.2.6 Updates for Criteria of Interoperation 14. 3.2.8 Updates for validation of Email Address 15. 3.2.10 Added section 16. 4.1, 4.2.1, 4.2.2 Updates for Certificate application 17. 4.3.1 Updates for Certificate issuance 18. 4.9.7.1, 4.9.7.2, added sections 19. 4.9.9, 4.9.10 Updates for Certificate revocation 20. 4.10.2 Updates for Service Availability 21. 5.3.3 Updates for Training Requirements 22. 5.4.1 Updates for Types of Events Recorded 23. 5.4.3 Updates for Retention Period Log 24. 5.5. Updates for Record Archival 25. 5.7 Updates for Comprise and Disaster Recovery 26. 6.1.1 Updates for Key Pair Generation and Installation 27. 6.1.2 Updates for Private Key Delivery to Subscriber 28. 6.1.5 Updates for Key Sizes 29. 6.1.6 Updates for Public Key Parameters 30. 6.2, 6.2.6, 6.2.7. Updates for Private Key Protection 31. 6.3.2 Updates for Certificate Operational Periods 32. 6.5.1 Updates for Computer Security Controls 33. 6.7 Updates for Network Security Controls 34. Updates for Certificate Profiles adding reference to the TLS BR and S/MIME BR updates for Compliance Audit 35. 8.1. Updates for Identity/Qualifications of Assessor 36. 8.4 Updates for Topics Covered by Assessment 37. 8.8 Added section 38. 9.4 Updates for Information Treated as Private 39. 9.4.1. 9.4.2, 9.4.4, 9.4.5, Updates for Privacy Plan 40. 9.6.1 Updates for CA Representations 41. 9.6.3 Updates for Subscriber Representations 42. 9.16.3 Updates for Severability

1.2.1 Alphanumeric Identifier

The alphanumeric identifier (i.e., the title) for this CP is the "IdenTrust TrustID Certificate Policy, v4.8.6” or “identrust_trustid_cp_v4.8.6_0901 2023.”

The following Root CAs are governed by this CP document:

- DST Root CA X3
- IdenTrust Commercial Root CA 1
- IdenTrust Public Sector Root CA 1

1.2.2 Object Identifier (OID)

The American National Standards Institute (“ANSI”) has assigned IdenTrust a unique numeric Object Identifier (“OID”) of 2.16.840.1.113839. IdenTrust has registered an OID for this Policy, which may not be used except as specifically authorized by this Policy. The Policy OID to be asserted in TrustID Certificates issued in accordance with this Policy will have a base arc of:{joint-iso-ccitt (2) country (16) USA (840) US-company (1) IdenTrust (113839) CP (0) TrustID-v2 (6)}

The following Certificate types and OIDs will be recognized for use within the PKI established by this Policy. The Certificate types listed below—Personal, Business, and Server—vary depending on the identity of the Subscriber (Individual, Affiliated Individual, and Electronic Device, respectively). All TrustID Certificates issued under this Policy may contain 1 or more OIDs listed below in the Certificate Policies field of the Certificate:

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

Name	Type	IdenTrust Policy OID	CA/B Forum OID
Personal SHA-256 (S/MIME Individual-Validated)	Signing /Encryption	2.16.840.1.113839.0.6.1.1	2.23.140.1.5.4.2
Personal Hardware SHA-256 (S/MIME Individual-Validated)	Signing /Encryption	2.16.840.1.113839.0.6.12.3	2.23.140.1.5.4.2
Medium Assurance Unaffiliated Hardware (S/MIME Individual-Validated)	Signing /Encryption AATL Enabled	2.16.840.1.113839.0.6.12.1	2.23.140.1.5.4.2
Business (S/MIME Sponsor-Validated)	Signing/Encryption/Identity	2.16.840.1.113839.0.6.10.2	2.23.140.1.5.3.2
	Card Authentication	2.16.840.1.113839.0.6.10.100	
Business SHA-256 (S/MIME Sponsor-Validated)	Signing /Encryption	2.16.840.1.113839.0.6.2.1	2.23.140.1.5.3.2
Business Hardware SHA-256 (S/MIME Sponsor-Validated)	Signing /Encryption AATL enabled	2.16.840.1.113839.0.6.12.2	2.23.140.1.5.3.2
Server Domain Validation (DV)	Server authentication	2.16.840.1.113839.0.6.5	2.23.140.1.2.1
Server Organization Validation (OV)	Server authentication	2.16.840.1.113839.0.6.3	2.23.140.1.2.2
EV Server (EV)	Server authentication	2.16.840.1.113839.0.6.9	2.23.140.1.1
EV Code Signing	Signing	2.16.840.1.113839.0.6.14.1	2.23.140.1.3
Code Signing	Signing	2.16.840.1.113839.0.6.14.2	2.23.140.1.4.1
Time-Stamping	Signing	2.16.840.1.113839.0.6.13.1 2.16.840.1.113839.0.6.13.3	2.23.140.1.4.2
FATCA Organization (S/MIME Organization-Validated	Signing/Encryption	2.16.840.1.113839.0.6.8	2.23.140.1.5.2.3

Name	Type	IdenTrust Policy OID	CA/B Forum OID
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 Mailbox-Validated)	Signing/Encryption	2.16.840.1.113839.0.6.11.1	2.23.140.1.5.1.3
Secure Email Hardware (S/MIME Mailbox-Validated)	Signing/Encryption	2.16.840.1.113839.0.6.11.2	2.23.140.1.5.1.3
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 CP 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 this Policy to fulfill any of the following roles: Policy Management Authority, Certification Authority, Registration Authority, Certificate Manufacturing Authority, Repository, Subscriber and Authorized Relying Party.

1.3.1 Certification Authorities (CAs)

Issuing CAs are Organizations authorized by the PMA to create, sign, issue, and manage Certificates. An Issuing CA may issue TrustID Certificates only if it is licensed to use the TrustID mark and approved by the PMA, following satisfaction of the requirements established under the PMA Charter and satisfaction of the requirements for Certificate interoperability specified by the PMA.

Each Issuing CA is bound to act according to the terms of this Policy. An Issuing CA's specific practices, in addition to the more general requirements set out in this Policy, must be set out in a Certification Practice Statement adopted by the Issuing CA and approved by the PMA. The Issuing CA’s CPS will set forth, among other things, the types of TrustID Certificates to be issued by the Issuing CA (e.g., Personal Certificates, Business Certificates, and Server Certificates). An Issuing CA must enter into an agreement with the PMA, for the benefit of all End Entities, to be bound by and comply with the undertakings and representations of this Policy, concerning all TrustID Certificates it issues.

1.3.2 Registration Authorities (RAs)

Each Issuing CA will remain ultimately responsible for all TrustID Certificates it issues. However, under this Policy, the Issuing CA 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 this Policy, and who will Accept TrustID Certificate applications and locally collect, and verify Applicant identity information to be entered into a TrustID Certificate. An RA operating under this Policy is only responsible for those duties assigned to it by the Issuing CA pursuant to an agreement with the Issuing CA or as specified in this Policy. The Issuing CA may require a RA Organization to submit a Registration Practice Statement.

For Server Certificates, the Issuing CA must not delegate domain validation or IP Address validation to third parties.

1.3.2.1 Enterprise Registration Authorities (Enterprise RA)

1. The CA may delegate to an Enterprise RA to verify Certificate Requests from Subjects within the Enterprise RA's own organization. IdenTrust shall not accept Certificate requests authorized by an Enterprise RA unless the following requirements are satisfied: If the Certificate request is for a Mailbox-Validated, Organization-Validated, or Sponsor-Validated profile, IdenTrust shall confirm that the Enterprise RA has authorization or control of the requested email domain(s) in accordance with Section 3.2.2.4.
2. The CA shall confirm that the subject:organizationName name is either that of the delegated Enterprise RA, or an Affiliate of the delegated Enterprise RA, or that the delegated Enterprise RA is an agent of the named Subject.

An Enterprise RA may also submit Certificate Requests using the Mailbox-Validated profile for users whose email domain(s) are not under the delegated organization's authorization or control. In this case, the CA shall confirm that the Email Address holder has control of the requested Email Address(es) in accordance with Section 3.2.8.

1.3.3 Subscribers

The Issuing CA may issue TrustID Certificates to the following classes of Subscribers: Individuals and Organizations.

1.3.4 Relying Parties

This Policy is intended for the benefit of Individuals and Organizations who have entered into an Authorized Relying Party Agreement to be bound by this Policy.

1.3.5 Other Participants

1.3.5.1 Certificate Policy Management Authority (PMA)

The PMA for this Policy is the IdenTrust Policy Management Authority, which will administer the Policy decisions regarding this Policy in the manner provided in the document entitled "Policy Management Authority" and adopted by the management of IdenTrust in 2004.

1.3.5.2 Certificate Manufacturing Authority (CMA)

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

1.3.5.3 Repositories

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

1.3.5.4 PKI Sponsors

Individuals who are employed by the Sponsoring Organization or by an authorized agent who has express authority to represent the Organization but is not the Subscriber. The Sponsoring Organization shall verify that PKI Sponsors are individuals that: (i) sign and submit, or approve a request for a Certificate issued to an Electronic Device on behalf of the Organization, and/or (ii) sign and submit a Certificate Subscriber Agreement on behalf of the Organization, and/or (iii) acknowledge and agree to the Certificate Terms of Use on behalf of the Organization when the Organization is an affiliate of the CA.

1.3.5.5 Trusted Agents

Authorized entities acting as representatives of Sponsoring Organizations to verify the Applicant’s or PKI Sponsor’s identification during the registration process. Trusted Agents shall not have automated interfaces with CAs.

1.3.5.6 Delegated Third Parties

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

1.4 CERTIFICATE USAGE

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

1.4.1 Appropriate Certificate Uses

Applications for which TrustID Certificates are suitable include, but are not limited to, applications that:

- Provide authentication-based access and secure communication with online sources of information, including those that distribute information based on a fee or subscription and those which handle the Subscriber’s personal or restricted information, such as financial institutions, governmental agencies, health/medical and insurance providers, and others;
- Provide support for form signing and other application processes and filings with governmental and non-governmental organizations;
- Sign, encrypt, decrypt and/or verify electronic messages and digital signatures on contracts, letters of credit, wire transfers, foreign exchange transactions, stock transactions, cash management transactions, security interests, bank statements, and other electronic documentation; and sign software that will be trusted by certain operating systems or other software applications;
- Authenticate a device via signed communication.

It is understood not all TrustID Certificates are approved for all applications described above, but that such descriptions provide an overview of applications found among the many different types of TrustID Certificates described under other provisions hereof.

1.4.2 Prohibited Certificate Uses

TrustID Certificates may not be used for: (i) any application requiring fail-safe performance such as (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or (ii) transactions where applicable law prohibits the use of Digital Signatures for such transactions or where otherwise prohibited by law.

Issuing CAs 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: (a) active eavesdropping (e.g., MitM) or (b) traffic management of Domain Names or Internet Protocol (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.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering this CP Document

This CP is owned and 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 Policy 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

1.5.3 Person Determining Certification Practices Statement Suitability for the Policy

The PMA will determine the suitability of any CPS to this Policy.

1.5.4 CPS Approval Procedures

The approval of an Issuing CA's CPS must be in accordance with the procedures specified by the PMA. Where the Issuing CA's CPS contains information relevant to the security of the Issuing CA, all or part of the CPS need not be made publicly available.

1.5.5 Publication and Notification Policies

1.5.5.1 Copy of Policy

A copy of this CP shall be available in electronic form on the Issuing CA's website and via email from the Issuing CA's help desk. Approved Issuing CAs shall post copies of, or links to, this Policy in their Repositories.

1.5.5.2 Notification of Changes

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

1.5.5.3 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 the 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.

The PMA shall review and update this CP on an annual basis or more frequently when required to ensure compliance with the latest approved version of the BR 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 Subscriber Agreement or Authorized Relying Party Agreement. Indications of Acceptance may include without limitation: • Using the TrustID Certificate (after Issuance); • Failing to notify the Issuing CA 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), Account Password, or a manually-held Key share used to unlock a Private Key before creating a Digital Signature).
Affiliate(d)	A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity
Affiliated Individual	An Individual having an affiliation with an Organization who has been authorized by the Organization to obtain a TrustID Certificate that identifies the Organization and the fact of the Individual's affiliation with the Organization. See "Sponsoring Organization."
Applicant	An authorized Individual or Organization that submits application information to an RA or an Issuing CA to obtain, renew, or request revocation of a TrustID Certificate.
Applicant Representative	A Natural Person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: 1. who signs and submits, or approves a Certificate Request on behalf of the Applicant; 2. who signs and submits a Subscriber Agreement on behalf of the Applicant; and/or 3. 3. who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

TERM	DEFINITION
Application Software Supplier	A supplier of email client software or other relying-party application software such as mail user agents (web-based or application based) and email service providers that process S/MIME Certificates
Assumed Name	Also known as "doing business as", "DBA", or "d/b/a" name in the US and "trading as" name in the UK.
Attestation Letter	A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or another reliable third party customarily relied upon for such information.
Audit Period	In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in Section 8.1.
Audit Report	A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirement
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 an Issuing CA allowing the party to rely on TrustID Certificates in accordance with this Policy.
CAA	From RFC 8659: "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS Domain Name holder to specify 1 or more Certification Authorities (CAs) authorized to issue Certificates for that domain name. CAA Resource Records allow a public a public CA to implement additional controls to reduce the risk of unintended Certificate mis-issue." A Certification Authority Authorization (CAA) record is used to specify which Certification 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 misuse.
CA/B Forum	The CA/Browser Forum is a collaborative consortium comprising certification authorities (CAs), providers of Internet browser software, and developers of various applications utilizing X.509 v.3 digital Certificates. These Certificates are employed for securing SSL/TLS connections, Code Signing, and S/MIME communications. The primary purpose of the CA/Browser Forum is to establish, update, and uphold the Baseline Requirements (BR) that govern the issuance of these specific Certificate types by publicly trusted CAs.
CA Certificate	A Certificate that is at the beginning of a certification chain within the TrustID PKI hierarchy. A CA Certificate is established as part of the set-up and activation of the Issuing CA. The CA Certificate contains the Public Key that corresponds to the CA Private Signing Key that the Issuing CA uses to create or manage TrustID Certificates. CA Certificates and their corresponding Public Key may be embedded in software or obtained or downloaded by the affirmative act of an Authorized Relying Party to establish a certification chain.
CA Private Signing Key	The Private Key that corresponds to the Issuing CA's Public Key that is 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

TERM	DEFINITION
	• 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 • 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 Agreement	See Subscriber Agreement.
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 to 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 Holder	See Subscriber
Certificate Manufacturing Authority (CMA)	An Organization that manufactures or creates TrustID Certificates for a particular Issuing CA.
Certificate Policy (CP)	A named set of rules that indicates the applicability of Certificates to particular communities and classes of applications and specifies the Identification and Authentication processes performed before Certificate Issuance, the Certificate Profile, and other allowed uses of Certificates.
Certificate Problem Report	Complaint of suspected Private Key compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
Certificate Profile	The protocol used in the Certificate, CRL, and OCSP Profiles Section, to establish the allowed format and contents of data fields within TrustID Certificates, which identify the Issuing CA, the End Entity, the Certificate's Validity Period, and other information that identifies the End Entity.
Certificate Request	Means a request to issue a Certificate, submitted to the CA by an authorized Individual.
Certificate Subject	See Individual-Validated
Certificate Revocation List (CRL)	A database or other list of Certificates that have been revoked before the expiration of their Validity Period.
Certificate Status Authority	A Certificate Status Authority ("CSA") provides status information on Certificates on behalf of a particular CA through online transactions. A CSA operates a Certificate Status Server ("CSS") which provides authoritative Certificate status and Revocation information to Relying Parties. Examples of a CSA include OCSP servers identified in the authority information access extension (AIA) of a Certificate.
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 organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs. See also Issuing CA.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in creating, issuing, managing, and revoking Certificates.
Code Signing	Term used to signify requirements that are applicable to TrustID Code Signing Certificates.

TERM	DEFINITION
Common Vulnerability Scoring System (CVSS)	A quantitative model used to measure the base level severity of a vulnerability (see https://nvd.nist.gov/home).
Compliance Inspector	A natural person or Legal Entity that meets the requirements of the Identity/Qualifications of an Assessor.
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 TLS BR
Cross-Certified Subordinate CA Certificate	A Certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module(s)	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 140-2].
CS BR	The most current version of the CA/B Forum "*Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates*" published at: https://cabforum.org/baseline-requirements-code-signing/
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 • 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: commonName (cn), emailAddress (mail), organizationName (o), organizationalUnit (ou), locality (l), state (st) and country (c)).
Domain Name	The label assigned to a node in the Domain Name system (see Fully-Qualified Domain Name).
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.
Email Address(es)	Same as Mailbox Address. The format of a Mailbox Address is defined as a "Mailbox" as specified in Section 4.1.2 of the RFC 5321 and amended by Section 3.2 of the RFC 6532, with no additional padding or structure.
End Entity(ies)	Subscribers and Authorized Relying Parties.
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.
EV TLS BR	The most current version of the CA/B Forum "*Baseline Requirements Guidelines for the Issuance and Management of Extended Validation Certificates*" published at: https://cabforum.org/extended-validation/
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 this Policy. The External CA will produce and publish a separate CP and CPS that they will be bound to adhere to its terms (each is publicly disclosed and independently audited with publicly

TERM	DEFINITION
	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 Signing) and Code Signing Certificates	Certificates that contain Subject information as specified in the most current CS BR and that are validated in accordance with those guidelines. Code Signing and EV Code and Code Signing Certificates focus only on assuring the identity of the Subscriber Organization and that the signed code has not been modified from its original form. These Certificates are not intended to provide any other assurances, representations, or warranties. Specifically, Code Signing and EV Code Signing Certificates do not warrant that code is free from vulnerabilities, malware, bugs, or other problems.
Extended Validation Server Certificate (EV Server)	A Certificate that contains Subject information specified in the EV TLS BR 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.
Fully-Qualified Domain Name (FQDN)	A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name system.
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 government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).
High-Security Zone	An area to which access is controlled through an entry point and limited to authorized, appropriately screened personnel and properly escorted visitors, accessible only from Security Zones, separated from Security Zones and Operations Zones by a perimeter. High-Security Zones are monitored 24 hours a day and 7 days a week by security staff, other personnel, and electronic means.
Identity Proofing	To ascertain and confirm through appropriate inquiry and investigation the identity of an End Entity or Sponsoring Organization.
Individual(s)	A natural person and not a juridical person or Legal Entity.
Individual-Validated	Refers to an S/MIME Certificate Subject that includes only Individual (Natural Person) attributes, rather than attributes linked to an Organization. In this CPS, these Certificate types: • Personal SHA-256 • Personal Hardware SHA-256 • Medium Assurance Unaffiliated Hardware
Internal Name	A string of characters (not an IP Address) in a commonName 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.

TERM	DEFINITION
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 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 this CP and the TrustID CPS. In both documents, the term “CA”, and/or “Issuing CA”, means issuance of IdenTrust CA TrustID Certificates.
Jurisdiction of Incorporation	The country and (where applicable) the state or province or locality where the organization’s legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity’s legal existence was created by law.
Key	A general term used throughout this Policy to encompass any 1 of the defined keys mentioned in this document.
Key Compromise	Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.
Key Generation	The process of creating a Key Pair.
Key Generation Script	A documented plan of procedures for the generation of a CA Key Pair.
Key Pair	Two mathematically related Keys (a Private Key and its corresponding Public Key), having the properties that: • One Key can be used to encrypt a communication that can only be decrypted using the other Key • 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.
Man-in-the-Middle Attack (MitM)	An attack on the authentication protocol run, in which the attacker positions himself or herself in between the claimant and verifier so that he can intercept and alter data traveling between them.
Mailbox Address	Refers to an S/MIME Certificate Subject that is limited to subject:emailAddress and/or subject:serialNumber attributes. In this CP, these Certificate types: - Secure Email Software - Secure Email Hardware
Mailbox-Validated	Refers to an S/MIME Certificate Subject that is limited to subject:emailAddress and/or subject:serialNumber attributes. In this CP, these Certificate types: • Secure Email Software

TERM	DEFINITION
	- Secure Email Hardware
Natural Person	An Individual; a human being as distinguished from a Legal Entity.
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).
NetSec BR	The most current version of the CA/B Forum Baseline Requirements for Network and Certificate System Security Requirements published at: https://cabforum.org/network-security-requirements/
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 this Policy, they are used to uniquely identify Certificates issued under this Policy and the cryptographic algorithms supported it.
OCSP Responder	An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.
Onion Domain Name	A FQDN ending with the RFC 7686 ".onion" Special-Use Domain Name. For example, 2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion is an Onion Domain Name, whereas torproject.org is not an Onion Domain Name.
Online Status Check	An online, real-time status check of the validity of a TrustID Certificate using either a CRL or an OCSP. An Online Status Check involving a CRL consists of checking the most recently issued CRL (e.g., not involving a cached CRL). An Online Status Check involving an OCSP consists of a protocol enabling relying-party application software to determine the status of an identified Certificate.
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.
Operations Zone	An area where access is limited to personnel who work there and to properly escorting visitors. Operations Zones should be monitored at least periodically and should preferably be accessible only from a Reception Zone.
Organization(s)	An entity that is legally recognized in its jurisdiction of origin (e.g., a corporation, partnership, sole proprietorship, government department, non-government Organization, university, trust, special interest group, or non-profit corporation).
Organization-Validated	Refers to an S/MIME Certificate Subject that includes only Organizational (Legal Entity) attributes, rather than attributes linked to an Individual. In this CP, the TrustID FATCA Organization Certificate.
Participants	All PKI Service Providers and End Entities authorized to participate in the PKI defined by this Policy.
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 types of

TERM	DEFINITION
	exploits, with a goal of breaking through layers of defenses and reporting on unpatched vulnerabilities and system weaknesses.
PKI Service Providers	The PMA, Issuing CAs, RAs, CMAs, and Repositories participating in the PKI defined by this Policy.
PKI Sponsor	An Individual who is employed by the Sponsoring Organization or an authorized agent who has express authority to represent the Organization but is not the Subscriber. The Sponsoring Organization verifies the PKI Sponsor is an Individual that: • Signs and submits, or approves a request for a Certificate issued to an Electronic Device on behalf of the Organization, and/or • Signs and submits a Subscriber Agreement on behalf of the Organization, and/or • Acknowledges and agrees to the Certificate Terms of Use on behalf of the Organization when the Organization is an affiliate of the CA. See Trusted Agents.
PMA Charter	The document adopted by the PMA that identifies the policies and procedures for administering the CPS and this CP.
Policy	This TrustID Certificate Policy.
Policy Management Authority (PMA)	The Organization responsible for setting up, implementing, and administering Policy decisions regarding this Policy.
Private Key	The Key of a Key Pair is kept secret by its holder, used to create Digital Signatures and to decrypt messages or files that were encrypted with the corresponding Public Key.
Pseudonym(s)	A fictitious identity that a person assumes for a particular purpose. Unlike an anonymous identity, a pseudonym can be linked to the person's real identity.
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 to collectively support the implementation and operation of a Certificate-based Public Key Cryptography system.
Publicly-Trusted Certificate	An IdenTrust TrustID Certificate that is trusted by virtue of the fact that its corresponding Root CA Certificate is distributed as a trust anchor in widely-available application software.
Qualified Auditor	A Natural Person or Legal Entity that meets the requirements of Section 8.2.
Random Value	A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.
Reasonable Reliance	For purposes of this Policy, 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 this Policy • 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 the Issuing CA • Used the TrustID Certificate for purposes appropriate under this Policy and under circumstances where reliance would be reasonable and in good faith in light of all the

TERM	DEFINITION
	circumstances that were known or should have been known to the Authorized Relying Party before reliance. An Authorized Relying Party bears all risk of relying on a TrustID Certificate while knowing or having reason to know of any facts that would cause a person of ordinary business prudence to refrain from relying on the Certificate).
Reception Zone	The entry to a facility where the initial contact between the public and the Issuing CA or RA occurs, where services are provided, information is exchanged, and access to Restricted Zones is controlled.
Registration Authority (RA)	A Legal Entity that is not a CA, and hence does not sign or issue Certificates, contractually delegated by IdenTrust to Accept and process Certificate applications, and to verify the identity of potential End Entities, and authenticate the information contained in Certificate applications, in conformity with the provisions of this Policy and related agreements. RA's do not sign or issue Certificates.
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.
Reliable Data Source	An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.
Reliable Method of Communication	A method of communication, such as a postal/courier delivery address, telephone number, or Email Address, that was verified using a source other than the Applicant Representative.
Repository	An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
Relying Party	Any Natural Person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.
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. See definitions for Supervised Remote Identity Proofing and Unsupervised Remote Identity Proofing for additional 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
Restricted Zones	Any 1 of: • An Operations Zone; • A Security Zone; and • A High-Security Zone.
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).

TERM	DEFINITION
Root CA Certificate	The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers, and that issues Subordinate CA Certificates.
Root Certificate	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
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 Email Software, Secure Email Hardware Certificates	Also referred as Mailbox-Validated, a Certificate that is issued to an Email Address over which the Certificate Applicant demonstrates control to the RA by the Certificate Applicant responding to a unique challenge sent during the authentication process conducted before Issuance. A Secure Email Certificate can be used for the purposes of email signing, email encryption, and client authentication when installed in an approved hardware Cryptographic Module.
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.
Security Office	IdenTrust's Security Office is comprised of a number of Security Officers 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. The Security Office operates under the oversight of the IdenTrust Security Officer and the IdenTrust Head of IdenTrust Operations.
Security Officer	Is a Trusted Role 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 the Issuing CA CPS.
Security Zone	An area to which access is limited to authorized personnel and to authorized and properly escorted visitors. Security Zones should preferably be accessible from an Operations Zone, and through a specific entry point. A Security Zone need not be separated from an Operations Zone by a secure perimeter. A Security Zone should be monitored 24 hours a day and 7 days a week by security staff, other personnel, or electronic means.
Shared Secret	Activation Data that is used to assist parties in authenticating identity 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 the Issuing CA. For purposes of establishing identity between the Subscriber and the Issuing CA necessary for Certificate Issuance, a Shared Secret consists of different Activation Data, which is shared among the RA, Subscriber, and Issuing CA.
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 Organization and the fact of the Individual's affiliation with the Organization. See "Affiliated Individual."
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.
S/MIME BR	The most current version of the CA/B Forum *"Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates"* published at: https://cabforum.org/smime-br/

TERM	DEFINITION
S/MIME Certificate	TrustID Mailbox-Validated, Individual-Validated, Sponsor-Validated and Organization-Validated Certificates.
Sponsor-Validated	Refers to an S/MIME Certificate Subject which combines Individual (Natural Person) attributes in conjunction with an subject:organizationName (an associated Legal Entity) attribute. In this CP, these TrustID Certificate types are considered Sponsor-Validated: • Business • Business SHA-256 • Business Hardware SHA-256 • Medium Assurance Unaffiliated Hardware
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
Subject Identity Information	Information that identifies the Certificate Subject. Subject Identity Information does not include an Email Address listed in the subject:commonName or subject:emailAddress fields, or in the subjectAltName extension.
Subject 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 another Subordinate CA's within the IdenTrust Root Chain. Subordinate CA Certificates and their corresponding Public Keys may be embedded into software obtained or downloaded by the affirmative act of an Authorized Relying Party in order to establish a certification chain within the TrustID PKI hierarchy.
Subscriber	A Natural Person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.
Subscriber Agreement	An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
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 that is utilized by the Applicant/Subscriber in order to ensure the Remote Identity Proofing process employs physical, technical, and procedural measures to provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person Identity Proofing process. Supervised Remote Identity Proofing requires that a third person, in addition to the RA/TA and the Applicant, participate in the Identity Proofing event to attest to the Applicant's identity and act as a witness to the proceedings. 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 Certificate	A Subordinate CA Certificate, that uses a combination of extended Key usage and Name Constraint extensions as defined within the Certificate Profile to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates. .
Terms of Use	Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with this CPS when the Applicant/Subscriber is an Affiliate of the CA or is the CA.
Time-Stamping Authority	An Organization that time-stamps data, thereby asserting that the data existed at the specified time.

TERM	DEFINITION
TLS BR	The most current version of the CA/B Forum "*Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates"* published at: https://cabforum.org/baseline-requirements-documents/
Token	A Cryptographic Module consisting of a hardware object (e.g., a "smart card"), often with memory and a microchip.
TrustID Business, Business SHA-256, Business Hardware SHA-256 Certificates	TrustID Certificates considered as S/MIME Sponsor-Validated.
TrustID FATCA Organization Certificate	TrustID Certificates considered as S/MIME Organization-Validated.
TrustID Personal, Personal SHA-256, Medium Assurance Unaffiliated Hardware Certificates	TrustID Certificates considered as S/MIME Individual-Validated.
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 Trusted Agents.
Trusted Platform Module (TPM)	An international standard for a secure crypto-processor, that is a dedicated microprocessor designed to secure hardware by integrating cryptographic keys into devices.
Trusted Role	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 this Policy.
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.
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 that is utilized by the Applicant/Subscriber in order to ensure the Remote Identity Proofing process employs physical, technical, and procedural measures to provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person Identity Proofing process. For Unsupervised Remote Identity Proofing, only the RA/Trusted Agent and the Applicant are required to participate in the session. Unsupervised Remote Identity Proofing may be used for Basic and Medium Assurance Certificate issuance. Refer to Remote Identity Proofing and Supervised Remote Identity Proofing for related information. Refer to Section 3.2.3.2 In-Person Identification for further definitions regarding Supervised versus Unsupervised Identity Proofing.
Validation Specialist	Someone who performs the information verification duties specified by the CA/B Forum BRs.

TERM	DEFINITION
Valid Certificate	Certificate that passes the validation procedures specified in this CPS which are in line with the RFC 5280.
Validity Period	The intended term of validity of a Certificate, beginning with the date of Issuance ("Valid From" or "Activation" date), and ending on the expiration date indicated in the Certificate ("Valid To" or "Expiry" date).
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.

1.6.2 Acronyms

ACRONYM	DEFINITION
AATL	Adobe® Approved Trust List
AO	Authorizing Officer
ARL	Authority Revocation List
BR	The CA/B Forum Baseline Requirements
CA	IdenTrust Issuing Certification Authority
CAA	Certification Authority Authorization
CMA	Certificate Manufacturing Authority
CMS	Card Management System
CN	Common Name
CP	IdenTrust TrustID Certificate Policy
CPS	IdenTrust TrustID Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
DBA	Doing Business As
DN	Distinguished Name
DNS	Domain Name System
DSA	Digital signature algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EV	Extended Validation
FATCA	Foreign Account Tax Compliance Act
FIPS	Federal Information Processing Standard (U.S. Government)
gTLD	General Top Level Domain
ISO	International Standards Organization
ITU	International Telecommunications Union
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number (e.g., a password)

ACRONYM	DEFINITION
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PMA	The IdenTrust Policy Management Authority
RA	Registration Authority
RFC 6962	Document on Certificate Transparency by the Internet Engineering Task Force (IETF) Organization: https://tools.ietf.org/html/rfc6962
RPS	Registration Practice Statement
RSA	Rivest-Shamir-Adleman cryptosystem
S/MIME	Secure /MIME (Secure/Multipurpose Internet Mail Extensions)
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TPM	Trusted Platform Module
TLS	Transport Layer Security
TTL	Time to Live
URL	Uniform Resource Locator
X.500	The ITU-T (International Telecommunication Union-T) standard 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

The CA shall develop, implement, enforce, and annually update a CP and CPS that describes in detail how the CA implements the latest version of the BRs.

2.1 REPOSITORIES

The CA shall make revocation information for Publicly Trusted Subordinate Certificates and Subscriber

Certificates available in accordance with this Policy.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The CA shall publicly disclose its CP and CPS through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA shall publicly disclose its CA business practices to the extent required by the CA's selected audit scheme (see Section 8.4).

The CA's CP and CPS must be structured in accordance with the RFC 3647 and must include all material required by the RFC 3647.

The CA shall conform to the current version of the BR published at http://www.cabforum.org. In the event of any inconsistency between the CA's CP and CPS, the BR, the BR take precedence over this CP and CPS.

The CA shall host test web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA shall host separate web pages using Server and EV Server Certificates that are i. valid, ii. revoked, and iii. Expired.

2.3 TIME OR FREQUENCY OF PUBLICATION

The CA shall develop, implement, enforce, and annually update the CP and CPS that describes in detail how the CA implements the latest version of the BR. The CA shall indicate conformance with this requirement by incrementing the version number and adding a dated changelog entry, even if no other changes are made to the document.

The CA shall review and update its CP and/or CPS at least every 365 days, incrementing the version number and adding a dated changelog entry, even if no other changes are made to the document.

2.4 ACCESS CONTROLS ON REPOSITORIES

The Issuing CA will not impose any read access controls on:

- This Policy
- The Issuing CA's CA Certificate
- Past and current versions of the Issuing CA's CPS and
- Current versions of WebTrust annual Audits.

The Issuing CA may impose read-only access controls on TrustID Certificates and Certificate status information, in accordance with provisions of this Policy.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

For human Certificates, the Subject Name used for TrustID Certificates shall be the End Entity's authenticated commonName. Each End Entity must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the Certificate Subject Name field and in accordance with PKIX Part 1. The components of the DN must be encoded as a PrintableString or UTF8String.

For Server Certificates, where the commonName is populated, the subject field must contain an X.500 Distinguished Name (DN). The DN must be unique for each subject entity certified by the CA as defined by the issuer field. If Subject naming information is present only in the subjectAltName extension, then the Subject Name must be an empty sequence and the subjectAltName extension must include the FQDN and must be flagged as critical.

The Issuing CA is responsible for performing the Identity Proofing of End Entities before the Issuance of TrustID Certificates. The Issuing CA may perform Identity Proofing itself or may designate 1 or more persons to act as RA. RAs may designate 1 or more employees or agents, to be referred to as Local Registration Agents, to perform Identity Proofing in accordance with this section:

Table 3 - 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.
Business	Identity shall be established by: Verification of the identity of the affiliated Applicant based on Section 3.2.3. Verification of the Organization based on Section 3.2.2.
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. Verification of the Organization based on Section 3.2.2.
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.
Secure Email	Identity shall be established by: Demonstration that the Applicant of the Certificate had control of the Applicant's provided Email Address at the time of email verification, based on Section 3.2.3.9 Secure Email Certificate.

TrustID Certificate Type	Identification Requirements
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 EV TLS BR. When the Subject Distinguished Name is present, it must contain a single IP address or a FQDN that is 1 of the values contained in the Certificate subjectAltName extension.
Server Organization Validation (OV)	Identity for Organization Validation (OV) Server Certificates is established by validating authorization and/or ownership by Domain Name Registrant and verification of the Subject identity information (i.e., identity, DBA/Tradename), the authenticity of the Certificate Request, verification of Individual 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 TLS BR.
EV Server	Identity for Extended Validation 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 EV TLS BR
Code Signing and EV Code Signing	Identity shall be established by: Verification of the Applicant's Organization in accordance with the CS BR.
Time-Stamping	Identity shall be established by: Verification of the Applicant's Organization in accordance with Section 3.2.3.8 of the TrustID CPS
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.

If applications are transmitted electronically, via email, or a website, the transmissions must be secure (e.g., SSL/TLS or similar protocol); otherwise, Certificate applications may be submitted by postal mail or in person.

3.1.2 Need for Names to Be Meaningful

The contents of each Certificate Distinguished Name field must have an association with the authenticated name of the End Entity:

TrustID Certificate Type	Naming Requirements
Personal and 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**
	In addition to the authenticated commonName (as described above), the DN must also include the authenticated legal Subscribing Organization name in the organizationName. Optionally, the organizationUnitName may be used to name the Subscribing Organization unit/department that is associated with the Subscriber, if provided by the Subscriber.

TrustID Certificate Type	**Naming Requirements**
for Authorized Relying Parties; **FATCA Organization**	
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 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 CN is empty, then the FQDN or a single IP Address must be named in the subjectAltName and must be flagged as critical. If the CN is present, then it will contain a single IP address or FQDN, which is 1 of the values contained in the Certificate's subjectAltName extension.
Server Organization Validation(OV)	Where the CN 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 TLS BR. If the CN is present, then it will contain a single IP address or FQDN which is 1 of the values contained in the Certificate's subjectAltName extension.
EV Server	If present, the CN 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). Wildcard Certificates are not allowed for EV Certificates except as permitted under Appendix F of the EV TLS BR If the CN is present, then it will contain a single IP address or FQDN which is 1 of the values contained in the Certificate's subjectAltName extension.
Code Signing and EV 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. Optionally, the organizationUnitName may be used to name the Subscribing Organization unit/department that is associated with the Subscriber, if provided by the Subscriber. Code Signing Certificates do not include a Domain Name.
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	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 shall not contain anonymous or Pseudonym identities.

Server Domain Validation (DV) Certificates, Device Certificates, and Secure Email Certificates do not name a Subscriber; rather these types of Certificates have subject fields identifying only Domain Names, device identification, or Email Addresses respectfully, (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 the TrustID CPS.

3.1.4 Rules for Interpreting Various Name Forms

The Issuing CA may defer to a naming authority for guidance on name interpretation and subordination.

3.1.4.1 Non ASCII Character Substitution

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

3.1.4.2 Geographic Names

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

3.1.5 Uniqueness of Names

The IdenTrust PMA is responsible for ensuring CAs and RAs enforce name uniqueness within the X.500 name space for which they have been authorized. Specifically, name uniqueness shall be enforced.

The Issuing CA's CPS shall define the following:

- What name forms shall be used, and
- How the CA will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (e.g., if "Joe Smith" leaves a CA's community of Subscribers, and a new, different "Joe Smith" enters the community of Subscribers, how will these two people be provided unique names).

3.1.6 Recognition, Authentication, and Role of Trademarks

An End Entity is not guaranteed that its Distinguished Name or Subject Name will contain any requested trademark. The Issuing CA is not required to subsequently issue a new TrustID Certificate to the rightful owner of any name if the Issuing CA has already issued to that owner a TrustID Certificate containing a DN and Subject Name that is sufficient for identification within the PKI. The Issuing CA is not obligated to seek evidence of trademarks or court orders.

3.1.6.1 Name Claim Dispute Resolution Procedure

The Issuing CA should reserve the right 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. The Issuing CA will investigate and correct if necessary any name collisions brought to its attention. If appropriate, the Issuing CA will coordinate with and defer to the appropriate naming authority.

3.2 INITIAL IDENTITY VALIDATION

The Issuing CA shall be responsible for performing the Identity Proofing of End Entities before the Issuance of TrustID Certificates. The Issuing CA performs Identity Proofing itself, aided by its LRAs, or by elected Enterprise RAs from Sponsoring Organizations, or may designate one or more institutions as RAs. RAs may designate one or more employees or agents, to be referred to as LRAs, and Trusted Agents may be nominated by Sponsoring Organizations and appointed by the Issuing CA 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 4 – TrustID Certificates Initial Identity Validation Requirements

Certificate Type	Identification Requirements
Personal **Medium Assurance Hardware Unaffiliated**	Verification of the identity of the unaffiliated Applicant based on Section 3.2.3 and the performance of electronic identification based on Section 3.2.3.2 or the performance of in-person or Remote Identity Proofing based on Section 3.2.3.3; 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 an in-person or Remote Identity Proofing based on Section 3.2.3.3; Verification of the Organization based on Section 3.2.2 and Section 3.2.2.1; Verification of Individual-Organization affiliation based on Section 3.2.2.2; 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 Section 3.2.2 and Section 3.2.2.1; Verification of the PKI Sponsor's Organization affiliation based on Section 3.2.2.3; Verification of a Certificate request based on Section 3.2.9; Authentication of a Device identity based on Section 3.2.2.4; 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 TLS BR.
EV Server*	In addition to the applicable verification requirements for the Server Certificate listed above, adherence to the requirements listed in the EV TLS BR, and the "TrustID IdenTrust SSL/TLS Organization Identity Extended Validated (EV) Subscriber Agreement", which includes defined roles.
Code Signing, EV Code Signing and Time-Stamping*	A TrustID Code Signing, EV Code Signing Certificate, or TrustID Time-Stamping Certificate identifies an Organization as the Subject of a Certificate, and such Organization is attributable for accountability and responsibility for signatures created by the Organization to be used to verify the integrity of its code. When issuing a TrustID Code Signing, EV Code Signing Certificate, or a TrustID Time-Stamping Certificate, the Issuing CA shall conform with the applicable provisions set forth in the CS BR

Certificate Type	Identification Requirements
FATCA Organization (Organization Validated)	Verification of the Organization based on Section 3.2.2; and Verification of Email Address based on Section 3.2.8.
Administrative RA Certificates	The Subscriber's identity must be established by the Authorized Official (AO). The AO is an elected representative of the Organization requesting an Administrative RA Certificate. This Individual must be bound by the Organization's agreement between the Organization and the Issuing CA. An Organization may have more than one AO but must provide a list including each AO to the Issuing CA for verification purposes.
Secure Email (Mailbox-Validated)	Demonstration of the Applicant's control of the Email Address at the time of email verification, based on Section 3.2.8.
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.
Authorized Relying Parties	Identification and authentication of Authorized Relying Parties may be performed by the Issuing CA and RAs as a consequence of the enrollment process by which an Authorized Relying Party enters into an Authorized Relying Party Agreement with the Issuing CA.

*All documents and data provided for verifying the Server Certificate must not be used by the RA if the document or data was obtained no more than 825 days prior to issuing the Certificate or in the case of EV Server and EV 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 EV TLS BR.

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

**This check is only performed when necessary for Server Certificates. It will be done 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. The Issuing CA or an authorized RA shall establish that the Applicant is in possession of the Private Key corresponding to the Public Key submitted with the application in accordance with an appropriately secure protocol, such as that described in the IETF PKIX Certificate Management Protocol. In the case where the Private Key is generated directly on a Token, or in a Key generator that benignly transfers the Key to a Token, then the End Entity is deemed to be in possession of the Private Key at the time of generation or transfer. 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 (see Private Key Delivery to Subscriber).

3.2.1.1 Binding Identity and Public Key

The Issuing CA must ensure that the Applicant's identity information and Public Key are adequately bound. This association may be established by the use of a Shared Secret (e.g., a password, code, or number), exchanged between the RA, the Applicant, and the Issuing CA, or through a secure referral process. If a Shared Secret is used, care must be taken to ensure that the Applicant and the Issuing CA or RA are the only recipients of the Shared Secret. If an account PIN is used, the RA should not provide it to the Issuing CA. Other mechanisms to achieve such binding may also include the use of a PKI-wide database, system account, or similar authentication mechanisms.

3.2.2 Authentication of Organization Identity

Requests by an Organization for Certificates may be made electronically and must include the Organization's legal name and address. The minimum Identity Proofing required of an Organization under this Policy requires confirmation that:

- The 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.

When Identity Proofing is performed by an RA, the RA will conduct Identity Proofing in accordance with its "Know Your Customer" Policy or other similar procedures, which 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 Organization applying for the Certificate, such as:

- Legal company name;
- A registered Assumed Name (if included in the Subject)
- An organizational unit Name (if included in the Subject)
- Type of entity;
- Year of formation;
- State/region and country jurisdiction of incorporation;
- Names of directors and officers;
- Unique identifier and type of identifier for the Legal Entity;*
- A Legal Entity Identifier (LEI) data reference*;
- Full business address;
- Telephone number;
- Proof of good standing in the jurisdiction where the Applicant is incorporated or otherwise organized; and
- A unique organization identifier shall be included in the Certificate subject:organizationIdentifier as specified in the Certificate Profile.*

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

The CA or RA may use the same documentation or listed above to verify both the Applicant's identity and address. When an LEI data reference is used, the CA shall verify that the RegistrationStatus is ISSUED and the EntityStatus is ACTIVE. The CA shall only allow the use of an LEI when the ValidationSources entry is FULLY_CORROBORATED.

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

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

2. The Assumed Name filing continues to be valid.

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

The sponsoring Organization information should also be 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 Organization's telephone number. Disconnected phone service and other insufficient, false, or suspicious information provided by the Organization warrants further investigation. If requested follow-up information is not forthcoming, or if an Applicant refuses to produce any such requested information, the Certificate application should not be approved. The LRA and/or RA may rely on information previously obtained concerning the Organization and will keep a record of the type and details of information used for verifying identity. Such procedures shall not conflict with other stipulations of this Policy.

For validation of Organizations that apply for EV Server, EV Code Signing, Organization-Validated, or Sponsor-Validated Certificates, at the time of Certificate issuance, IdenTrust must disclose in a publicly available location the sources used to vet the Organization: registration / incorporating agency information.

3.2.2.1 Authentication of the Individual-Organization Affiliation

The Issuing CA may issue Certificates to Applicants affiliated with 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, the Issuing CA may impose, through the Subscriber Agreement, additional restrictions in view of other jurisdictions' laws governing privacy, consumer protection, and other rights of Individuals. For example, if an Applicant is located within the European community, the Subscriber Agreement may contain an additional attestation from the Applicant that the information provided shall be considered business data rather than personal data under European Directive 95/46/EC and/or that the Individual gives his/her unambiguous consent to the processing of such data by IdenTrust.

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

3.2.2.2 Authentication of Subscribing Organization Identity

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

3.2.2.3 Authentication of the PKI Sponsor-Organization Affiliation

For Certificates issued to a Sponsoring Organization and requested by a PKI Sponsor, LRAs and Trusted Agents shall 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. The Issuing CA or the RA shall verify this affiliation through a Sponsoring Organization's representative other than the PKI Sponsor, usually the Trusted Agent where such exists; otherwise, the Issuing CA or the RA initiates communication with the Sponsoring Organization using an independently verified point of contact, i.e., the Issuing CA or the RA obtains telephone numbers for the Sponsoring Organization from a trusted source unrelated to the prospective Sponsoring Organization. The contact used for verification within the Sponsoring Organization may be the human resources department or any Individual in a capacity within the Sponsoring Organization to confirm the affiliation.

3.2.2.4 Verification of Authorization by Domain Registrant

The issuing CA shall confirm that before issuance of Server or S/MIME Certificates, the CA has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least 1 of the methods listed in Section 3.2.2.4 of the TrustID CPS. Additional checks and verification shall be made for Server EV Certificate applications based on the requirements within the EV TLS BR.

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 Section 4.2.1) before Certificate issuance.

For Server Certificates, Domain or IP Address validation must not be delegated to third parties and the Issuing CA shall maintain a record of which of the domain or IP Address validation methods below, including the relevant CA/B Forum BR version number was used to validate every domain or IP Address.

FQDNs may be listed in Server Certificates using dNSNames in the subjectAltName extension or Subordinate CA Certificates via dNSNames in permittedSubtrees within the Name Constraints extension.

Code Signing Certificates shall not include a Domain Name.

3.2.2.5 Authentication for an IP Address

The Issuing CA shall confirm that before issuance, it has validated each IP Address listed in the Certificate Application using at least one of the methods specified in Section 3.2.2.5 of the TrustID CPS.

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, before Certificate issuance. For purposes of IP Address validation, the term Applicant includes the Applicant's parent company, subsidiary company, or Affiliate.

The Issuing CA shall maintain a record of which IP validation method, including the relevant CA/B Forum Baseline Requirements BR version number that was used to validate every IP Address.

3.2.2.6 Wildcard Domain Validation

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

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

See Section 3.2.2.3.3 of the CPS (Verification of gTLD Domains).

3.2.2.7 Data Source Accuracy

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

1. The age of the information provided,
2. The frequency of updates to the information source,

3. The data provider and purpose of the data collection,
4. The public accessibility of the data availability, and
5. The relative difficulty in falsifying or altering the data.

3.2.2.8 CAA Records

As part of the Server Certificate issuance process, the CA shall retrieves and process CAA records in accordance with RFC 8659 for each dNSName in the subjectAltName extension that does not contain an Onion Domain Name. If the CA issues, it is done within the "TTL" field of the CAA record, or 8 hours, whichever is greater.

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, the CA shall limit the length of CNAME chains that are accepted and processes CNAME chains that contain 8 or fewer CNAME records.

The action taken on CAA records shall be logged and when issued, it is done following the instructions in the Section Time to Process Certificate Applications.

3.2.2.9 Authentication of Device Identity

Certificate Requests identifying an Electronic Device as the Subject of a Certificate may only be made by a human sponsor of an approved End Entity to whom the Electronic Device's signature is attributable for accountability and responsibility. When issuing a Certificate identifying an Electronic Device as the Subject of the Certificate, the Issuing CA shall conform with the applicable provisions in the TLS BR; provided, however, when such Certificate is an EV Server Certificate, the Issuing CA shall conform with the applicable provisions of the EV TLS BR.

Certificates identifying an Electronic Device as the Subject of the Certificate can only be issued by an Issuing CA that can ensure accomplishment of the Identity Proofing required in Section 3.2 of the CPS.

3.2.2.10 Code Signing and EV Code Signing Certificates

Likewise, checks and verifications will be made for Code Signing and EV Code Signing Certificate applications based on the requirements within the CS BR

3.2.2.10.1 Card Authentication Certificate and Device Certificates

For TrustID Card Authentication Certificates and TrustID Device Certificates, the Certificate shall 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.

3.2.2.11 Authentication of TrustID Administrative RA Certificates for Devices and Individuals

For TrustID Administrative RA Certificates for Electronic Devices and Individuals, 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.

3.2.3 Authentication of Individual Identity

The Issuance of a TrustID Certificate will be based on Identity Proofing performed by the CA, RA, or Enterprise RA. Process documentation shall include a signed (in writing or digitally) indication by the person performing the identification that the person named was properly identified. The number and types of identification documents (IDs), the process documentation, and the authentication requirements for Issuance of a Certificate shall depend upon the type of Certificate as set forth in the table below:

Table 5 - TrustID Certificates Individual Identity Authentication Requirements

TrustID Certificate Type	Description
Personal	Identity shall be established by: Verification and validation of identity information provided by the Applicant, including out-of-band confirmation, performed in accordance with Verification and Validation of Information ; Maintenance of an ongoing, trusted business relationship in accordance with Know Your Customer Identity Proofing; or Contemporaneous in-person or Remote Identity Proofing consists of a review of at least two acceptable forms of ID, one of which shall be a government-issued photo-ID (see Section Acceptable Forms of Identification Documents), performed in accordance with performance of In-Person Identification.
Medium Assurance Hardware Unaffiliated	Identity shall be established by: Contemporaneous in-person or Remote Identity Proofing consists of a review of at least two acceptable forms of ID, one of which shall be a government-issued photo-ID (see Section Acceptable Forms of Identification Documents), performed in accordance with performance of In-Person Identification.
Business	The Sponsoring Organization confirms the Affiliated Individual's affiliation with the Sponsoring Organization. For non-Enterprise Subscribers, the CA or RA may verify the authority or affiliation of an Individual to represent an Organization to be included in the subject:organizationName of the Certificate using an Attestation Letter provided by the Organization and verified in accordance with Section 3.2.10. In the case of Sponsor-validated Certificates approved by an Enterprise RA, The RA shall validate all identity attributes of an Individual to be included in the Certificate. The RA may rely upon existing internal records to validate Individual Identity. The Enterprise RA shall maintain records to satisfy the requirements of Section 1.3.2.1.

An Organization's Certificates may be issued to Affiliated Individuals after Authentication of Organization Identity outlined in Section 3.2.2 and confirming with the Sponsoring Organization that the Individual has the affiliation alleged in the Certificate application and is authorized to hold a Certificate identifying the Individual as affiliated with the Organization. The identity of an Individual who is affiliated with an Organization is confirmed as explained in Section 3.2.3. For those cases where there are several Individuals acting in 1 capacity, a Certificate may be issued in the Organization's name. In these cases, such an Organizational Certificate may only be issued after the Issuing CA has performed Identity Proofing of the Affiliated Individual who will be initially responsible for the Organizational Certificate. Thereafter, the Organization is responsible and assumes liability related to maintaining a list of Individuals authorized to use the Organization's Certificate(s). The name of the person to whom the Organization's Token is issued will be retained by the Issuing CA and RA, and the Organization is responsible for ensuring control of these Certificates and their associated Private Keys and accounting for who had control of the Keys and when. In cases where the affiliation between the Organization and the responsible

Affiliated Individual is discontinued, the Organization shall replace him or her with a new responsible Affiliated Individual through a request to the RA or CA. The new responsible Affiliated Individual will undergo the same Identity Proofing process as explained above.

Where Remote Identity Proofing is allowed, the authorized Individual conducting the Remote Identity Proofing session must adhere to all processing requirements as defined in Section 3.2.3 of the TrustID CPS, "Authentication of Individual Identity".

3.2.3.1 Acceptable Forms of Identification Documents

All Individuals seeking the Issuance of a TrustID Certificate who participate in an in-person or via Remote Identity Proofing event must present satisfactory proof of identity.

1. The following are considered by this Policy to be acceptable "Government-issued photo IDs" for in-person or Remote Identity Proofing (all photo IDs must be currently valid (i.e., unexpired) at the time of presentment by the Applicant during the in-person or Remote Identity Proofing event):

    - 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
    - another currently-valid photo ID issued by a governmental agency

2. The following are considered by this Policy 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 the 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

3.2.3.2 In-Person Identification

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

- a CA or a CA's Trusted Agent;
- an RA or an RA's Trusted Agent (i.e., a Local Registration Agent);
- an authorized representative of an Affiliated Individual's Sponsoring Organization;

- a licensed notary, or
- a person or entity certified by a governmental agency as being authorized to confirm identities (e.g., a driver's license bureau, a county clerk, etc.)
- Enterprise RA

All information submitted by the Applicant for in-person or Remote Identity Proofing must be reviewed and cross-checked to determine that it is:

- Internally consistent and
- Consistent with the information contained in the application for the Certificate.

Identity established in this manner shall be communicated to the CA by signed communication (in writing or digitally) indicating that the Applicant was properly identified.

Documentation that in-person or Remote Identity Proofing was performed may be submitted electronically in accordance with the next section: Attestation by an Employer or Other Person.

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 this CP and the TrustID 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 and in accordance with the practices defined in Section 3.2.3.2 of the TrustID CPS, "In-Person Identification".

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, 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.

3.2.3.3.1 Disclosure of Verification Sources

For Organization-Validated and Sponsor-Validated Certificates the CA or RA shall verify the unique organization identifier used in the Certificate from a register that is maintained or authorized by the relevant government agency. The CA shall disclose the authorized sources it uses to verify the Applicant's creation, existence, or recognition. This disclosure shall be through an appropriate and readily accessible online means. The CA shall document where to obtain this information within Section 3.2.3.3.1 of the TrustID CPS.

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

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

3.2.3.4 Electronic Identification

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

To meet the requirements for completing the identity-proofing algorithm, an Applicant must provide at least one form of antecedent in-person based information identification plus two or more of non-antecedent pieces of information.

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

If the RA has previously established the identity of an Individual, and 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 CP.

3.2.3.7 Authentication of Subscribers for Group Certificates

Group Certificates are currently not issued under this CP.

3.2.3.8 Code Signing, EV Code Signing and Time-Stamping Certificates

A TrustID Code Signing or EV Code Signing Certificate or TrustID Time-Stamping Certificate shall identify 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 Code Signing, EV Code Signing, or TrustID Time-Stamping Certificates, the CA shall conform with the provisions of the current version of the CS BR. In the event of any conflict between the provisions of this CP and the provisions of the above referenced document, then the provisions of the above referenced document, as applicable, shall govern. A TrustID Code Signing, EV Code Signing, 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

A Secure Email Certificate is issued to an Applicant upon successful demonstration of the Applicant's control over the Email Address included in the Certificate at the time of email verification. The control of the Applicant's provided Email Address is demonstrated through an automated process, per Section 3.2.8.

The 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.

Identity confirmation of the End Entity in control of the Email Address is not required.

3.2.3.10 TrustID Card Authentication Certificate

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

The Issuing CA shall not include unverified Subscriber information in the Certificate

3.2.5 Validation of Authority

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

3.2.6 Criteria for Interoperation

A CA shall adhere to the following requirements:

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

- Disclose all Cross-Certified Subordinate CA Certificates that identify the CA as the Subject, provided that it has arranged for or accepted the establishment of the trust relationship (i.e. the Cross-Certified Subordinate CA Certificate at issue).

3.2.6.1 Cross-Certification

The PMA may approve cross-certification between an Issuing CA and other Certification Authorities. Issuing CAs must inform End Entities of the uses allowed within the cross-certified PKI. Any cross-certification to external Organizations will only be done after approval by the PMA or its designee.

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., manual review after receipt of a database printout by mail). Registration information provided by the Applicant must include at least his or her name, address, telephone number, Email Address, and the serial numbers of two acceptable forms of ID, one of which shall be a government-issued photo ID. The “trusted information” used for comparison may consist of either (i) a database of user-supplied information previously compiled and maintained by the CA or RA based on an antecedent identification of and continuing relationship with the user; or (ii) information provided through third party vendors of such information

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

- Delivery of a Shared Secret to a confirmed and trusted data point (e.g., street address, telephone number, or Email Address)
- Delivery in-person of a Shared Secret upon presentment of at least two acceptable forms of ID in accordance with Sections 3.2.3.1 and Section 3.2.3.2.
- 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
- Presentment by the Applicant 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
- Another equivalent process.

3.2.8 Validation of Email Address Authorization or Control

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.

For Electronic validation, the CA shall verify that Applicant controls the email accounts associated with S/MIME certificates and that Email address fields referenced in the Certificate have been authorized by the email account holder to act on the account holder’s behalf using the method described in section 3.2.8.1.1 of the TrustID CPS

The CA shall not delegate the verification of mailbox authorization or control.

The CA’s CPS shall specify the procedures that the CA employs to perform this verification. The CA shall maintain a record of which validation method, including the relevant version number from the TLS BR or S/MIME BR, was used to validate every domain or Email Address in issued Certificates.

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation shall have been initiated within the time period specified in Section 4.2.1 prior to Certificate issuance.

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 is to be placed into the system for documentation purposes.

3.2.10 Reliability of Verification Sources

Before relying on a source of verification data to validate Certificate Requests, the CA shall verify its suitability as a Reliable Data Source. Enterprise RA records are a Reliable Data Source for Individual Subject attributes included in Sponsor-Validated Certificates issued to the Enterprise RA's Organization.

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

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

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 been revoked, the End Entity may, within 3 months before the end of the TrustID Certificate's Validity Period, request Issuance of a new TrustID Certificate with a new Key Pair. Such a request must be made to the Issuing CA or RA that originally issued or authorized the TrustID Certificate, and may be made electronically via a Digitally Signed message based on the old Key Pair in the original TrustID Certificate.

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

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

Updating a TrustID Certificate means creating a new TrustID Certificate that:

- Has the same or a different Public Key
- Has a different serial number and
- Differs in one or more other fields from the old Certificate.

For example, the Issuing CA may choose to update a TrustID Certificate of a Subscriber who gains authorization. The old Certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

3.3.2 Identification and Authentication for Re-Key After Revocation

Revoked or expired TrustID Certificates may not be re-keyed, renewed, or updated. Applicants with revoked or expired TrustID Certificates will, upon reapplication, be subject to the same Identity Proofing procedures as first-time Applicants.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

An End Entity may request Revocation or suspension of his, her, or its TrustID Certificate at any time for any reason. The Issuing CA, when faced with such a request, must adopt authentication mechanisms that balance the need to prevent unauthorized requests against the need to quickly revoke or suspend TrustID Certificates. Therefore, in the event the request is electronically submitted, the identity of the requestor may be authenticated based on the Digital Signature used to submit the message. If the request is signed using the Private Key corresponding to the requestor's Public Key, such a request will always be accepted as valid.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

This CP is not intended to impose implementation requirements on the Issuing CA or End Entities. However, this CP does identify the required information and procedures that constitute assurance and support trust in the CA PKI. To this end, the Policy endorses the following procedures for satisfying the security requirements of this PKI. The following steps are required when applying for a TrustID Certificate: (i) submission of a Certificate Request; (ii) sign a Subscriber Agreement and/or Terms of Use; (iii) establish the identity of Subject (per Section 3); (iv) obtain a Key Pair for each TrustID Certificate required; (v) prove to the Issuing CA that the Public Key forms a functioning Key Pair with the Private Key held by the End Entity; and (vi) provide a point of contact for verification of any roles or authorizations requested.

The Certificate Request and Subscriber Agreement or Terms of Use shall be in a form prescribed by the CA and shall comply with the BR including Section 9.6.3. The CA should obtain any additional documentation the CA determines necessary to fulfill these Requirements.

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

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

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

4.1.1 Who Can Submit a Certificate Application

The Issuing CA shall maintain access to all previously revoked Certificates and Certificate applications, whether approved or rejected, based on the record archival procedure described in Section 5.5.2; and the Issuing CA shall use this information to identify subsequent suspicious Certificate requests.

The Certificate application process may be initiated by Individuals (Personal) or by Organizations (Business).

4.1.1.1 Personal Certificates

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

4.1.1.2 Business Certificates, Organization Certificates

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

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

- An Individual who is already a Subscriber, or who can fulfill the same requirements of a Subscriber though it does not obtain a human Certificate, and when appropriate, 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 EV TLS BR
- Likewise, checks and verifications will be made for EV Code Signing Certificate applications based on the requirements within the CS BR

4.1.1.4 FATCA Organization Certificates

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

4.1.1.5 RA Systems Certificates

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

4.1.2 Enrollment Process and Responsibilities

The Issuing CA shall design an enrollment process that facilitates the submission of registration information from the Applicant/PKI Sponsor to the Issuing CA.

A Sponsoring Organization may enter into an agreement with the Issuing CA 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 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.

4.2 CERTIFICATE APPLICATION PROCESSING

For non-Server Certificate or EV Code Signing Certificate applications, Issuing CA's and RA's may appoint Individuals within the Organization to act in the role of an LRA to responsible for approving Certificate applications.

An Applicant/PKI Sponsor for a TrustID Certificate must complete a TrustID Certificate application and provide the requested information in a form prescribed by the TrustID CPS and this CP.

Information in the Certificate application must be verified for accuracy before Certificates are issued as specified in Section 3.2.

Issuing CA's and RAs shall include checking of CAA records to process validation of FQDNs in Server Certificate applications. As part of the Issuance process, the Issuing CA must check for a CAA record and follow the processing instructions found on property tags for each dNSName in the subjectAltName extension of the Certificate to be issued, as specified in the RFC 8659. Issuewild property tags shall be ignored unless the request is for a wildcard Certificate.

To prevent resource exhaustion attacks, the Issuing CA shall limit the length of CNAME chains that are accepted and process CNAME chains that contain 8 or fewer CNAME records.

Action taken on CAA records must be logged and when issued, it must be done following the instructions in Section 4.2.3 "Time to Process Certificate Applications".

4.2.1 Performing Identification and Authentication Functions

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

Applicants will complete a Certificate application and provide requested information in a form prescribed by the Issuing CA in accordance with this Policy. An Applicant must also enter into a Subscriber Agreement or Authorized Relying Party Agreement with the Issuing CA. All applications are subject to review, approval, and Acceptance by the Issuing CA or an authorized RA.

The Issuing CA may use the documents and data provided in Section 3.2 to verify Certificate information or may reuse previous validations themselves provided that the data or document used in the prior validation is no more than 39 7 days before issuing the Certificate. For EV Server and EV Code Signing Certificates, the age of all data used to support renewals shall not exceed the period specified in Section 11.14.3 of the EV TLS BR.

The CA may reuse completed validations and/or supporting evidence performed in accordance with Section 3.2 within the following limits:

1. **Validation of Email Address Authorization or Control**: Completed validation of the control of a mail server in accordance with Section 3.2.8 shall be obtained no more than 397 days prior to issuing the Certificate.

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

   Completed validation of control of an Email Address in accordance with Section 3.2.8 shall be obtained no more than 30 days prior to issuing the Certificate.

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

   Validation of authority in accordance with Section 3.2.5 shall be obtained no more than 825 days prior to issuing the Certificate, unless a contract between the CA and the Applicant specifies a different term. For example, the contract may include the perpetual assignment of roles until revoked by the Applicant or CA, or until the contract expires or is terminated.

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

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

4.2.2 Approval or Rejection of Certificate Applications

For non-Server Certificate or EV Code Signing Certificate applications, Issuing CA's and RA's may appoint Individuals within the Organization to act in the role of an LRA to responsible for approving Certificate applications.

The Issuing CA and RAs approve an Applicant/PKI Sponsor Certificate application if the Identity Proofing processes described in Section 3.2 and Section 3.3 are completed successfully.

CA's shall not issue Server Certificates containing Internal Names or Reserved IP Addresses.

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

4.3.1 CA or RA Actions During Certificate Issuance

After all application and approval processes identified in this Policy are completed, the Issuing CA will:

- Issue the requested TrustID Certificate;
- Notify the Applicant of the TrustID Certificate's Issuance;
- Make the TrustID Certificate available to the Applicant for Acceptance; and
- Require at least 2 Individuals with Trusted Roles 1 of whom deliberately issues a direct command in order for the Root CA to perform a Certificate signing operation.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The procedures for notifying the Applicant of the TrustID Certificate's Issuance, and the procedure used to deliver or make the Certificate available to the Applicant must be secure and confidential.

4.4 CERTIFICATE ACCEPTANCE

An End Entity’s Acceptance of its TrustID Certificate will be a pre-condition to the End Entity’s use of such TrustID Certificate. The Issuing CA will define in its agreements with End Entities (or in its CPS, if incorporated by reference to its agreements with End Entities) the procedure that constitutes Acceptance by an End Entity. The process of Issuance, notification, and Acceptance, and the mechanisms used, may depend on factors such as where the Key Pair is generated and how the TrustID Certificate is made available to the End Entity. By Accepting a TrustID Certificate, the End Entity warrants all of the information provided by the End Entity (and by its Sponsoring Organization, where applicable) and included in the TrustID Certificate, and all representations made by the End Entity (and by its Sponsoring Organization, where applicable) as part of the application and Identity Proofing process, are true and not misleading.

4.4.1 Conduct Constituting Certificate Acceptance

Upon Issuance 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 4.4.

4.4.2 Publication of the Certificate by the CA

The Issuing CA’s Certificates shall be published in a publicly available Repository.

4.4.3 Notification to Subscriber of Certificate Issuance by the CA to Other Entities

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

4.5 KEY PAIR AND CERTIFICATE USAGE

TrustID Certificates may not be used for purposes counter to the principles and applications outlined in this Policy.

4.5.1 Subscriber Private Key and Certificate Usage

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

- Provide complete and accurate responses to all requests for information made by the Issuing CA (or a Trusted Agent or RA) during the Applicant/PKI Sponsor registration, Certificate application, and Identity Proofing processes;
- Generate a Key Pair using a reasonably Trustworthy System, and take reasonable precautions to prevent any compromise, modification, loss, disclosure, or unauthorized use of the Private Key;
- Upon Issuance of a TrustID Certificate naming the Applicant/PKI Sponsor as the Subscriber reviews the TrustID Certificate to ensure that all Subscriber information included in it is accurate, and to expressly indicate Acceptance or rejection of the TrustID Certificate;
- Promises to protect a Private Keys at all times, in accordance with the applicable Subscriber Agreement, this CP, the TrustID CPS, and any other obligations that the Subscriber may otherwise have;
- Uses the TrustID Certificate and the corresponding Private Key exclusively for purposes authorized by this CP and only in a manner consistent with the TrustID CPS;
- Instructs the Issuing CA (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 another 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 the Issuing CA or its authorized agents.

Subscribers who receive Certificates from the Issuing CA shall assert that they will comply with the requirements of this CP as well as those in the TrustID CPS by either signing the Subscriber Agreement online or in paper copy; or, by undergoing a full registration process before receiving the Certificate. Additional information concerning the rights and obligations of Subscribers can be found in Section 9.6.1.2.

See Key Usage Purpose.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to Accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for each application and is not controlled by this CP or by the TrustID 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 this CP or the TrustID CPS should preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the Digital Signatures on that data for as long as it may be necessary to verify the signature on that data.

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstance for Certificate Renewal

Renewing a TrustID Certificate means creating a new TrustID Certificate with the same name, Public Key, and authorization as the old one, but a new, extended Validity Period and a new serial number. 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, the Issuing CA may choose to implement a three-year re-key period with an initial issue and two annual renewals before re-key is required. The old Certificate need not be revoked, but must not be further re-keyed, renewed, or updated.

4.6.2 Who May Request Renewal

Only the End Entity may request Certificate renewal.

4.6.2.1 Treatment of a Request for Certification of a New Key

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

4.6.3 Processing Certificate Renewal Requests

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

4.6.4 Notification of New Certificate Issuance to Subscriber

The notification procedures used by the Issuing CA or RA should be 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 4.4.

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 to be 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.

4.7.1 Circumstance for Certificate Re-Key

The Issuing CA shall allow the Re-key of a TrustID Certificate if such Certificate has not been revoked, suspended, or expired (i.e., Certificate is valid).

4.7.2 Who May Request Certification of a New Public Key

The original Subscribers are also entitled to request its Re-key.

4.7.3 Processing Certificate Re-Keying Requests

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

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

4.7.4 Notification of New Certificate Issuance to Subscriber

The procedures for notifying the Applicant of the TrustID Certificate's Issuance, and the procedure used to deliver or make the Certificate available to the Applicant must be secure and confidential.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Upon Issuance 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 4.4.

4.7.6 Publication of the Re-Keyed Certificate by the CA

The Issuing CA’s Certificates shall be published in a publicly available Repository.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstance for Certificate Modification

The Issuing CA may allow for Certificate modification for any of the following changes during the Certificate's Operational Period:

- Legal name due to marriage, divorce, or court petition
- Organizational affiliation
- Location information
- Email Address or
- Any attribute/extension of a Certificate.

4.8.2 Who May Request Certificate Modification

Subscribers with Valid Certificates are entitled to request email modification and replacements. See Section 3 and Section 4.11 for specific details.

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, the Issuing CA shall replace the Certificate and record all of the Certificate replacement transaction data.

4.8.4 Notification of New Certificate Issuance to Subscriber

Upon successful completion of the Subscriber Identity Proofing process explained in Section 3.2.3, and before Certificate Issuance explained in Section 4.3.1; the Issuing CA, Enterprise RA or the RA notify the Applicant/PKI Sponsor about the approval of the Certificate.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

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. The Issuing CA shall require the Subscriber to review the Certificate and affirmatively communicate Acceptance of its content at the end of the retrieval process. The Issuing CA shall record the act of the Acceptance of the TrustID Certificate in accordance with Section 4.4.

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.

4.8.6 Publication of the Modified Certificate by the CA

Issuing CA's TrustID Certificates shall be published in the Repository upon Issuance. The Repository shall be publicly available.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Server Certificate

The Issuing CA shall revoke a Subscriber Server Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the Issuing CA revoke the Certificate;
2. The Subscriber notifies the Issuing CA that the original Certificate request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
4. The Issuing CA 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);
5. The Issuing CA 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.

The Issuing CA should revoke a Server Certificate within 24 hours and must revoke a Server Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements in the relevant section of the CA/B Forum BR;
2. The Issuing CA obtains evidence that the Certificate was misused;
3. The Issuing CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. The Issuing CA is made aware of any circumstance indicating that use of a FQDN or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
5. The Issuing CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
6. The Issuing CA is made aware of a material change in the information contained in the Certificate;
7. The Issuing CA is made aware that the Certificate was not issued in accordance with the CA/B Forum BR or Issuing CA's CP or CPS;
8. The Issuing CA determines or is made aware that any of the information appearing in the Certificate is inaccurate;
9. The Issuing CA's right to issue Certificates under the CA/B Forum BR expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement; or
11. The Issuing CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

4.9.1.2 Reasons for Revoking a Subordinate CA

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

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

4.9.1.3 Reasons for Revocation Non-Server Certificates

Before revoking a non-server Certificate, the Issuing CA must verify the identity and authority of the entity requesting Revocation and shall proceed with the Revocation within 24 hours if 1 or more of the following events take place:

1. The Subscriber or Applicant with whom a Certificate application is affiliated requests written Revocation for any reason;
2. The Applicant of an approved Secure Email Certificate notifies the Issuing CA that the Domain Name Email Address associated with the Individual holding the Certificate is no longer affiliated with the Organization.
3. The Subscriber notifies the Issuing CA that the original Certificate request was not authorized and does not retroactively grant authorization;
4. The Issuing CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate has been compromised or is suspected of compromise;
5. The Issuing CA obtains reasonable evidence that the Certificate has been used for a purpose outside of that indicated in the Certificate or in the Issuing CA Subscriber Agreement;
6. The Issuing CA receives notice or otherwise becomes aware that a Subscriber has violated 1 or more of its material obligations under the Issuing CA Subscriber Agreement;
7. The Issuing CA receives notice or otherwise becomes aware of any circumstance indicating that use of the Email Address in the Certificate is no longer legally permitted;
8. The Issuing CA receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
9. A determination that the Certificate was not issued in accordance with IdenTrust's Certificate Policy or Certification Practice Statement;
10. IdenTrust determines that any of the information appearing in the Certificate is not accurate;
11. 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;
12. IdenTrust CA private key used in issuing the Certificate is suspected to have been compromised;
13. The Certificate was issued in violation of the then-current version of the browser's root store program requirements.
14. A Sponsoring Organization may request the Issuing CA Revocation of a TrustID Certificate issued to its Affiliated Individual or a Device at any time for any reason;
15. The Issuing CA shall revoke any Certificate deemed out of compliance;
16. For EV Code Signing Certificates, the Certificate has been used to sign, publish or distribute malware, downloaded without user consent or other malicious purpose; or
17. For Certificates used to sign Adobe documents, Adobe has requested Revocation.

4.9.1.4 Revocation Based on an Application Software Supplier Request

If an Application Software Supplier requests IdenTrust to revoke a Code Signing or EV Code Signing Certificate because the Application Software Supplier believes that a Certificate attribute is deceptive, or that the Certificate is being used for malware, bundle ware, unwanted software, or some other illicit purpose, then the Application Software Supplier may request that IdenTrust revoke the Certificate.

Within two (2) business days of receipt of the request, IdenTrust must either revoke the Certificate or inform the Application Software Supplier that it is conducting an investigation.

If IdenTrust decides to conduct an investigation, it must inform the Application Software Supplier whether or not it will revoke the Certificate, within two (2) business days. If IdenTrust decides that the revocation will have an unreasonable impact on its customer, then IdenTrust must propose an alternative course of action to the Application Software Supplier based on its investigation.

4.9.2 Who Can Request Revocation

Different parties may request Certificate Revocation as follows:

- The Issuing CA may summarily revoke Certificates within its domain.
- An RA can request the Revocation of an End Entity's TrustID Certificate on behalf of the End Entity, the Sponsoring Organization, or other authorized party, or its behalf.
- An End Entity is authorized to request the Revocation of his, her, or its Certificate, as is a Subscriber's Sponsoring Organization.
- Additionally, Subscribers, Authorized Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the Issuing CA of reasonable cause to revoke the Certificate. Other third parties may submit Certificate Problem Reports informing the Issuing CA of reasonable cause to revoke the Certificate. See Section 1.5.2.

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

4.9.3 Procedure for Revocation Request

As described in this Policy, a Certificate Revocation request should be promptly communicated to the Issuing CA, either directly or through the RA authorized to Accept such notices on behalf of the Issuing CA.

A Certificate Revocation request may be communicated electronically if it is Digitally Signed with the Private Key of the End Entity (or of the Sponsoring Organization, where applicable). Alternatively, the End Entity (or Sponsoring Organization, where applicable) may request Revocation by contacting the Issuing CA or its RA in person and providing adequate proof of identification in accordance with this Policy or an equivalent method.

When revocation takes place for SSL/TLS Certificates, the Issuing CA must include the relevant revocation reason code "CRLReason" based on the RFC 5280 for the end entity SSL/TLS Certificate.

Refer to Section 4.10.2.1 "Certificate Problem Reporting" of the TrustID CPS for details on submitting revocation request or reporting Certificate issues to IdenTrust.

4.9.4 Revocation Request Grace Period

There is no Revocation grace period. In the case of Key compromise, Subscribers are required to request Revocation within one hour. For all other reasons, Subscribers are required to request Revocation within 24 hours.

4.9.5 Time within Which CA Must Process the Revocation Request

The Issuing CA shall revoke a TrustID Certificate as quickly as practical after receipt of a proper Revocation request and confirmation of the authority of the person requesting Revocation. The Issuing CA may suspend a TrustID non-Server Certificate before deciding whether to revoke it. Promptly following the Revocation of a TrustID Certificate, the Issuing CA shall update the online Certificate database and/or CRL, as applicable. All Revocation requests and the resulting actions taken by the Issuing CA will be archived.

Revocations of Certificates shall occur on the following schedule:

- For End Entities:
    - No more than 24 hours after verification of receipt of a request from the End Entity; if the Certificate is shown to be compromised; or if the FQDN or IP Address should not be relied upon.

- No more than 5 days upon evidence of Certificate misuse; evidence of material change in the Certificate's information; or for Server Certificates, under other circumstances specified in the applicable CA/B Forum BR section.

- For Subordinate CA Certificates:

No more than 7 days following verification of a Subordinate CA request for Revocation; following receipt of evidence of Certificate misuse; if the information contained in the Certificate has changed; or if the Subordinate Certificate can issue Server Certificates, under other circumstances specified in the applicable CA/B Forum BR For Subscriber Server Certificates, Revocation shall not exceed 24 hours, 5 or 7 days based on the circumstances prompting the Revocation request as described in the applicable CA/B Forum BR section.

4.9.6 Revocation Checking Requirement for Relying Parties

The use of revoked TrustID Certificates could have damaging or catastrophic consequences in certain applications. Therefore, before relying on a TrustID Certificate an Authorized Relying Party must conduct a validation request in accordance with the method and procedures established by the Issuing CA pursuant to Section 4.10. If it is temporarily infeasible to obtain Revocation information, then the Authorized Relying Party must either reject use of the TrustID Certificate, or make an informed decision to Accept the risk, responsibility, and consequences of using a TrustID Certificate whose authenticity cannot be guaranteed to the standards of this Policy.

4.9.7 CRL Issuance Frequency

4.9.7.1 Subscriber Certificates:

For the status of Subscriber Certificates, the CA shall update and reissue CRLs at least once 7 days, and the value of the nextUpdate field must not be more than 10 days beyond the value of the thisUpdate field.

4.9.7.2 CA Certificates:

For the status of Subordinate CA Certificates, the CA shall update and reissue CRLs at least:

i. once every 12 months; and
ii. within 24 hours after revoking a Subordinate CA Certificate.

The value of the nextUpdate field must not be more than 12 months beyond the value of the thisUpdate field. 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

Authorized Relying Parties who rely on a CRL must:

- Check for an interim CRL before relying on a TrustID Certificate and
- Log their validation requests.

Failure to do so negates the ability of the Authorized Relying Party to claim that it acted on the TrustID Certificate with Reasonable Reliance. Interim CRLs will only be made available to Authorized Relying Parties.

4.9.9 Online Revocation/Status Checking Availability

When an Issuing CA provides an online Certificate status database as a method of verifying the validity and status of Certificates, the Issuing CA will validate online, near-real-time the status of the Certificate indicated in a Certificate validation request message.

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

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

In the latter case, the OCSP signing Certificate shall contain the ocspSigning EKU (1.3.6.1.5.5.7.3.9) and an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.

4.9.10 Online Revocation Checking Requirements

OCSP responders operated by the CA shall support the HTTP GET method, as described in RFC 6960 and/or RFC 5019.

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

For the status of Subscriber Certificates:

1. OCSP responses shall have a validity interval greater than or equal to 8 hours;
2. OCSP responses shall have a validity interval less than or equal to 10 days;
3. For OCSP responses with validity intervals less than 16 hours, then the CA shall update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate; and
4. For OCSP responses with validity intervals greater than or equal to sixteen hours, then the CA shall 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, the CA shall update information provided via OCSP:

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

If the OCSP responder receives a request for the status of a Certificate serial number that is “unused”, then the responder should not respond with a “good” status. If the OCSP responder is for a CA that is not Technically Constrained in line with Section 7.1.5, the responder shall not respond with a “good” status for such requests. The CA SHOULD monitor the OCSP responder for requests for “unused” serial numbers as part of its security response procedures.

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

4.9.11 Other Forms of Revocation Advertisements Available

An Issuing CA may also use other methods to publicize revoked TrustID Certificates.

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.

Reports of key compromise to IdenTrust must include proof of key compromise in 1 of the following formats:

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

Practices followed in the case of a CA Private Key compromised are explained in Section 5.7.6 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

The Issuing CA shall allow 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. The risk evaluation is at the discretion of the LRA (for Human Certificates) based on the situation and information available at the time.

Certificate suspension shall not be available for any Server Certificate and the Repository must not include these Certificate types in a suspended state.

4.9.14 Who Can Request Suspension

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

4.9.15 Procedure for Suspension Request

A suspension may be requested at any time for any reason. To effect a suspension, minimal identity validation may be required depending upon the circumstances (source of the request, circumstances for the request, etc.) and when completed, the Issuing CA 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 of the TrustID CPS.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 CERTIFICATE STATUS SERVICES

The Issuing CA shall use OCSP and CRLs to distribute Certificate status information.

4.10.1 Operational Characteristics

Each Issuing CA shall provide one or more secure, trustworthy methods for Authorized Relying Parties to verify the validity and status of TrustID Certificates, which shall include either CRLs and/or an online Certificate status database.

Revocation entries on a CRL or OCSP response must not be removed until after the expiration date of the revoked Certificate, except for Code Signing Certificates and Timestamping Certificates, which shall remain on the CRL for at least 10 years after the expiration of the Certificate.

Where an Issuing CA makes available to Authorized Relying Parties more than one method of verifying the validity and status of TrustID Certificates, it may establish one of the methods as the primary method and may disclaim all warranties and liability to any Authorized Relying Party to the extent the Authorized Relying Party uses the other method(s).

4.10.2 Service Availability

The CA shall operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

The CA shall maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

The CA shall maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

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.

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 unless the Issuing CA provides mechanisms (hardware, software, or procedural) that permit recovery of the Private Key while protecting it from being used to impersonate the End Entity.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

When the Issuing CA supports Key escrow and recovery using Key encapsulation techniques, it shall document the procedure in its CPS.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

The Issuing CA, and all RAs, CMAs, and Repositories, will implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external Cryptographic Modules used in connection with providing CA services. Access to such hardware and software will be limited to those personnel performing in a Trusted Role as described in Section 5.2.1. Access will be controlled through the use of electronic access controls, mechanical combination locksets, or deadbolts. Such access controls must be manually or electronically monitored for unauthorized intrusion at all times.

5.1.1 Site Location and Construction

The site for the Issuing CA's server must satisfy the requirements for a High-Security Zone, including:

- Be manually or electronically monitored for unauthorized intrusion at all times
- Ensure that access to the Issuing CA server is limited to personnel identified on an access list and implement dual access control requirements to the Issuing CA server for such personnel
- Ensure personnel not on the access list are properly escorted and supervised
- Ensure a site access log is maintained and inspected periodically and
- Ensure all removable media and paper containing sensitive clear text information are stored in secure, protective containers.

All RA sites must be located in areas that satisfy the controls required for a Reception Zone. If an RA workstation is used for online entity management with the Issuing CA, the workstation must be located in either:

- A Security Zone or
- An Operations Zone while attended, with all media security protected when unattended.

The Issuing CA must ensure that the operation of the RA's site provides appropriate security protection of the Cryptographic Module, all system software, and Private Keys. For example, the Cryptographic Module and the RA’s Private Key should be stored in a secure container or safe. Where a PIN or password is recorded, it must be stored in a security container accessible only to designated personnel. Employees of RAs must not leave their workstations unattended when the cryptography is in an unlocked state (i.e., when the PIN or password has been entered). A workstation that contains Private Keys on a hard drive must be physically secured or protected with an appropriate access control product. Hardware Cryptographic Modules must be protected physically, which may be done through site protection.

5.1.2 Physical Access

Issuing CA equipment will always be protected from unauthorized access. Authenticating RA equipment will be protected from unauthorized access while the Cryptographic Module is installed and activated. The RA will implement physical access controls to reduce the risk of equipment tampering even when the Cryptographic Module is not installed and activated. These security mechanisms will be commensurate with the level of threat in the RA equipment environment. For example, RA equipment in facilities with controlled access occupied primarily by security personnel will not require an additional layer of controlled access surrounding inactivated RA equipment. RA equipment in less secure environments will require additional protection, such as being located in a room that is kept locked when the RA security or authorized personnel are not present. Removable CA Cryptographic Modules will be inactivated and placed in locked containers sufficient for housing equipment commensurate with the classification, sensitivity, or value level of the information being protected by the Certificates issued. Any Activation Data used to access or enable the Cryptographic Module or Issuing CA equipment will be stored separately. Such information should be memorized and not written down. If such information is written, it must be securely stored in a locked container.

An in-person security check to the facility housing Issuing CA equipment will occur at least once every 24 hours during business working hours. The check should ensure that: (i) the equipment is in a state appropriate to the current mode of operation (e.g., that Cryptographic Modules and removable hard disks are in place when "open", and secured when "closed"); (ii) any security containers are properly secured; (iii) physical security systems (e.g., door locks, vent covers) are functioning properly; and (iv) the area is secured against unauthorized access. A role or person will be made explicitly responsible for making such checks. When a role is responsible, a log identifying the Individual performing such a check will be maintained. A record will be kept that describes the type of checks performed, the time, and the Individual who performed them. If the Issuing CA equipment is located in a continuously attended facility, there will be a security check once per shift. If the facility is not continuously attended, the last person to depart will initial a sign-out sheet that asserts that the facility entrance door is locked and that, where installed, intrusion detection systems are activated. If the facility housing the Issuing CA equipment will be unattended for periods greater than 24 hours, it will be protected by an intrusion detection system. Additionally, a check will be made at least once every 24 hours during business working hours to ensure that all doors to the facility are locked and there have been no attempts at forceful entry.

5.1.3 Power and Air Conditioning

The facility which houses the Issuing CA equipment will be supplied with power and air conditioning sufficient to create a reliable operating environment. In addition, personnel areas within the facility must be supplied with sufficient utilities to satisfy operational, health, and safety needs. The actual quantity and quality of utility service will depend on how the facility operates, e.g., its times of operation (24 hours/7 days or 8 hours/5 days), or whether online Certificate status checking is provided. The Issuing CA equipment will have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. The Revocation mechanisms will be supported by uninterruptible power supplies and sufficient backup power generation.

5.1.4 Water Exposures

This Policy makes no stipulation on prevention of exposure of Issuing CA equipment to water beyond that called for by best business practices. Issuing CA equipment will be installed such that it is not in danger of exposure to water, e.g., on tables or elevated floors. Moisture detectors will be installed in areas susceptible to flooding. CA operators who have sprinklers for fire control will have a contingency plan for recovery should the sprinklers malfunction, or cause water damage outside of the fire area.

5.1.5 Fire Prevention and Protection

This Policy makes no stipulation on prevention of exposure of Issuing CA equipment to fire beyond that called for by best business practices. An automatic fire extinguishing system will be installed in accordance with local code. The Issuing CA will have a contingency plan that accounts for damage by fire.

5.1.6 Media Storage

Media will be stored to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit archives or backup information will be stored in a location separate from the Issuing CA equipment.

5.1.7 Waste Disposal

Normal office waste will be removed or destroyed in accordance with best business practices. Media used to collect or transmit information discussed in Section 9.4 will be destroyed, such that the information is unrecoverable, before disposal.

5.1.8 Offsite Backup

System backups, sufficient to recover from system failure, will be made on a periodic schedule, described in the TrustID CPS. At least 1 backup copy will be stored at an offsite location (separate from the Issuing CA equipment). Only the latest backup must be retained. The backup will be stored at a site with physical and procedural controls commensurate to that of the operational CA system.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A Trusted Role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill Trusted Roles must be careful and above reproach as described in the next section. The functions performed in Trusted Roles form the basis of trust in the entire PKI.

If an authentication control used by a Trusted Role is a username and password, then, where technically feasible, implement the following controls outlined in Section 2 of the NetSec BR.

5.2.2 Number of Persons Required Per Task

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

The Issuing CA must ensure that no single Individual may gain access to End Entity Private Keys stored by the Issuing CA. At a minimum, procedural or operational mechanisms must be in place for Key recovery, such as a Split-Knowledge Technique, to prevent the disclosure of the Encryption Key to an unauthorized Individual. Multi-user control is also required for CA Key generation as outlined in Section 6.2.2. All other duties associated with CA roles may be performed by an Individual operating alone. The Issuing CA must ensure that any verification process it employs provides for oversight of all activities performed by privileged CA role holders.

To best ensure the integrity of the Issuing CA equipment and operation, it is recommended that wherever possible a separate Individual be identified for each Trusted Role. The separation provides a set of checks and balances over the Issuing CA operation. Under no circumstances will the incumbent of a CA role perform his or her own auditor function.

5.2.3 Identification and Authentication for Each Role

All Issuing CA personnel must have their identities and authorization verified before they are:

- Included in the access list for the Issuing CA site;
- Included in the access list for physical access to the Issuing CA system;
- Given a Certificate for the performance of their CA role; or
- Given an account on the PKI system.

Each of these Certificates and accounts (with the exception of CA signing Certificates) must:

- Be directly assigned to an Individual;
- Not be shared; and
- Be restricted to actions authorized for that role through the use of CA software, operating system, and procedural controls.

When accessed across shared networks, CA operations must be secured, using mechanisms such as Token-based strong authentication and encryption.

5.2.4 Roles Requiring Separation of Duties

The Issuing CA shall maintain strict separation-of-duties/multi-party controls for its Trusted Roles.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

Issuing CAs, RAs, CMAs, and Repositories will formulate and follow 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 this Policy.

5.3.2 Background Check Procedures

Issuing CAs will conduct an appropriate investigation of all personnel who serve in Trusted Roles (before their employment and periodically thereafter as necessary), to verify their trustworthiness and competence in accordance with the requirements of this Policy and the Issuing CA's personnel practices or equivalent. All personnel who fail an initial or periodic investigation will not serve or continue to serve in a Trusted Role.

5.3.3 Training Requirements

The Issuing CA must ensure that all personnel performing managerial duties with respect to the operation of the Issuing CA and RAs receive comprehensive training in:

- The Issuing CA/RA security principles and mechanisms –
- Security awareness
- All PKI software versions in use on the Issuing CA system
- All duties they are expected to perform
- Disaster recovery and business continuity procedures.

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

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

The CA shall document that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

The CA shall require all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the CA/B Forum BRs.

5.3.4 Retraining Frequency and Requirements

The requirements of Section 5.3.3 must be kept current to accommodate changes in the Issuing CA system. Refresher training must be conducted as required, and the Issuing CA must review these requirements at least once a year.

5.3.5 Job Rotation Frequency and Sequence

This Policy makes no stipulation regarding the frequency or sequence of job rotation.

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

The Issuing CA must ensure that contractor access to the Issuing CA site is in accordance with Section 5.1.2, Physical Access.

5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role will be provided to the persons acting in that role.

5.4 AUDIT LOGGING PROCEDURES

The Issuing CA shall:

- Implement a security support system under its control to monitor, detect, and reports any security-related configuration change to Certificate systems;
- Identify those Certificate systems under its control capable of monitoring and logging system activity and enable those systems to continuously monitor and log system activity;
- Implement automated mechanisms under its control to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible critical security events;
- Require Trusted Role personnel to follow up on alerts of possible critical security events;
- Conduct 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; and
- Maintain, archive, and retain logs in accordance with disclosed business practices and applicable legislation.

5.4.1 Types of Events Recorded

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

The CA shall record at least the following events:

1. CA certificate and key lifecycle events, including:
    1. Key generation, backup, storage, recovery, archival, and destruction;
    2. Certificate Requests, renewal, and re-key requests, and revocation;
    3. Approval and rejection of certificate requests;
    4. Cryptographic device lifecycle management events;
    5. Generation of Certificate Revocation Lists;
    6. Signing of OCSP Responses (as described in Section 4.10); and
    7. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate lifecycle management events, including:
    1. Certificate requests, renewal, and re-key requests, and revocation;
    2. All verification activities stipulated in these Requirements and the CA's Certification

    3. Practice Statement;
    4. Approval and rejection of certificate requests;
    5. Issuance of Certificates;
    6. Generation of Certificate Revocation Lists; and
    7. Signing of OCSP Responses (as described in Section 4.10).
3. Security events, including:
    1. Successful and unsuccessful PKI system access attempts;
    2. PKI and security system actions performed;
    3. Security profile changes;
    4. Installation, update and removal of software on a Certificate System;
    5. System crashes, hardware failures, and other anomalies;
    6. Firewall and router activities; and
    7. Entries to and exits from the CA facility.

Log records must include the following elements:

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

Description of the event.

5.4.2 Frequency of Processing Log

The Issuing CA must ensure that its audit logs are reviewed by CA personnel at least weekly and all significant events are explained in an audit log summary. 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. Supporting manual and electronic logs from the Issuing CA and RA should be compared where any action is deemed suspicious. Actions taken following these reviews must be documented.

5.4.3 Retention Period for Audit Log

The CA shall retain, for at least 2 years:

1. CA certificate and key lifecycle management event records as set forth in Section 5.4.1(1) after the later occurrence of:
    a. the destruction of the CA Private Key; or
    b. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records as set forth in Section 5.4.1 (2) after the expiration of the Subscriber Certificate;
3. Any security event records as set forth in Section 5.4.11(3) after the event occurred.

The information generated on the Issuing CA equipment will be kept on the Issuing CA equipment until the information is moved to an appropriate archive facility. Deletion of the audit log from the Issuing CA equipment will be performed by a person other than the CA Operator. This person will be identified in the Issuing CA's CPS. Audit logs will be retained as archive records in accordance with Section 5.5.2.

5.4.4 Protection of Audit Log

The audit log, to the extent possible, will not be open for reading or modification by any human, or by any automated process other than those that perform audit processing. Any entity that does not have modification access to the audit log may archive it (note that deletion requires modification access). Weekly audit data will be moved to a safe, secure storage location separate from the Issuing CA equipment.

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (Internal vs. External)

There is no requirement for the audit log collection system to be external to the Issuing CA equipment. The audit process will run independently and will not in any way be under the control of the CA Operator. Audit processes will be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, the Issuing CA operation will cease until the audit capability can be restored. If it is unacceptable to cease CA operation, other means will be employed to provide audit capability that has been previously arranged with the Issuing CA's auditor.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system no notice need be given to the Individual, Organization, device or application that caused the event.

5.4.8 Vulnerability Assessments

The Issuing CA shall:

- Implement intrusion detection and prevention controls under the control of CA to protect Certificate Systems against common network and system threats;
- Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities;
- Undergo or perform a Vulnerability Scan (i) within one week of receiving a request from the CA/Browser Forum, (ii) after any system or network changes that the CA determines are significant, and (iii) at least every three months, on public and private IP Addresses identified by the CA Certificate systems;
- Undergo 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;
- Record evidence that each Vulnerability Scan and Penetration Test was performed by an Individual 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; and
- Do one of the following within 96 hours of the discovery of a Critical Vulnerability not previously addressed by the CA’s vulnerability correction process:
    - Remediate the Critical Vulnerability;
    - If remediation of the Critical Vulnerability within ninety-six (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.

Events in the audit process are logged, in part, to monitor system vulnerabilities. The Issuing CA must ensure that a vulnerability assessment is performed, reviewed, and revised following an examination of these monitored events.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

The CA shall archive all audit logs (as set forth in Section 5.4.1).

Additionally, shall archive:

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

5.5.2 Retention Period for Archive

The CA and the Time-Stamping Authority must archive records for a period of at least 7 years, 6 months without any loss of data; less or greater retention archival period is permitted for external RAs and PKI Service Providers based on contractual requirements and the requirements of the current version of the TLS BR.

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

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

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

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

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for Time-Stamping of Records

CA archive records shall be automatically time-stamped as they are created. The TrustID CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System (Internal or External)

The applicable CPS or RPS shall describe the archive collection system.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures to obtain and verify archive information and procedures detailing how to create, package, and send the archive information will be published in the Issuing CA procedures handbook or CPS. Only authorized users will be allowed to access the archive. During any inspections required by this Policy, the Compliance Inspector will verify the integrity of the archives.

5.6 KEY CHANGEOVER

An End Entity may only apply to renew his, her, or its TrustID Certificate within three months before the expiration of one of the Keys, provided the previous Certificate has not been revoked. An End Entity, the Issuing CA, or the RA may initiate this Key changeover process. Automated Key changeover is permitted. The Issuing CA must ensure that the details of this process are indicated in its CPS or another publicly available document. End Entities without valid Keys must be re-authenticated by the Issuing CA or RA in the same manner as the initial registration. Where an End Entity's TrustID Certificate has been revoked as a result of non-compliance, the Issuing CA must verify that any reasons for non-compliance have been addressed to its satisfaction before Certificate re-issuance. Keys may not be renewed using an expired Key.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

CA operators shall have an Incident Response Plan and a Disaster Recovery Plan.

The CA shall make its business continuity plan and security plans available to the CA's auditors upon request. The CA shall annually test, review, and update these procedures.

The business continuity plan shall include:

1. The conditions for activating the plan;
2. Emergency procedures;
3. Fallback procedures;
4. Resumption procedures;
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans;
10. The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes;
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time;
13. How frequently backup copies of essential business information and software are taken;
14. The distance of recovery facilities to the CA's main site; and

15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

The Issuing CA shall document and maintain security incident response and compromise handling policies and procedures, as well as disaster recovery and business continuity plans. Such procedures and plans are to be made available for onsite review by its auditors and major Authorized Relying Parties under appropriate non-disclosure agreements.

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

The Issuing CA must have in place an appropriate disaster recovery and business resumption plan. The plan must set up and render operational a facility located in a geographically diverse area that is capable of providing CA services in accordance with this Policy within 48 hours of an unanticipated emergency. Such plan will include a complete and periodic test of readiness for such facility. Such plan will be referenced within the CPS or other appropriate documentation and available to Authorized Relying Parties for inspection.

5.7.3 Entity (CA) Private Key Compromise Procedures

In the event of the compromise, or suspected compromise, of the Issuing CA's CA Private Signing Key, the Issuing CA must immediately notify all CAs with whom it has cross-certified. In the event of the compromise, or suspected compromise, of any other Participant's signing Key, the Participant must notify the Issuing CA immediately. The Issuing CA must ensure that its CPS or a publicly available document and appropriate agreements contain provisions outlining the means it will use to provide notice of compromise or suspected compromise.

In the event of the compromise of an Issuing CA's CA Private Signing Key, the Issuing CA must revoke all Certificates issued using that Key and provide appropriate notice. See Entity Private Key Compromise Procedures. After addressing the factors that led to the Private Key compromise, the Issuing CA may: (i) generate a new CA Signing Key Pair; (ii) re-issue Certificates to all End Entities and ensure all CRLs and ARLs are signed using the new Key.

5.7.4 Business Continuity Capabilities After a Disaster

The Issuing CA must establish a disaster recovery plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. Where a Repository is not under the control of the Issuing CA, the Issuing CA must ensure that any Agreement with the Repository provides that a disaster recovery plan be established and documented by the Repository.

5.7.5 Customer Service Center

As described in this Policy, the Issuing CA will implement and maintain a Customer Service Center to provide assistance and services to Subscribers and Authorized Relying Parties, and a system for receiving, recording, responding to, and reporting problems within the Issuing CA's organization and for reporting such problems to the PMA.

5.7.6 Entity Public Key is Revoked

In the event of the need for Revocation of an Issuing CA's CA Certificate, the Issuing CA must immediately notify:

- The PMA
- All CAs to whom it has issued cross-Certificates
- All of its RAs
- All Subscribers and
- All Individuals or Organizations who are responsible for a Certificate are used to an Electronic Device.

The Issuing CA must also:

- Publish the CA Certificate serial number on an appropriate CRL and
- Revoke all cross-Certificates signed with the revoked CA Certificate.

After addressing the factors that led to Revocation, the Issuing CA 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, see Certificate Revocation and Suspension.

5.8 CA OR RA TERMINATION

In the event that the Issuing CA ceases operation, all Subscribers, Sponsoring Organizations, RAs, CMAs, Repositories, and Authorized Relying Parties will be promptly notified of the termination. In addition, all CAs with which cross-certification agreements are current at the time of cessation will be promptly informed of the termination. All TrustID Certificates issued by the Issuing CA that reference this Policy 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 designate) within 24 hours of Issuing CA cessation and in accordance with this Policy. Transferred data will not include any data unrelated to this Policy. No Key recovery enabled Repository data will be co-mingled with this data.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

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

6.1.1.1 CA Key Pair Generation

For CA Key Pairs that are either

1. used as a CA Key Pair for a Root CA Certificate; or
2. used as a CA Key Pair for a Subordinate CA Certificate, where the Subordinate CA is not the operator of the Root CA or an Affiliate of the Root CA,

The CA shall:

1. prepare and follow a Key Generation Script;
2. have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process; and
3. have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

For other CA Key Pairs that are for the operator of the Root CA or an Affiliate of the Root CA, the CA SHOULD:

1. prepare and follow a Key Generation Script; and
2. either (i) have a Qualified Auditor witness the CA Key Pair generation process, or (ii) video-record the entire CA Key Pair generation process for review by its Qualified Auditor.

In all cases, the CA shall:

1. generate the CA Key Pair in a physically secured environment as described in the CA’s CP and/or CPS;
2. generate the CA Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge;
3. generate the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA’s CP and/or CPS;
4. log its CA Key Pair generation activities; and
5. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its CP and/or CPS and (if applicable) its Key Generation Script.

6.1.1.2 RA Key Pair Generation

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

6.1.1.3 Subscriber Key Pair Generation

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

Subscriber signature Private Keys shall not be generated by the CA.

In those cases where Key Pairs are generated by the CA on behalf of the Subscribers (e.g., Encryption Key Pair), The CA shall implement procedures to ensure that the Cryptographic Module is not activated by an unauthorized entity.

The CA shall reject a Certificate Request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. The CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. The CA has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1;
5. The CA is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

The CA may generate the Private Key on behalf of the Subscriber

6.1.2 Private Key Delivery to Subscriber

If the CA generates the Private Key on behalf of the Subscriber where the Private Keys will be transported to the Subscriber, then the entity generating the Private Key shall either transport the Private Key in hardware with an activation method that is equivalent to 128 bits of encryption or encrypt the Private Key with at least 128 bits of encryption strength. Example methods include using a 128-bit AES key to wrap the Private Key or storing the key in a PKCS 12 file encrypted with a randomly generated password of more than 16 characters containing uppercase letters, lowercase letters, numbers, and symbols for transport. The CA shall not store Subscriber Private Keys in clear text.

The material used to activate/protect the Private Key (e.g., a password used to secure a PKCS 12 file) must be delivered to the Subscriber securely and separately from the container holding the Private Key.

6.1.3 Public Key Delivery to Certificate Issuer

Public Keys must be delivered to the Issuing CA in a secure and trustworthy manner, such as a Certificate request message. Delivery may also be accomplished via non-electronic means. These means may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a Token to the Issuing CA for local Key Generation at the point of Certificate Issuance or request. Off-line means will include identity checking and will not inhibit proof of possession of corresponding Private Key. Any other methods used for Public Key delivery will be stipulated in a CPS or Subscriber Agreement. In those cases where Key Pairs are generated by the Issuing CA on behalf of the End Entity, the Issuing CA will implement secure mechanisms to ensure that the Token on which the Key Pair is held, is securely sent to the proper End Entity and that the Token is not activated before receipt by the proper End Entity.

6.1.4 CA Public Key Delivery to Relying Parties

The Public Key corresponding to the Issuing CA's CA Private Signing Key may be delivered to Relying Parties in an online transaction in accordance with the IETF PKIX Part 3, or other appropriate mechanism.

6.1.5 Key Sizes

For RSA key pairs the CA shall

- Ensure that the modulus size, when encoded, is at least 2048 bits; and
- Ensure that the modulus size, in bits, is evenly divisible by 8.

For ECDSA key pairs, the CA shall:

- Ensure that the key represents a valid point on the NIST P-256, NIST P-384, or NIST P-521 elliptic curve.

For OCSP responder signing requests, the Issuing CA shall respond using SHA-256 or higher hash algorithms.

Effective June 1, 2021, the minimum key size for Code Signing, EV Code Signing, and Time-Stamping Subordinate CAs is 4096 bits RSA and for equivalent End-Entity Certificates, it is a minimum of 3072 bits RSA.

6.1.6 Public Key Parameters Generation and Quality Checking

For RSA key pairs: the CA shall confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent should be in the range between $2^{16}+1$ and $2^{256}-1$. The modulus should also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. (See NIST SP 800-89, Section 5.3.3.)

6.1.7 Key Usage Purposes (As per X.509 v3 Key Usage Field)

Keys may be used for authentication, non-repudiation, and data encryption. They may also be used for session Key establishment. CA Private Signing Keys are the only Keys permitted to be used for signing Certificates and CRLs. The Certificate Key Usage field must be used in accordance with the PKIX-1 Certificate and CRL Profile. 1 of the following Key Usage values must be present in all Certificates: (i) Digital Signature; or (ii) Non-Repudiation. 1 of the following additional values must be present in CA Certificate-signing Certificates: (i) Key Cert Sign; or (ii) CRL Sign. The use of a specific Key is determined by the Key usage extension in the X.509 Certificate. This restriction is not intended to prohibit the use of protocols (like the Secure Sockets Layer) that provide authenticated connections using Key management Certificates.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

The CA shall implement physical and logical safeguards to prevent unauthorized Certificate issuance. Protection of the CA Private Key outside the validated system or device specified above shall consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Key. The CA shall encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part. Cryptographic Module Standards and Controls

The relevant standard for Cryptographic Modules is FIPS140-2; however, the PMA may determine that other comparable validation, certification, or verification standards are sufficient. Cryptographic Modules will be validated to the specific FIPS 140 security level ("Level") identified in this section, or validated, certified, or verified via one of the standards published by the PMA in Appendix A of this CP document.

- End Entities will use Cryptographic Modules that meet at least the criteria specified for Level 1.
- End Entity Certificates with a Policy OID within the arch for hardware (i.e., 2.16.840.1.113839.0.6.12.x; 2.16.840.1.113839.0.14.x), TrustID EV Code Signing, TrustID Time-Stamping and Signing Authority Certificates shall be issued on hardware Cryptographic Modules validated to meet the minimum criteria specified in the FIPS 140-2 Level 2 standards.
- TrustID Card Authentication and TrustID Device Certificates will use Cryptographic Modules that meet at least the criteria specified for Level 1 or equivalent standards or Trusted Platform Module.

- RAs require at least Level 2 hardware Cryptographic Modules.
    - A higher level may be used if available or desired.
    - RAs and Issuing CAs should provide the option of using any acceptable Cryptographic Module, to facilitate the management of Certificates.
- The Issuing CA may use hardware or software Cryptographic Modules for CA Key generation and protection, validated at Level 2. Certificates will be signed using a hardware Cryptographic Module that meets Level 2.

6.2.1 Private Key (n out of m) Multi-Person Control

Multi-person control is a security mechanism that requires multiple authorizations for access to the CA Private Signing Key. For example, access to the CA Private Signing Key should require authorization and validation by multiple parties, including CA personnel and separate security officers. This mechanism prevents a single party (CA or otherwise) from gaining access to the CA Private Signing Key.

CA Private Signing Keys may be backed up only under two-person control. The parties used for two-person control will be maintained on a list that will be made available for inspection by PKI Service Providers.

6.2.2 Private Key Escrow

Private Keys used for encryption and decryption only, and not for Digital Signatures, may be escrowed for Key recovery purposes.

6.2.3 Private Key Backup

A Participant may optionally create a backup of 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 Private Key Archival

If the Issuing CA is acting as a Key Recovery agent, then it will archive Private Key Management Keys as part of its service. Private Keys supporting non-repudiation services will never be archived. A Participant may optionally archive its own Private Key.

Parties other than the Subordinate CA shall not archive the Subordinate CA Private Keys without authorization by the Subordinate CA.

6.2.5 Private Key Transfer Into or From a Cryptographic Module

If the Issuing CA generated the Private Key on behalf of the Subordinate CA, then the Issuing CA shall encrypt the Private Key for transport to the Subordinate CA. If the Issuing CA becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not Affiliated with the Subordinate CA, then the Issuing CA shall revoke all certificates that include the Public Key corresponding to the communicated Private Key.

PKI Service Provider Private Keys are to be generated by and in a Cryptographic Module. In the event that a Private Key is to be transported from 1 Cryptographic Module to another, the Private Key must be encrypted during transport. Private Keys must never exist in clear text form outside the Cryptographic Module boundary.

6.2.6 Private Key Storage on Cryptographic Module

The CA shall protect its Private Key in a system or device that has been validated as meeting at least FIPS 140-2 level 3, FIPS 140-3 level 3, or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats. Method of Activating Private Key

An End Entity must be authenticated to the Cryptographic Module before the activation of the Private Key. This authentication may be in the form of a password. When deactivated, Private Keys must be kept in encrypted form only.

For TrustID Card Authentication and TrustID Device Certificates, activation of the Private Key is accomplished upon installation to the corresponding device or card.

6.2.7 Method of Deactivating Private Key

Cryptographic Modules that have been activated must not be left unattended or otherwise open to unauthorized access. After use, they must be deactivated, using, for example, a manual logout procedure or a passive timeout. When not in use, hardware Cryptographic Modules should be removed and stored, unless they are within the End Entity's sole control.

6.2.8 Method of Destroying Private Key

Private Keys should be destroyed when they are no longer needed, or when the Certificates to which they correspond expire or are revoked. For software Cryptographic Modules, this can be done by overwriting the data. For Tokens, this will likely be accomplished by executing a "zeroize" command. Physical destruction of hardware is not required.

6.2.9 Cryptographic Module Rating

The relevant standard for Cryptographic Modules is FIPS140-2; however, the PMA may determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published by the PMA. Cryptographic Modules will be validated to the specific FIPS 140 security level ("Level") identified in this section, or validated, certified, or verified via 1 of the standards published by the PMA.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The Issuing CA must retain all verification Public Keys.

6.3.2 Certificate Operational Periods

All Certificates and corresponding Keys shall have maximum Validity Periods not to exceed the following:

Table 7 – TrustID Operational Certificate Validity Periods

Key Type	Certificate Lifetime
Root CA	20 years
Subordinate CA	15 years
CSA OCSP Responder	3 years
LRA (Signature)	2 years Plus up to 90 days of validity remaining on a renewing Certificate
LRA (Encryption)	2 years Plus up to 90 days of validity remaining on a renewing Certificate
End Entity Human (S/MIME)	2 years

Key Type	Certificate Lifetime
	Plus up to 90 days of validity remaining on a renewing Certificate
End Entity Server	1 year Plus up to 90 days of validity remaining on a renewing Certificate
Code Signing and EV Code Signing	3 years Plus up to 90 days of validity remaining on a renewing Certificate
Time-Stamping	**End Entity:** 1 Year plus 3 months **Subordinate CA:** 11 years plus 3 months
End Entity FATCA Organization	2 years Plus up to 90 days of validity remaining on a renewing Certificate
End Entity – Other Devices	7 years

Certificates and Keys must not be used after the expiration of the Validity Periods as defined in this section. Exceptions to the Private Key Usage period may be permissible if approved by the PMA and so long as such exceptions do not conflict with documented best practices, including RFC 5280 and CA/B Forum BR.

6.3.3 Restrictions on CA's Private Key Use

The Private Key used by the Issuing CA for issuing Certificates shall be used only for signing such Certificates and, optionally, CRLs or other validation services responses. A Private Key held by an RA, if any, is: (i) considered the Issuing CA's Private Key; (ii) is held by the RA as a fiduciary; and (iii) will not be used by the RA for any other purposes, except those specifically agreed to between the Issuing CA and the RA. Further, any other Private Key used by an RA for purposes associated with its RA functions shall not be used for any other purpose without the express permission of the Issuing CA. The Private Key used by each RA in connection with the Issuance of Certificates 85hall be used only for communications relating to the approval or Revocation of such Certificates.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

A pass-phrase, PIN or other Activation Data shall be used to protect access to the Private Key. The Activation Data may be user-selected. If the Activation Data must be transmitted to the End Entity, it shall be via a channel of appropriate protection, and distinct in time and place from the associated Cryptographic Module. If this is not done by hand, the End Entity should be advised of the date sent, method of sending, and expected delivery date of any Activation Data. As part of the delivery method, End Entities should acknowledge receipt of the Cryptographic Module and Activation Data. In addition, End Entities should also receive (and acknowledge receipt of) information regarding the use and control of the Cryptographic Module. See Cryptographic Module Standards and Controls.

6.4.2 Activation Data Protection

Activation Data 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. Activation Data must never be shared.

6.4.3 Other Aspects of Activation Data

This 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. CAs may define Activation Data requirements in their CPSs or Subscriber Agreements.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

The CA shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

All Issuing CA servers must include the following functionality either provided by the operating system or through a combination of the operating system, PKI application, and physical safeguards: (i) access control to CA services and PKI roles; (ii) enforced separation of duties for PKI roles; (iii) identification and authentication of PKI roles and associated identities; (iv) object re-use or separation for CA random access memory; (v) use of cryptography for session communication and database security; (vi) archival of CA and End-Entity history and audit data; (vii) audit of security related events; (viii) self-test of security related CA services; (ix) trusted path for identification of PKI roles and associated identities; (x) recovery mechanisms for Keys and the Issuing CA system; and (xi) enforcement of domain integrity boundaries for security critical processes.

6.5.2 Computer Security Rating

The Issuing CA's equipment will meet and be operated to at least a C2 [TCSEC] or E2/F-C2 [ITSEC] rating or equivalent. The Issuing CA's equipment operating at a C2 equivalence will, as a minimum, implement: (i) self-protection; (ii) process isolation; (iii) discretionary access control; (iv) object reuse controls; (v) Individual Identity Proofing; and (vi) a protected audit record.

6.6 LIFE CYCLE TECHNICAL CONTROLS

Issuing CA equipment (hardware and software) procured to operate a PKI will be purchased in a fashion to reduce the likelihood that any particular copy was tampered with; for instance, by random selection. Issuing CA equipment developed for a PKI will be developed in a controlled environment and the development process will be defined and documented. Equipment procured before registration as the Issuing CA will be deemed to satisfy this requirement.

Issuing CA equipment will be protectively packaged and delivered via a documented method. Tamper-evident packaging will be used or equipment will be hand-carried from a controlled procurement environment to the installation site. Equipment procured before registration as the Issuing CA will be deemed to satisfy this requirement. The Issuing CA equipment will be dedicated to administering a Key management infrastructure. It will not have installed applications or component software, which are not part of the CA configuration. Equipment updates will be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.1 System Development Controls

The CA must use software that has been designed and developed with the following standards:

- For commercial off-the-shelf software, the software shall be designed and developed under a formal, documented development methodology;
- Where open source software has been utilized, the CA shall demonstrate that security requirements were achieved through software verification and validation, structured development, and lifecycle management.

The design and development process must provide sufficient documentation to support third party security evaluation of the Issuing CA components and be supported by third party verification of process compliance and ongoing assessments to influence security safeguard design and minimize residual risk.

6.6.2 Security Management Controls

A formal configuration management methodology must be used for the installation and ongoing maintenance of the Issuing CA system. The Issuing CA software, when first loaded, must provide a method for the Issuing CA to verify that the software on the system: (i) originated from the software developer; (ii) has not been modified before installation; and (iii) is the version intended for use. The Issuing CA must provide a mechanism to periodically verify the integrity of the software. The Issuing CA must also have mechanisms and policies in place to control and monitor the configuration of the Issuing CA system. Upon installation time, and at least once every 24 hours, the integrity of the Issuing CA system must be validated.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 NETWORK SECURITY CONTROLS

Issuing CA equipment should be connected to no more than 2 network domains at a time. Issuing CA equipment intended to connect to more than 1 network classification domain will have procedures defined in a CPS, or other documents made available to its auditors, that prevent information from 1 domain from reaching another (e.g., equipment shutdown, removable hard drives, switching the network connection). Issuing CA equipment may operate through a network guard insofar as it does not circumvent the function of the guard. Protection of Issuing CA equipment will be provided against known network attacks. Use of appropriate boundary controls will be employed. All unused network ports and services will be turned off. Any network software present on the Issuing CA equipment will be necessary to the functioning of the Issuing CA application. Root Issuing CA equipment will be stand-alone (off-line) configurations.

The CA equipment used for PKI activities shall adhere to the NetSec BR.

6.8 TIME-STAMPING

The Issuing CA's system clock time shall be 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

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

TrustID Certificates shall contain Public Keys used for authenticating the sender of electronic messages and verifying the integrity of such messages – i.e., Public Keys used for Digital Signature verification. TrustID Certificates will be issued in the X.509 version 3 format unless another format is necessary to facilitate secure wireless communications or interoperability with devices using Wireless Application Protocol (WAP) or other technologies. Nothing in this CP would require an Authorized Relying Party to use or process non-standard Certificates. Where applicable, TrustID Certificates will include a reference to the OID for the Certificate type identified by this Policy within the appropriate field. The CPS or other publicly available document will identify the Certificate extensions supported, and the level of support for those extensions.

7.1.1 Version Number(s)

The Issuing CA must issue X.509 Version 3 Certificates, in accordance with the PKIX Certificate and CRL Profile. The PKI End-Entity software must support all the base (non-extension) X.509 fields:

7.1.1.1 Version

The version of X.509 Certificates version 3(2).

7.1.1.2 Serial Number

The unique serial number for Certificate with numbers greater than 0 and containing at least 64 bits of output from a cryptographically secure pseudo-random number generator, as well as the Certificate extensions as defined in that section.

7.1.1.3 Signature

The Issuing CA signature to authenticate Certificate.

7.1.1.4 Issuer

The name of the Issuing CA.

7.1.1.5 Validity Period

The Activation and expiry date for the Certificate.

7.1.1.6 Subject

The End Entity's DN

7.1.1.7 Subject Public Key Information

The End Entity's Public Key.

7.1.2 Certificate Content and Extensions

The TrustID CPS must define the use of any Certificate extensions supported by the Issuing CA, its RAs, and End Entities.

7.1.3 Algorithm Object Identifiers

7.1.3.1 Algorithms and OIDs for Signatures

Algorithm	OID
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-SHA224	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1 }
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha256(2)}
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }
ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }

7.1.3.2 Algorithms and OIDs for Identifying Subject Public Key Information

Algorithm	OID
rSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) public-key-type(2) 1}

Where non-CA Certificates contain an elliptic curve Public Key, the parameters shall be specified as 1 of the following named curves:

Algorithm	OID
Curve P-256 (ansip256r1)	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
Curve P-384 (ansip384r1)	{iso(1) identified-organization(3) certicom(132) curve (0) 34}

7.1.4 Name Forms

Every DN must be in the form of an X.501 PrintableString or UTF8String.

Issuing CAs shall not issue Server Certificates with a Reserved IP Address or Internal Names.

7.1.5 Name Constraints

Subject and Issuer DNs must comply with PKIX standards and be present in all Certificates.

Not fully Technically Constrained Subordinate CA’s must be publicly disclosed 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

The Issuing CA must ensure that the Policy OID is contained within the Certificates it issues.

7.1.7 Usage of Policy Constraints Extension

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

7.1.8 Policy Qualifiers Syntax and Semantics

For Certificates not subject to the CA/B Forum BRs, the Issuing CA may populate the policyQualifiers extension with the URI of its CP. If the Issuing CA populates the userNotice extension, it will contain text substantially similar to the following:

"This TrustID Certificate may only be relied upon by Authorized Relying Parties and only in accordance with the TrustID Certificate Policy found at {Issuing CA's URL Repository pointer}."

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.

7.1.10 Inhibit Any Policy Extension

The Issuing CA may assert InhibitAnyPolicy in CA Certificates. When used, the extension is marked noncritical*, to support legacy applications that cannot process InhibitAnyPolicy.

7.2 CRL PROFILE

If utilized, CRLs will be issued in the X.509 version 2 format. The TrustID CPS or other publicly available document will identify the CRL extensions supported and the level of support for these extensions.

7.2.1 Version Number(s)

The Issuing CA must issue X.509 version two (2) CRLs in accordance with the PKIX Certificate and CRL Profile.

7.2.2 CRL and CRL Entry Extensions

All End Entity PKI software must correctly process all CRL extensions identified in the Certificate and CRL profile. The TrustID CPS or other publicly available document will identify must define the use of any extensions supported by the Issuing CA, its RAs, and End Entities.

7.3 OCSP PROFILE

7.3.1 Version Number(s)

The version number for requests and responses shall be version 1.

7.3.2 OCSP Extensions

The Issuing CA shall require Relying Parties to refer to the local clock to check for response freshness.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The CA shall at all times:

1. Issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates;
2. Comply with the CA/B Forum BR;
3. Comply with the audit requirements set forth in this section; and
4. Be licensed as a CA in each jurisdiction where it operates, if licensing is required by the law of such jurisdiction for the issuance of Certificates.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

An Issuing CA will undergo a review and approval process by the PMA to demonstrate compliance with this Policy. This Policy makes no stipulation as to the exact frequency of compliance inspections, but inspections for re-certification will be required anytime a significant change in Issuing CA operations is made. In any event, the Issuing CA, RAs, and CMAs must certify annually that they have at all times during the period in question complied with the requirements of this Policy. The Issuing CA, RAs, and CMAs must also state any periods of non-compliance with this Policy and provide reasons for non-compliance.

If the CA does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in Section 8.4, then, before issuing Publicly-Trusted Certificates, the CA shall successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in Section 8.4. The point-in-time readiness assessment shall be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates and shall be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.

8.2 IDENTITY /QUALIFICATIONS OF ASSESSOR

Subject to further qualifications identified in Section 8.4, Compliance Inspectors must: (i) have qualifications in accord with commercial best practices; (ii) perform CA or Information System Security inspections as their primary responsibility; and (iii) be familiar with the Issuing CA's practices.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The Compliance Inspector(s) and CA must have a contractual relationship for the performance of the inspection, or be sufficiently separated organizationally from the Issuing CA to provide an unbiased, independent evaluation.

8.4 TOPICS COVERED BY ASSESSMENT

The CA shall undergo an audit in accordance with one of the following schemes:

1. For Audit Periods starting before the Effective Date defined in Section 1.2.1 of the first version of these Requirements, "WebTrust for CAs v2.2.2 or newer"; or
2. For Audit Periods starting after the Effective Date defined in Section 1.2.1 of the first version of these Requirements, "WebTrust for CAs v2.2.2 or newer" AND "WebTrust for S/MIME Baseline Requirements v1.0.0 or newer";

The audit shall be conducted by a Qualified Auditor, as specified in Section 8.2.

Inspections must follow any guidelines adopted by the PMA, including whether the Issuing CA's practices comply with the technical, procedural, and personnel policies and practices outlined in this Policy. This inspection requirement does not require a review of whether RAs implement and comply with technical, procedural, and personnel practices and policies set forth in this Policy. An RA will conduct an internal review of compliance with this Policy, certify compliance to the Issuing CA on an annual basis, and be subject to audits for security, systems, and procedures by either its regulator, licensing body, the Issuing CA, or the PMA.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Issuing CA inspection results must be submitted to the Issuing CA's regulator or licensing body where applicable, and the PMA. If irregularities are found, the Issuing CA must submit a report to its regulator or licensing body and the PMA as to any action the Issuing CA will take in response to the inspection report. Where the Issuing CA fails to take appropriate action in response to the inspection report, the Issuing CA's regulator, licensing body or the PMA may: (i) indicate the irregularities, but allow the Issuing CA to continue operations until the next programmed inspection; (ii) allow the Issuing CA to continue operations for a maximum of 30 days pending correction of any problems before Revocation; (iii) downgrade the level of assurance of any Certificates issued by the Issuing CA (including Cross-Certificates); or (iv) revoke the Issuing CA's Certificate. Any decision regarding which of these actions to take will be based on the severity of the irregularities. Any remedy may include permanent or temporary CA cessation, but all relevant factors must be considered before making a decision. A special audit may be required to confirm the implementation and effectiveness of the remedy. The Issuing CA will post any appropriate results of an inspection, in whole or in part, so that it is accessible for review by Subscribers, Authorized Relying Parties, and RAs. The manner and extent of the publication will be defined by the Issuing CA.

8.6 COMMUNICATION OF RESULTS

The results of the Issuing CA internal Certificate Issuance quality audits shall be fully documented, and reports resulting from it are to be submitted to Operations Management for review by risk management within 30 calendar days of the date of their completion by the Security Office. Such reports will identify the CP and CPS used in the assessment including their dates and version numbers.

The CA must make its Audit Report publicly available no later than 3 months after the end of the audit period. In the event of a delay greater than 3 months, and if so requested by an Application Software Supplier, the CA 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 must contain at least the following clearly-labeled information:

1. name of the Organization being audited;
2. name and address of the Organization performing the audit;
3. the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross Certificates, that were in-scope of the audit;
4. audit criteria, with version number(s), that were used to audit each of the Certificates (and associated keys);
5. a list of the CA policy documents, with version numbers, referenced during the audit;
6. whether the audit assessed a period of time or a point in time;
7. the start date and end date of the Audit Period, for those that cover a period of time;
8. the point in time date, for those that are for a point in time; and
9. the date the report was issued, which will necessarily be after the end date or point in time date;

An authoritative English language version of the publicly available audit information must be provided by the Qualified Auditor and the CA shall ensure it is publicly available. The Audit Report must be available as a PDF and shall be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report must be uppercase letters and must not contain colons, spaces, or line feeds.

8.7 SELF AUDITS

During the period in which the CA issues Certificates, the CA shall monitor adherence to its CP, CPS to strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of 1 Certificate or at least 3 percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

The CA shall perform self-audits on Server Certificates, and Code Signing Certificates in accordance with the CA/B Forum BR The CA may perform self-audit on other Certificate types to validate reasonable compliance with browser’s root store CA Policies.

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

Issuing CAs 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

The Issuing CA may establish and charge a reasonable fee for providing TrustID Certificate status information services.

9.1.3 Revocation or Status Information Access Fees

The Issuing CA may establish and charge a reasonable fee for providing TrustID Certificate Revocation information services.

9.1.4 Fees for Other Services

The Issuing CA and RAs may establish and charge other reasonable fees. However, no fee may be charged for access to review the provisions of this Policy.

9.1.5 Refund Policy

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

The Issuing CA shall maintain insurance related to its respective performance and obligations as follows:

A. Commercial General Liability insurance (occurrence form) with policy limits of at least 2 million USD in coverage; and
B. Professional Liability/Errors and Omissions insurance, with policy limits of at least 5 million USD in coverage, and including coverage for:
    a. claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and;
    b. claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

Such insurance must be with a company rated no less than A- as to Policy Holder’s Rating in the current edition of Best’s Insurance Guide (or with an association of companies each of the members of which are so rated).

9.2.2 Other Assets

CAs and RAs shall maintain reasonable and sufficient financial resources to maintain operations, fulfill duties, and address commercially reasonable liability obligations to entities described in Section 1.3 of this 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 this 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 this Policy. However, such information may not be used by any non-Authorized Relying Party or for any unauthorized purpose (e.g., mass, unsolicited emailing, junk email, spam, etc.). A TrustID Certificate should only contain information that is relevant and necessary to effect transactions with the Certificate.

9.3.3 Responsibility to Protect Confidential Information

9.3.3.1 Private Key Information

Private Keys are sensitive and confidential information and, therefore, Private Keys should be held in the strictest confidence. Under no circumstances will any Private Key appear unencrypted outside the Cryptographic Module.

9.3.3.2 CA and RA Information

All non-public information stored locally on Issuing CA and/or RA equipment (not in the Repository) is considered confidential for purposes of this Policy. 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 Issuing CA management of TrustID Certificates, such as compilations of Certificate information, shall be treated as confidential.

9.4 PRIVACY OF PERSONAL INFORMATION

All Subscribers' identifying information as defined by local privacy regulations including information that links a subject pseudonym to the real identity of a Subject Individual shall be protected from unauthorized disclosure. Any sensitive information shall be explicitly identified in a CA CPS or RA'S RPS. All information stored electronically on the component equipment and not in the Repository, and all physical records shall be handled as sensitive. Access to this information shall be restricted to those with an official need-to-know in order to perform their responsibilities as defined in this CP, and such information shall not be disclosed to any third party unless authorized by this CP, by agreement, by order of a court of competent jurisdiction, or as required by law, government rule or regulation. Requirements for notice and consent to use private information shall be defined in the respective CPS and/or privacy Policy.

CAs, RAs, LRAs, and Trusted Agents shall disclose a privacy Policy to all entities that submit Subscriber identifying information to CAs and RAs.

9.4.1 Privacy Plan

9.4.1.1 Permitted Acquisition of Private Information

The Issuing CA or 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, the Issuing CA or 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.

The CA shall publish a privacy policy that provides information on the CA's data protection practices. The privacy policy should include information on how the CA collects, uses, shares, store, and deletes or retains data, as well as contact information for the exercise of privacy rights. The CA shall document where to obtain this information within Section 9.4.1 of the CPS.

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. The Issuing CA or 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

The CA or RA shall treat all personal information about an Individual that is not publicly available in the contents of a Certificate as private information. This includes information that links a subject pseudonym to the real identity of the Subject Individual.

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

Effective April 20, 2018, the Issuing CA shall comply with Certificate Transparency (CT) by publishing new, renewed and replaced TrustID Server Certificates (DV, OV, and EV) into at least 3 public Certificate Transparency logs created for this purpose.

9.4.4 Responsibility to Protect Private Information

Each PKI Participant is responsible for protecting the confidentiality of private information that is in its possession, custody, or control with the same degree of care that it exercises with respect to its own information of like importance, but in no event less than reasonable care, and shall use appropriate safeguards and otherwise exercise reasonable precautions to prevent the unauthorized disclosure of private information.

The CA or RA shall require the same from any service providers who handle private information on behalf of the CA or RA.

9.4.5 Notice and Consent to Use Private Information

The CA or RA shall provide appropriate notices to, and receive the necessary consent, from Subject Individuals before using private information for any purpose other than providing services related to the issuance and management of Certificates. The CA or RA shall require the same from any service providers who handle private information on behalf of the CA or RA.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Participants may be required to participate in, and bear financial responsibility for, a centrally administrated Alternative Dispute Resolution (ADR) process established under Section 9.13.

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. This Policy, its OID, and the TrustID mark are the intellectual property of IdenTrust Inc., protected by trademark, copyright, and other laws regarding intellectual property, and may be used only pursuant to a license or other express permission from IdenTrust Inc. and only in accordance with the provisions of this Policy. Any other use of the above without express written permission of the owner is expressly prohibited.

9.6 REPRESENTATIONS AND WARRANTIES

No joint venture, partnership, trust, agency, or fiduciary relationship is established or deemed to be established among any of the parties using this Policy or the PKI established pursuant hereto. Issuance of TrustID Certificates in accordance with this Policy does not make the Issuing CA, or any RA, an agent, fiduciary, trustee, or other representative of Subscribers or Authorized Relying Parties.

PKI Service Providers assume no liability whatsoever in relation to the use of TrustID Certificates or associated Key Pairs for any use other than in accordance with this Policy or related agreements. Each End Entity will indemnify and hold the PKI Service Providers and their respective directors, officers, employees, agents, and affiliates harmless from any and all liability arising out of the End Entity’s use of a TrustID Certificate for other than its intended use.

The PKI Service Providers, and their employees, servants, or agents, make no representations or warranties, express or implied, other than as expressly stated in this Policy or in an agreement between the PKI Service Provider and an End Entity. Except as expressly prohibited in this Policy, PKI Service Providers may disclaim all warranties and obligations of any type, including without limitation: (i) any warranty of merchantability; (ii) any warranty of fitness for a particular purpose; (iii) any warranty of accuracy of information provided; and (iv)any warranty of non-infringement.

The PMA, Issuing CAs, and RAs are neither intermediaries nor guarantors of the underlying transactions between End Entities. Recourse, liability, and dispute resolution for claims solely between End Entities (e.g., claims of non-performance not related to Subscriber identity) shall be under applicable law. Claims against PKI Service Providers are limited to showing that the PKI Service Providers operated in a manner inconsistent with this Policy, the applicable CPS, or a related agreement or warranty. PKI Service Providers are responsible to an Authorized Relying Party only if the Authorized Relying Party has complied with all obligations, terms, and conditions of this Policy and of the applicable Authorized Relying Party Agreement, and only to the extent otherwise allowed by this Policy. In addition, PKI Service Providers are responsible to an Authorized Relying Party only for direct damages suffered by such Authorized Relying Party that are (i) caused by the failure of the PKI Service Provider to comply with the terms of this Policy, the CPS, or a related agreement or warranty, and (ii) sustained by such Authorized Relying Party as a result of Reasonable Reliance on a TrustID Certificate in accordance with this Policy.

PKI Service Providers may enter into indemnification agreements with other PKI Service Providers to appropriately allocate the risk and financial responsibility arising from the parties’ respective duties and obligations.

9.6.1 CA Representations and Warranties

The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with this CP, the TrustID CPS and the CA/B Forum BR in issuing and managing the Certificate.

9.6.1.1 Notification of Certificate Issuance and Revocation

Issuing CAs (CAs who have cross-certified or are otherwise authorized to issue TrustID Certificates by the PMA) may enter into arrangements to provide notification of Certificate Issuance and Revocation to each other and to share other information relevant to the operation of the PKI established by this Policy. The Issuing CA must make an online Certificate status database or Certificate Revocation Lists available to End Entities in accordance with Section 4.10. The Issuing CA must notify an End Entity when a TrustID Certificate bearing the End Entity's DN is issued or revoked.

9.6.1.2 Subscriber Warranties

Issuing CAs must provide the following warranties, in separate writing or in contract, to all Subscribers of TrustID Certificates they issue:

- The issuing ca has issued and managed the TrustID Certificate in accordance with the applicable Subscriber Agreement (and in accordance with this policy and any applicable cps) if this policy has been incorporated by reference in the Subscriber Agreement (see end entity agreements); and;
- The TrustID Certificate meets all requirements of the applicable Certificate Agreement (and this policy and any applicable cps), if this policy has been incorporated by reference in the Subscriber Agreement, (see end entity agreements).

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

An Issuing CA may provide a validation warranty to an Authorized Relying Party for a per transaction amount for transactions in which the Authorized Relying Party exercises Reasonable Reliance on a TrustID Certificate. In such instances, the Issuing CA warrants that:

- The Issuing CA has issued and managed the TrustID Certificate in accordance with this Policy;
- The Issuing CA complied with the requirements of this Policy and any applicable CPS when verifying the identity of the Subscriber;
- There are no material misrepresentations of fact in the TrustID Certificate known to the Issuing CA, and the Issuing CA has taken steps as required under this Policy to verify the information contained in the TrustID Certificate;
- The Issuing CA has taken all steps required by this Policy to ensure that the Subscriber's submitted information has been accurately transcribed to the TrustID Certificate;
- Information provided by the Issuing CA concerning the current validity of the TrustID Certificate is accurate and that validity has not been diminished by the Issuing CA's failure to promptly revoke the TrustID Certificate in accordance with Section 4.9; and;
- The TrustID Certificate meets all material requirements of this Policy and any applicable CPS.

These warranties apply to any Authorized Relying Party who: (i) relies on a TrustID Certificate in an electronic transaction in which the TrustID Certificate played a material role in verifying the identity of 1 or more persons or devices; (ii) exercises Reasonable Reliance on that TrustID Certificate; and (ii) follows all procedures required by this Policy and by the applicable Authorized Relying Party Agreement for verifying the status of the TrustID Certificate. These warranties are made to the Authorized Relying Party as of the time the Repository is referenced to determine TrustID Certificate validity, and only if the TrustID Certificate is valid and not revoked at that time.

9.6.1.4 Warranty Limitations

The warranties offered to both Subscribers and Authorized Relying Parties will be subject to the limitations set forth elsewhere in this Policy. Issuing CAs may provide further limitations and exclusions on these warranties as the Issuing CA deems appropriate, relating to: (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 this Policy or of any agreement with the Issuing CA or RA, and/or (d) other actions giving rise to any loss; (ii) events beyond the reasonable control of the Issuing CA and the RAs; and (i) time limitations for the filing of claims. However, such limitations and exclusions may not, in any event, be less than those provided for in Section 9.6.1.3.

9.6.1.5 Time Between Certificate Request and Issuance

There is no stipulation for the period between the receipt of an application for a TrustID Certificate and the Issuance of a TrustID Certificate, but the Issuing CA will make reasonable efforts to ensure prompt Issuance.

9.6.1.6 Certificate Revocation and Renewal

The Issuing CA must ensure that any procedures for the expiration, Revocation and renewal of a TrustID Certificate will conform to the relevant provisions of this Policy and will be expressly stated in a Subscriber Agreement and any other applicable document outlining the terms and conditions of Certificate use, including ensuring that: (i) Key Changeover Procedures are in accordance with Section 5.6; (ii) notice of Revocation of a Certificate will be posted to an online Certificate status database and/or a CRL, as applicable, within the time limits stated in Section 4.9; and (iii) the address of the online Certificate status database and/or CRL is defined in the TrustID Certificate.

9.6.1.7 End Entity Agreements

The Issuing CA will enter into agreements with End Entities governing the provision of Certificate and Repository services and delineating the parties' respective rights and obligations.

The Issuing CA will ensure that all Subscriber Agreements incorporate by reference the provisions of this Policy regarding the Issuing CA's and the Subscriber's rights and obligations. In the alternative, the Issuing CA may ensure that its Subscriber Agreements, by their terms, provide the respective rights and obligations of the Issuing CA and the Subscribers as set forth in this Policy, 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 A PARTY TO THE AGREEMENT;
- ANY WARRANTIES MADE BY THE ISSUING CA AND ANY LIMITATIONS ON WARRANTIES OR LIABILITY OF THE ISSUING CA AND/OR RA;
- PROVISIONS REGARDING THE PROTECTION OF PRIVACY AND CONFIDENTIAL INFORMATION; AND
- PROVISIONS REGARDING ALTERNATIVE DISPUTE RESOLUTION.
- NOTHING IN THE SUBSCRIBER AGREEMENTS MAY WAIVE OR OTHERWISE LESSEN THE OBLIGATIONS OF THE SUBSCRIBER AS PROVIDED IN SECTION 9.6.3 OF THIS POLICY.

The Issuing CA will ensure that all Authorized Relying Party Agreements incorporate by reference the provisions of this Policy regarding the Issuing CA’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 this Policy.

9.6.1.8 Protection of Private Keys

The Issuing CA must ensure that its Private Keys and Activation Data are protected in accordance with Section 4 and Section 6 of this Policy.

9.6.1.9 Restrictions on Issuing CA's Private Key Use

The Issuing CA must ensure that its CA Private Signing Key is used only to sign Certificates and CRLs. The Issuing CA must ensure that Private Keys issued to its personnel to access and operate CA applications are used only for such purposes. To the extent CA 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

The Issuing CA must ensure that: (i) it only accepts information from RAs that understand and are obligated to comply with this Policy; (ii) it complies with the provisions of this Policy in its certification and Repository services, Issuance and Revocation of TrustID Certificates and Issuance of CRLs; (iii) it makes reasonable efforts to ensure RA and End Entity adherence to this Policy 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

An Issuing CA’s liability to an End Entity will be determined in accordance with any agreement between the Issuing CA and the End Entity; as such liability may be limited by Section 9.6 and other provisions of this Policy.

9.6.2 RA Representations and Warranties

The Issuing CA must ensure that all its RAs comply with all the relevant provisions of this Policy and the Issuing CA's CPS. The Issuing CA shall continue to be responsible for any matters delegated to an RA, although an Issuing CA and an RA may enter into an indemnification agreement in accordance with Section 9.6.

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 Verification Responsibilities.

9.6.2.2 Accuracy of RA Representations

When an RA submits End Entity or Sponsoring Organization information to an Issuing CA, it certifies to the Issuing CA that it has authenticated the identity of that End Entity or Sponsoring Organization in accordance with Sections 3 and 4 of this Policy.

9.6.2.3 Protection of RA Private Keys

Each person performing RA duties online through a remote administration application with the Issuing CA must ensure that his or her Private Keys are protected in accordance with Sections 5 and 6 of this Policy.

9.6.2.4 Restrictions on RA Private Key Use

Private Keys used by RA personnel to access and operate RA Applications online with the Issuing CA must not be used for any other purpose.

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 the Issuing CA 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 and other provisions of this Policy.

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 performs the Key Pair generation on an approved Cryptographic Module in accordance with Section 6.2.1.

9.6.3 Subscriber Representations and Warranties

The CA shall require, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, the CA shall obtain, for the express benefit of the CA and the Certificate Beneficiaries, either the Applicant's:

1. Agreement to the Subscriber Agreement with the CA; or
2. Acknowledgement of the Terms of Use.

The CA shall implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement shall apply to the Certificate to be issued pursuant to the Certificate Request. The CA may use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement may be used for each Certificate Request, or a single Agreement may be used to cover multiple future Certificate Requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use.

The Subscriber Agreement or Terms of Use shall contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. **Accuracy of Information**: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the Certificate Request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;
2. **Protection of Private Key**: An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device such as a password or token);
3. **Acceptance of Certificate**: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. **Use of Certificate**: An obligation and warranty to use the Certificate only on Mailbox Addresses listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
5. **Reporting and Revocation**: An obligation and warranty to:
    a. promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and
    b. Promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
6. **Termination of Use of Certificate**: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
7. **Responsiveness**: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. **Acknowledgment and Acceptance**: An acknowledgment and acceptance that the CA is entitled to revoke the Certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use, or if revocation is required by this CP and, the TrustID CPS or the CA/B Forum BR

9.6.3.1 Representations

Provide complete and accurate responses to all requests for information made by the Issuing CA (or an RA) during Applicant registration, Certificate application, and Identity Proofing processes; and upon Issuance of a TrustID Certificate naming the Applicant 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;

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. Notwithstanding the immediately preceding sentence, where a Key Pair is for TrustID Card Authentication Certificate or TrustID Device Certificate and is generated by a CA or an RA, the Applicant will not be responsible for the generation of such Key Pair;

9.6.3.3 Restrictions on Subscriber Private Key Use

Use the TrustID Certificate and the corresponding Private Key exclusively for purposes authorized by this Policy and only in a manner consistent with this Policy, including but not limited, in the case of Code Signing and 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; and;

9.6.3.4 Notification Upon Private Key Compromise

Instruct the Issuing CA (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 3.2.3, 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 will have his, her, or its TrustID Certificate revoked and will forfeit all claims he, she, or it may have against PKI Service Providers.

9.6.3.6 Other Agreements

A Subscriber's obligations will be governed by the Subscriber Agreement between the Subscriber and the Issuing CA.

9.6.4 Relying Party Representations and Warranties

Before relying on or using a TrustID Certificate issued under this Policy, an Authorized Relying Party is obligated to:

9.6.4.1 Use of Certificates for Appropriate Purpose

Ensure that the TrustID Certificate and intended use are appropriate under the provisions of this Policy;

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; and;

9.6.4.3 Revocation Check Responsibility

Check the status of the TrustID Certificate by Online Status Check or against the appropriate and current CRL, as applicable, in accordance with the requirements stated in Section 4.10.

9.6.4.4 Reasonable Reliance

For Digital Signatures created during the Operational Period of a TrustID Certificate, an Authorized Relying Party has a right to rely on the Certificate only under circumstances constituting Reasonable Reliance as defined in Section 1.6.1.

9.6.4.5 Consequences of Relying on Revoked Certificate

If an Authorized Relying Party relies on a TrustID Certificate that was expired or that the Authorized Relying Party knew or should have known was revoked at the time of reliance (e.g., a decision to rely on a revoked TrustID Certificate based on the reasons for Revocation, information from other sources, or specific business considerations pertaining to the Authorized Relying Party), the Authorized Relying Party does so at its own risk and, in so relying, waives any warranties that any PKI Service Provider may have provided.

9.6.4.6 Consequences of Breach

An Authorized Relying Party found to have acted in a manner counter to these obligations will forfeit all claims he, she or it may have against any PKI Service Providers.

9.6.4.7 Other Agreements

An Authorized Relying Party's obligation will be governed by the Authorized Relying Party Agreement between the Authorized Relying Party and the Issuing CA.

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 this Policy, 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 CP, the TrustID CPS, and any applicable agreement between the Issuing CA and an End Entity, the provisions of Section 9.6 shall apply.

9.6.5.3 Representations and Warranties of Affiliated/Subscribing Organizations

A Subscribing Organization shall represent and warrant that they will:

- Authorize the affiliation of Subscribers with the Organization and
- Immediately inform the Participant CA of any severance of affiliation with any current Subscriber.

9.7 DISCLAIMERS OF WARRANTIES

EXCEPT FOR THOSE WARRANTIES EXPRESSLY PROVIDED IN THIS CP 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 this section shall not form any limitation on any limitations or disclaimers of IdenTrust, set forth under this CP, other provisions of the TrustID CPS, or any agreement between IdenTrust and an End Entity. Further, the provisions of this section 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 the TrustID CPS is prevented or delayed by an event beyond such IdenTrust's reasonable control, including without limitation, crime, fire, flood, war, terrorism, riot, acts of civil or military authority (including governmental priorities), severe weather, strikes or labor disputes, or by disruption of telecommunications, power or Internet services not caused by such IdenTrust, then IdenTrust will be excused from such performance to the extent it is necessarily prevented or delayed thereby.

9.8 LIMITATIONS OF LIABILITY

This Policy establishes an open-but-bounded PKI. PKI Service Providers will not be liable to any person who relies upon a Certificate unless such liability is clearly established by contract, special warranty, or law.

Individual Certificate type liabilities may be set forth in the Issuing CA's CPS.

UNLESS OTHERWISE SPECIFIED IN SECTION 9.8 OF THE TRUSTID CPS, IDENTRUST WILL NOT BE LIABLE TO YOU UNDER ANY CIRCUMSTANCES WITH RESPECT TO ANY SUBJECT MATTER HEREOF UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY, OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE OR EXEMPLARY DAMAGES OF ANY KIND (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUE OR GOODWILL OR ANTICIPATED PROFITS OR LOST BUSINESS), REGARDLESS OF WHETHER IDENTRUST KNEW OR HAD REASON TO KNOW OF THE POSSIBILITY THEREOF.

9.9 INDEMNITIES

Neither IdenTrust nor its agents assume financial responsibility for improperly used Certificates.

Without forming any limitation on any other provision of this CP, the TrustID CPS or any agreement between IdenTrust and an End Entity: (i) a Relying Party under an IdenTrust TrustID Relying Party Agreement shall indemnify IdenTrust under the applicable terms and conditions of any indemnification provision therein; and (ii) a Subscriber under an IdenTrust TrustID Subscriber Agreement shall indemnify IdenTrust under the applicable terms and conditions of any indemnification provision therein.

Notwithstanding any limitations on its liability to Subscribers and Authorized Relying Parties, IdenTrust understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with IdenTrust do not assume any obligation or potential liability of IdenTrust under the CA/B Forum BR or that otherwise might exist because of the Issuance or maintenance of TrustID Certificates or reliance thereon by Authorized Relying Parties or others. IdenTrust will defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a TrustID Certificate issued by IdenTrust, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a TrustID Certificate issued by IdenTrust where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a TrustID Certificate that is still valid or displaying as trustworthy: (1) a TrustID Certificate that has expired, or (2) a TrustID Certificate that has been revoked (but only in cases where the Revocation status is currently available from IdenTrust online, and the application software either failed to check such status or ignored an indication of revoked status).

9.10 TERM AND TERMINATION

9.10.1 Term

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

9.10.2 Termination

The requirements of this CP remain in effect through the end of the archive period for the last Certificate issued.

9.10.3 Effect of Termination and Survival

The conditions and effects resulting from termination of this document 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

The provisions below in this section shall govern with respect to any notice provided in relation to this CP to or from IdenTrust; provided; however, this section shall not be construed to govern with respect to any communication, including notices, for which a different method is expressly provided for (a) in this CP (e.g., notices under Section 9.12) or (b) in an agreement between IdenTrust and the Participant.

9.11.1 Notices by Individual Participants to IdenTrust

Notices by Individual Participants to IdenTrust shall be made by at least 1 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 1 of the following methods, with the choice between methods to be made by IdenTrust:

i. 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

ii. 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 CP is reviewed by IdenTrust PMA from time to time. Errors, updates, or suggested changes to this document should be communicated to the contact mentioned in Section 1.5.2. Such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.1 Procedure for Amendment

For an amendment of this CP to become effective, it must first be approved by the IdenTrust PMA in accordance with Section 1.5.4. Amendments in the CP will most frequently reflect amendments and timing driven updates to the TrustID CPS changes, typically once a year, but frequently when required in accordance with this CP. Changes that may materially affect Subscribers or Relying Parties are subject to a public comment period before consideration by the IdenTrust PMA. Other amendments such as editorial or typographical corrections, changes to the contact details, or other such minor changes will not be submitted to the TrustID Policy Authority and no comment period will be necessary.

After the PMA accepts changes, IdenTrust's PMA Chair will submit the document for final preparation and publication. Before publication, the document is redacted for sensitive information that can post security risks. The redacted document is the Public version CP. The final and accepted copy of this CP, 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.

9.12.2 Notification Mechanism and Period

IdenTrust will notify interested Participants of proposed changes, the final date for receipt of comments, and the proposed effective date of the change. Comments may be filed with IdenTrust within the comment period. Decisions with respect to the proposed changes are at the sole discretion of IdenTrust.

A copy of the TrustID CPS and this CP are available in electronic form on the Internet at: https://www.identrust.com/support/documents/trustid

9.12.3 Circumstances Under Which OID Must Be Changed

OIDs will be changed in this CP if the PMA determines that a change in the CPS requires a change in OIDs.

9.13 DISPUTE RESOLUTION PROVISIONS

In the event of any dispute or disagreement between 2 or more Participants ("Disputing Parties") arising out of or related to this Policy or a TrustID Certificate, the Disputing Parties will use their best efforts to settle the dispute or disagreement through mediation or good faith negotiations following notice from 1 Disputing Party to the other(s). If the Disputing Parties cannot reach a mutually agreeable resolution of the dispute or disagreement within sixty (60) days following the date of such notice, then the Disputing Parties will submit the dispute to binding arbitration. The American Arbitration Association's Rules for Commercial Arbitration and Optional Rules for Emergency Measures of Protection will apply to the proceedings.

This provision will not limit the right of party to obtain other recourse and relief under any applicable law for disputes or disagreements that do not arise out of or which are not related to this Policy or a TrustID Certificate.

9.13.1 Specific Provisions/ Incorporation of Policy

The Issuing CA must ensure that its agreements with RAs and End Entities contain appropriate provisions that (i) incorporate the provisions of this Policy by reference, or (ii) provide to the respective contracting parties the protections established by this Policy.

9.14 GOVERNING LAW

The enforceability, construction, interpretation, and validity of this Policy will be governed by the laws of the United States of America and the law of the State of Utah, without regard to its conflicts of law principles.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CP 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

Except where specified by other contracts, this CP shall constitute the entire understanding and agreement between the parties with respect to the transactions contemplated, and supersedes any and all prior or contemporaneous oral or written representation, understanding, agreement, or communication concerning the subject matter hereof. No party is relying upon any warranty, representation, assurance, or inducement not expressly set forth herein and none shall have any liability in relation to any representation or other assurance not expressly set forth herein unless it was made fraudulently. Without prejudice to any liability for fraudulent misrepresentation, no party shall be under any liability or shall have any remedy in respect of misrepresentation or untrue statement unless and to the extent that a claim lies for breach of a duty set forth in this CP.

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

In the event of a conflict between these Requirements and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which a CA operates or issues Certificates, a CA may 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, the CA shall immediately (and prior to issuing a Certificate under the modified requirement) include in Section 9.16.3 of the CPS a detailed reference to the Law requiring a modification of these Requirements under this section, and the specific modification to these Requirements implemented by the CA.
The CA shall also (prior to issuing a Certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CPS by sending a message to public@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/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to these Requirements accordingly.

Any modification to CA practice enabled under this section shall be discontinued if and when the Law no longer applies, or these Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to the CA's CPS and a notice to the CA/Browser Forum, as outlined above, shall be made within 90 days...

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

No waiver of any breach or default or any failure to exercise any right hereunder shall be construed as a waiver of any subsequent breach or default or relinquishment of any future right to exercise such right. The headings in this CP are for convenience only and cannot be used in interpreting this CP.

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 Waivers

Waivers will not be granted under any level of assurance. Variation in the Issuing CA's practice will either be deemed acceptable under this Policy, or a change will be requested to this Policy, or a new Policy will be established for the non-compliant practice.

9.17.1.2 Issuance

To be legally valid, a TrustID Certificate must be issued in accordance with this Policy and any applicable law.

9.17.1.3 Acceptance

The act of Acceptance will be logged by the Issuing CA 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 the Issuing CA in a trustworthy manner that comports with industry standards and any applicable laws or provisions of this Policy 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 Authorized Relying Party's Digital Signature verification request is able to confirm that the Digital Signature in question was created during the Operational Period of a valid TrustID Certificate. Exceptions to the Private Key Usage period may be permissible if approved by the PMA and so long as such exceptions do not conflict with documented best practices, including RFC 5280 and CA/B Forum BR.

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 the Issuing CA or RA 4 months after termination of the applicable Authorized Relying Party Agreement or 2 (2) years after the Authorized Relying Party’s validation of the TrustID Certificate with the Issuing CA's Repository, whichever occurs first.

APPENDIX A: OTHER PMA APPROVED CRYPTOGRAPHIC MODULES

Besides the Cryptographic Module standards defined in Section 6.2.1, the following Cryptographic Modules have been approved by IdenTrust PMA:

Product Name	Certificate OID Approved	Approval Date
HID® Crescendo® Mobile https://www.hidglobal.com/products/cards-and-credentials/crescendo/crescendo-mobile	• 2.16.840.1.113839.0.6.10.2 • 2.16.840.1.113839.0.6.10.100 • 2.16.840.1.113839.0.6.11.1 • 2.16.840.1.113839.0.6.11.2	May 31, 2019
HID® Crescendo® Key https://www.hidglobal.com/doclib/files/resource_files/hid-iams-crescendo-key	For usage within any TrustID Certificate requiring software or KSM based Private Key storage.	November 21, 2019
HID® Crescendo® C2300 Smart Card Series https://www.hidglobal.com/products/cards-and-credentials/crescendo/c2300	For usage within any TrustID Certificate requiring software or KSM based Private Key storage	November 21, 2019
SafeNet® eToken® 5110 CC	• 2.16.840.1.113839.0.6.14.1 • 2.16.840.1.113839.0.6.14.2	August 3, 2021