TrustID®

Certificate Policy

IdenTrust Services LLC.

Version 4.7

January 31, 2020

IdenTrust.com

TABLE OF CONTENTS

Table of Contents 2

1 INTRODUCTION 12

1.1 OVERVIEW 12

1.2 DOCUMENT NAME AND IDENTIFICATION 12

1.2.1 Alphanumeric Identifier 14

1.2.2 Object Identifier (OID) 14

1.3 PKI PARTICIPANTS 15

1.3.1 Certification Authorities (CAs) 15

1.3.2 Registration Authorities (RAs) 16

1.3.3 Subscribers 16

1.3.4 Authorized Relying Parties 16

1.3.5 Other Participants 16

1.4 CERTIFICATE USAGE 17

1.4.1 Appropriate Certificate Uses 17

1.4.2 Prohibited Certificate Uses 17

1.5 POLICY ADMINISTRATION 18

1.5.1 Organization Administering this CP Document 18

1.5.2 Contact Person 18

1.5.3 Person Determining CPS Suitability for the Policy 18

1.5.4 CPS Approval Procedures 18

1.5.5 Publication and Notification Policies 18

1.6 DEFINITIONS AND ACRONYMS 19

1.6.1 Definitions 19

1.6.2 Acronyms 28

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 29

2.1 REPOSITORIES 29

2.2 PUBLICATION OF CERTIFICATION INFORMATION 29

2.3 TIME OR FREQUENCY OF PUBLICATION 30

2.4 ACCESS CONTROLS ON REPOSITORIES 30

3 IDENTIFICATION AND AUTHENTICATION 31

3.1 NAMING 31

3.1.1 Types of Names 31
3.1.2 Need for Names to Be Meaningful 32
3.1.3 Anonymity or Pseudonymity of Subscribers 34
3.1.4 Rules for Interpreting Various Name Forms 34
3.1.5 Uniqueness of Names 34
3.1.6 Recognition, Authentication, and Role of Trademarks 34
3.2 INITIAL IDENTITY VALIDATION 35
3.2.1 Method to Prove Possession of Private Key 35
3.2.2 Authentication of Organization Identity 35
3.2.3 Authentication of Individual Identity 36
3.2.4 Non-verified Subscriber Information 39
3.2.5 Validation of Authority and Other Attributes 39
3.2.6 Criteria for Interoperation 39
3.2.7 Verification and Validation of Information 39
3.2.8 Verification of Email address 40
3.2.9 Verification of the Certificate Request 40
3.2.10 Authentication of Device Identity 40
3.2.11 Authentication of TrustID Administrative RA Certificates for Devices and Individuals 41
3.2.12 Authentication of Other Certificates 42
3.2.13 Authorized Relying Parties 42
3.3 IDENTIFICATION AND AUTHENTICATION 42
3.3.1 Identification and Authentication for Routine Re-Key 42
3.3.2 Identification and Authentication for Re-key After Revocation 42
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS 42
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 43
4.1 CERTIFICATE APPLICATION 43
4.1.1 Who Can Submit a Certificate Application 43
4.1.2 Enrollment Process and Responsibilities 43
4.1.3 Enrollment Process / Bulk Loading 43
4.1.4 Information Collection 43
4.2 CERTIFICATE APPLICATION PROCESSING 43
4.2.1 Performing Identification and Authentication Functions 44
4.2.2 Approval or Rejection of Certificate Applications 44

4.2.3 Time to Process Certificate Applications 44
4.3 CERTIFICATE ISSUANCE 44
4.3.1 CA or RA Actions During Certificate Issuance 44
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 45
4.4 CERTIFICATE ACCEPTANCE 45
4.4.1 Conduct Constituting Certificate Acceptance 45
4.4.2 Publication of the Certificate by the CA 45
4.4.3 Notification to Subscriber of Certificate Issuance by the CA to Other Entities 45
4.5 KEY PAIR AND CERTIFICATE USAGE 45
4.5.1 Subscriber Private Key and Certificate Usage 45
4.5.2 Relying Party Public Key and Certificate Usage 46
4.6 CERTIFICATE RENEWAL 46
4.6.1 Circumstance for Certificate Renewal 46
4.6.2 Who May Request Renewal 46
4.6.3 Processing Certificate Renewal Requests 47
4.6.4 Notification of New Certificate Issuance to Subscriber 47
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 47
4.6.6 Publication of the Renewal Certificate by the CA 47
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 47
4.7 CERTIFICATE RE-KEY 47
4.7.1 Circumstance for Certificate Re-Key 47
4.7.2 Who May Request Certification of a New Public Key 47
4.7.3 Processing Certificate Re-Keying Requests 48
4.7.4 Notification of New Certificate Issuance to Subscriber 48
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 48
4.7.6 Publication of the Re-Keyed Certificate by the CA 48
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 48
4.8 CERTIFICATE MODIFICATION 48
4.8.1 Circumstance for Certificate Modification 48
4.8.2 Who May Request Certificate Modification 48
4.8.3 Processing Certificate Modification Requests 48
4.8.4 Notification of New Certificate Issuance to Subscriber 49
4.8.5 Conduct Constituting Acceptance of Modified Certificate 49

4.8.6 Publication of the Modified Certificate by the CA 49
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 49
4.9 CERTIFICATE REVOCATION AND SUSPENSION 49
4.9.1 Circumstances for Revocation 49
4.9.2 Who Can Request Revocation 51
4.9.3 Procedure for Revocation Request 51
4.9.4 Revocation Request Grace Period 51
4.9.5 Time Within Which CA Must Process the Revocation Request 51
4.9.6 Revocation Checking Requirement for Relying Parties 52
4.9.7 CRL Issuance Frequency 52
4.9.8 Maximum Latency for CRLs 52
4.9.9 Online Revocation/Status Checking Availability 53
4.9.10 Online Revocation Checking Requirements 53
4.9.11 Other Forms of Revocation Advertisements Available 53
4.9.12 Special Requirements Re-Key Compromise 53
4.9.13 Circumstances for Suspension 53
4.9.14 Who Can Request Suspension 53
4.9.15 Procedure for Suspension Request 53
4.9.16 Limits on Suspension Period 54
4.10 CERTIFICATE STATUS SERVICES 54
4.10.1 Operational Characteristics 54
4.10.2 Service Availability 54
4.10.3 Optional Features 54
4.11 END OF SUBSCRIPTION 54
4.11.1 Subscribers 54
4.12 KEY ESCROW AND RECOVERY 55
4.12.1 Key Escrow and Recovery Policy and Practices 55
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 55
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 55
5.1 PHYSICAL SECURITY CONTROLS 55
5.1.1 Site Location and Construction 55
5.1.2 Physical Access 56
5.1.3 Power and Air Conditioning 56

5.1.4 Water Exposures 56
5.1.5 Fire Prevention and Protection 57
5.1.6 Media Storage 57
5.1.7 Waste Disposal 57
5.1.8 Offsite Backup 57
5.2 PROCEDURAL CONTROLS 57
5.2.1 Trusted Roles 57
5.2.2 Number of Persons Required Per Task 57
5.2.3 Identification and Authentication for Each Role 58
5.2.4 Roles Requiring Separation of Duties 58
5.3 PERSONNEL SECURITY CONTROLS 58
5.3.1 Qualifications, Experience, and Clearance Requirements 58
5.3.2 Background Check Procedures 58
5.3.3 Training Requirements 59
5.3.4 Retraining Frequency and Requirements 59
5.3.5 Job Rotation Frequency and Sequence 59
5.3.6 Sanctions for Unauthorized Actions 59
5.3.7 Independent Contractor Requirements 59
5.3.8 Documentation Supplied to Personnel 59
5.4 AUDIT LOGGING PROCEDURES 59
5.4.1 Types of Events Recorded 60
5.4.2 Frequency of Processing Log 60
5.4.3 Retention Period for Audit Log 60
5.4.4 Protection of Audit Log 60
5.4.5 Audit Log Backup Procedures 60
5.4.6 Audit Collection System (Internal vs. External) 60
5.4.7 Notification to Event-Causing Subject 61
5.4.8 Vulnerability Assessments 61
5.5 RECORDS ARCHIVAL 61
5.5.1 Types of Records Archived 61
5.5.2 Retention Period for Archive 65
5.5.3 Protection of Archive 65
5.5.4 Archive Backup Procedures 65

5.5.5 Requirements for Time-Stamping of Records 65
5.5.6 Archive Collection System (Internal or External) 65
5.5.7 Procedures to Obtain and Verify Archive Information 66
5.6 KEY CHANGEOVER 66
5.7 COMPROMISE AND DISASTER RECOVERY 66
5.7.1 Incident and Compromise Handling Procedures 66
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 66
5.7.3 Entity Private Key Compromise Procedures 66
5.7.4 Business Continuity Capabilities After a Disaster 67
5.7.5 Customer Service Center 67
5.7.6 Entity Public Key is Revoked 67
5.7.7 Entity Private Key is Downgraded 67
5.8 CA OR RA TERMINATION 67
6 TECHNICAL SECURITY CONTROLS 68
6.1 KEY PAIR GENERATION AND INSTALLATION 68
6.1.1 Key Pair Generation 68
6.1.2 Private Key Delivery to Subscriber 68
6.1.3 Public Key Delivery to Certificate Issuer 68
6.1.4 CA Public Key Delivery to Relying Parties 68
6.1.5 Key Sizes 69
6.1.6 Public Key Parameters Generation and Quality Checking 69
6.1.7 Key Usage Purposes (As per X.509 v3 Key Usage Field) 69
6.1.8 Hardware/Software Key Generation 69
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 69
6.2.1 Cryptographic Module Standards and Controls 69
6.2.2 Private Key (N out of M) Multi-Person Control 70
6.2.3 Private Key Escrow 70
6.2.4 Private Key Backup 70
6.2.5 Private Key Archival 70
6.2.6 Private Key Transfer Into or From a Cryptographic Module 70
6.2.7 Private Key Storage on Cryptographic Module 70
6.2.8 Method of Activating Private Key 71
6.2.9 Method of Deactivating Private Key 71

6.2.10 Method of Destroying Private Key 71
6.2.11 Cryptographic Module Rating 71
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 71
6.3.1 Public Key Archival 71
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 71
6.3.3 Restrictions on CA's Private Key Use 72
6.3.4 Certificate Periods for the Public and Private Keys 72
6.4 ACTIVATION DATA 72
6.4.1 Activation Data Generation and Installation 72
6.4.2 Activation Data Protection 72
6.4.3 Other Aspects of Activation Data 72
6.5 COMPUTER SECURITY CONTROLS 73
6.5.1 Specific Computer Security Technical Requirements 73
6.5.2 Computer Security Rating 73
6.6 LIFE CYCLE TECHNICAL SECURITY CONTROLS 73
6.6.1 System Development Controls 73
6.6.2 Security Management Controls 74
6.6.3 Life Cycle Security Controls 74
6.7 NETWORK SECURITY CONTROLS 74
6.8 TIME-STAMPING 74
7 CERTIFICATE, CRL, AND OCSP PROFILES 74
7.1 CERTIFICATE PROFILE 74
7.1.1 Version Number(s) 75
7.1.2 Certificate Extensions 75
7.1.3 Algorithm Object Identifiers 76
7.1.4 Name Forms 77
7.1.5 Name Constraints 77
7.1.6 Certificate Policy Object Identifier 77
7.1.7 Usage of Policy Constraints Extension 77
7.1.8 Policy Qualifiers Syntax and Semantics 77
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 77
7.2 CRL PROFILE 77
7.2.1 Version Number(s) 77

7.2.2 CRL and CRL Entry Extensions 78
7.3 OCSP PROFILE 78
7.3.1 Version Number(s) 78
7.3.2 OCSP Extensions 78
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 78
8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 78
8.2 IDENTITY /QUALIFICATIONS OF ASSESSOR 78
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 78
8.4 TOPICS COVERED BY ASSESSMENT 78
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 79
8.6 COMMUNICATION OF RESULTS 79
9 OTHER BUSINESS AND LEGAL MATTERS 79
9.1 FEES 79
9.1.1 Certificate Issuance or Renewal Fees 79
9.1.2 Certificate Access Fees 79
9.1.3 Revocation or Status Information Access Fees 80
9.1.4 Fees for Other Services 80
9.1.5 Refund Policy 80
9.1.6 Monetary Amounts 80
9.2 FINANCIAL RESPONSIBILITY 80
9.2.1 Insurance Coverage 80
9.2.2 Other Assets 80
9.2.3 Insurance or Warranty Coverage for End-Entities 80
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 80
9.3.1 Scope of Confidential Information 80
9.3.2 Information Not Within the Scope of Confidential Information 80
9.3.3 Responsibility to Protect Confidential Information 81
9.4 PRIVACY OF PERSONAL INFORMATION 81
9.4.1 Privacy Plan 81
9.4.2 Information Treated as Private 82
9.4.3 Information Not Deemed Private 82
9.4.4 Responsibility to Protect Private Information 82
9.4.5 Notice and Consent to Use Private Information 82

9.4.6 Disclosure Pursuant to Judicial or Administrative Process 82
9.4.7 Other Information Disclosure Circumstances 82
9.5 INTELLECTUAL PROPERTY RIGHTS 82
9.6 REPRESENTATIONS AND WARRANTIES 83
9.6.1 CA Representations and Warranties 83
9.6.2 RA Representations and Warranties 87
9.6.3 Subscriber Representations and Warranties 87
9.6.4 Relying Party Representations and Warranties 88
9.6.5 Representations and Warranties of Other Participants 89
9.7 DISCLAIMERS OF WARRANTIES 89
9.8 LIMITATIONS OF LIABILITY 90
9.9 INDEMNITIES 91
9.10 TERM AND TERMINATION 91
9.10.1 Term 91
9.10.2 Termination 91
9.10.3 Effect of Termination and Survival 91
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 92
9.11.1 Notices by Individual Participants to IdenTrust 92
9.11.2 Notices by IdenTrust to Individual Participants 92
9.11.3 Notices Delivery Method 92
9.12 AMENDMENTS 92
9.12.1 Procedure for Amendment 93
9.12.2 Notification Mechanism and Period 93
9.12.3 Circumstances Under Which OID Must Be Changed 93
9.13 DISPUTE RESOLUTION PROVISIONS 93
9.13.1 Specific Provisions/ Incorporation of Policy 93
9.14 GOVERNING LAW 94
9.15 COMPLIANCE WITH APPLICABLE LAW 94
9.16 MISCELLANEOUS PROVISIONS 94
9.16.1 Entire Agreement 94
9.16.2 Assignment 94
9.16.3 Severability 94
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights) 94

9.16.5 Force Majeure.....94
9.17 OTHER PROVISIONS.....95
9.17.1 Legal Validity of Certificates 95
APPENDIX A: OTHER PMA APPROVED CRYPTOGRAPHIC MODULES.....96

1 INTRODUCTION

1.1 OVERVIEW

This IdenTrust TrustID Certificate Policy, the Policy under which 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 the Amendments 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, transmission of confidential information, signature of electronic documents and authentication of infrastructure components such as web servers, firewalls, and directories.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the TrustID Certificate Policy approved for publication on January 31, 2020 by the IdenTrust Policy Management Authority (PMA). The following table contains subsequent revisions:

Table 1 - TrustID Certificate Policy Revisions

Revision	Date	Summary of Changes/Comments
1.7	May 22, 2015	Updates for TrustID CP compliance, inclusion of FATCA Organization Certificate, inclusion of Certificate Policy OID for hardware practices, compliance with CA/B Forum Requirement in relationship to use of CAA records for verification of Domain Name ownership/control, enhancement of Certificates definitions, and clarification on practices of unique names for Server Certificates.
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 CA/B Forum Baseline Requirements v.1.4.0 and CA/B Forum Extended Validation Guidelines v.1.6.0.
2.2	April 12, 2017	Add SHA-256 hash algorithm support with its own OID for TrustID Personal, TrustID Personal Hardware and TrustID Business Certificates.
2.3	September 8, 2017	Updated the document to include updates for the CA/B Forum Baseline Requirements v.1.4.1, CA/B Forum Extended Validation Code Signing Certificate Guidelines v. 1.4, Device Certificates, and Card

Revision	Date	Summary of Changes/Comments
		Authentication Certificates. Implemented September 8, 2017 and CP documentation approved by PMA committee on September 12, 2017.
2.4	January 30, 2018	Updates to reflect updated CA/B Forum Baseline Requirements.
4.0	May 31, 2018	- Conversion to RFC 3647 format. - Add CT Logging.
4.1	August 17, 2018	Section 1.2.2: Add the last two OIDs for TrustID Business Certificates.
4.2	October 18, 2018	Updates to clarify comments by Mozilla in reference to the EV SSL/TLS application.
4.3	January 31, 2019	- Section 1.1: Updates to reflect conformance with the version number of the CA/B Forum Baseline Requirement documents. - Section 1.6.1: Add definitions: o Certificate Chain o Subordinate CA Certificate - Section 4.9.1 and 4.9.5: Updates to better reflect the process in place to handle Server Certificate Revocation that is line with the CA/B Forum Baseline Requirements. - Section 9.8: Update liability language for Extended Validation Certificates.
4.4	May 31, 2019	- Section 1.1 move text to Section 2.2 - Section 1.2.2 OID renaming and new OID. - Section 1.6.1 Added definitions: CAA Resource Record Set; Technically Constrained Subordinate CA. - Section 2.2 Added text removed in Section 1.1. - Section 3.1.1 Added Medium Assurance Hardware Unaffiliated. - Section 3.2.3 Added TrustID Medium Assurance HW Unaffiliated. - Section 3.2.6.1 Added Cross-Certification. - Section 3.2.10 Update to reflect that the validation method for Server Certificates is being recorded. - Section 4.2 Updates on how the processing for CAA Records is handled. - Section 4.2.1 Updates to reflect how data and documents supplied for Server Certificates vetting are used and reused. - Section 6.2.1 Updates pointing to the PMA approved list of FIPS 140 Cryptographic Modules in Appendix A. - Section 7.1.5 Update to reflect that not fully Technically Constrained Subordinate CA's are publicly disclosed. - Appendix A: List of PMA approved list of FIPS 140 Cryptographic Modules.
4.5	September 27, 2019	- Updates relevant to the Network Security Controls to be line with CA/B Forum SC3 approved on 8/16/18 to be effective 04/01/2020: Sections 1.6.1; 5.4 and 5.4.8. - Updates relevant to Extended Validation 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.

Revision	Date	Summary of Changes/Comments
4.6	November 21, 2019	- OID Updates to support offering of Server Certificates for Domain Validation (DV) only, Domain Validation (DV) with Organization Validation (OV) only and Extended Validation only.
4.7	January 31, 2020	- Section 3.1.1: Updates to allow null Subject commonName for Server Certificates as long as the subjectAlternativeName extension is not null. - Section 3.1.3: Updates to allow anonymous Certificates. - Updates to support Issuance of Server Certificates to IP Addresses. - Section 5 updates. - Addition of Subordinate CA A13 as replacement for Subordinate CA A12.

1.2.1 Alphanumeric Identifier

The alphanumeric identifier (i.e., the title) for this CP is the "IdenTrust TrustID Certificate Policy, V4.7 January 31, 2020 or “identrust-trustid-cp-v4.701312020.”

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 will contain the OID listed below in the Certificate Policies field of the Certificate:

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

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

Name	Type	Policy OID
		2.16.840.1.113839.0.6.5
TrustID Server Organization Validation	SSL/TLS	2.23.140.1.2.2 2.16.840.1.113839.0.6.3
TrustID Server Extended Validation	SSL/TLS	2.23.140.1.1 2.16.840.1.113839.0.6.9
TrustID Extended Validation Code Signing	Signing	2.23.140.1.3 2.16.840.1.113839.0.6.14.1
TrustID Timestamping	Signing	2.16.840.1.113839.0.6.13.1 2.16.840.1.113839.0.6.13.3
TrustID FATCA Organization	Signing/Encryption	2.16.840.1.113839.0.6.8
Administrative CA	Signing/Encryption	2.16.840.1.113839.0.7 (arc)
Administrators	Signing/Encryption	2.16.840.1.113839.0.7.1
Registration Authorities	Signing/Encryption	2.16.840.1.113839.0.7.2
Authorized Relying Parties	Signing/Encryption	2.16.840.1.113839.0.7.3
TrustID Secure Email Software (S/MIME)	Signing/Encryption	2.16.840.1.113839.0.6.11.1
TrustID Secure Email Hardware (S/MIME)	Signing/Encryption	2.16.840.1.113839.0.6.11.2
TrustID Card Authentication Certificate	Signing/Encryption	2.16.840.1.113839.0.6.30.1
TrustID 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, with respect to 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 I&A 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.

For Certificates supporting the secure/multipurpose internet mail extensions (S/MIME) protocol, the Issuing CA must not delegate email address validation to third parties.

1.3.3 Subscribers

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

1.3.4 Authorized 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 IdenTrust Policy Management Authority (PMA)

The PMA for this Policy is 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 Authorities (CMAs)

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 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 Individual that: (i) sign and submit, or approves a request for a Certificate issued to an Electronic Device on behalf

of the Organization, and/or (ii) sign and submit a Certificate 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 Applicant's or PKI Sponsor's identification during the registration process. Trusted Agents shall not have automated interfaces with CAs.

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 a 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 Policy is owned and administered by IdenTrust Services, LLC.

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

IdenTrust shall provide a link to a webpage or an email address with contact details in case of Certificate Problem Report requests.

1.5.3 Person Determining CPS 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 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 Policy 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 change. The PMA may request that the Issuing CA notify RAs and Subscribers of the proposed changes. The PMA will also post a notice of the proposal on the PMA World Wide Web site.

1.5.5.3 Mechanism to Handle Comments

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

1.5.5.4 Final Change Notice

The PMA will determine the period for final change notice.

1.5.5.5 Items Whose Change Requires a New Policy

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

The PMA shall review and update this Policy on an annual basis or more frequently when required to include the most recent "CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", "CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates", "CA/Browser Guidelines for the Issuance and Management Of Extended Validation Code Signing Certificates", published at https://cabforum.org and/or browser's root store CA Policy.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

Term	Definition
Accept or Acceptance	An End Entity's act that triggers the End Entity's rights and obligations with respect to its TrustID Certificate under the applicable Certificate Agreement or Authorized Relying Party Agreement. Indications of Acceptance may include without limitation: • Using the TrustID Certificate (after Issuance); • Failing to notify 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 prior to creating a Digital Signature).
Affiliated Individual	An Individual having an affiliation with an Organization who has been authorized by the Organization to obtain a TrustID Certificate that identifies the Organization and the fact of the Individual's affiliation with the Organization. See "Sponsoring Organization."
Applicant	An Individual or Organization that submits application information to an RA or an Issuing CA for the purpose of obtaining or renewing a TrustID Certificate.
Application Software Supplier	A supplier of Internet browser software or other Relying Party application software that displays or uses Certificates and incorporates Root Certificates.
Authority Revocation List (ARL)	A list of revoked CA Certificates. An ARL is a CRL for CA Certificates.

Term	Definition
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	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 Certificate	A Certificate 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 in order to establish a certification chain.
CA Private Signing Key	The Private Key that corresponds to the Issuing CA's Public Key listed in its CA Certificate and used to sign TrustID Certificates.
CA Private Root Key	The Private Key used to sign CA Certificates.
Certificate	A computer-based record or electronic message that: • Identifies the Certification Authority issuing it • Names or identifies a Subscriber, Authorized Relying Party or Electronic Device • Contains the Public Key of the Subscriber, Authorized Relying Party or Electronic Device • Identifies the Certificate's Validity Period • Is Digitally Signed by a Certification Authority • 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	The contract between a Subscriber and the CA and/or RA that details the procedures, rights, and obligations of each party with respect to a TrustID Certificate issued to the Subscriber.
Certificate Chain	A Certificate Chain is a series of Certificates connecting a Subscriber's Certificate to the Root Certificate. Successive and superior CA and Subordinate CA Certificates up to the Root Certificate connect superior Certificates (which may be self-signed) in a Certificate Chain. For Subscribers under this CP, a self-signed Root Certificate is issued in compliance with this Policy.
Certificate Holder	An Individual or Organization that: • Is named or identified in a TrustID Certificate, or is responsible for the Electronic Device named, as the Subject of the TrustID Certificate; and • Holds a Private Key that corresponds to the Public Key listed in that TrustID Certificate. However, for purposes of interpreting this Policy, persons holding Certificates for administrative purposes (e.g., the subject of an Authorized Relying Party Certificate used to access a Repository to verify Certificate status) will not be considered "Certificate Holders" with respect to Certificates issued under this Policy.

Term	Definition
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 prior to Certificate Issuance, the Certificate Profile, and other allowed uses of Certificates.
Certificate Problem Report	Complaint of suspected Private Key compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
Certificate Profile	The protocol used in the Certificate, CRL and OCSP Profiles section of this Policy, 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 Revocation List (CRL)	A database or other list of Certificates that have been revoked prior to 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 entity that creates, issues, manages and revokes Certificates. See also Issuing CA.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in creating, issuing, managing and revoking Certificates.
Common Vulnerability Scoring System (CVSS)	A quantitative model used to measure the base level severity of a vulnerability (see http://nvd.nist.gov/home.cfm).
Compliance Inspector	A natural person or Legal Entity that meets the requirements of Identity/Qualifications of Assessor.
Critical Vulnerability	A system vulnerability that has a CVSS score of 9.0 or higher according to the NVD or an equivalent to such CVSS rating (see http://nvd.nist.gov/home.cfm), or as otherwise designated as a Critical Vulnerability by the CA or the CA/Browser Forum.
Cross-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].

Term	Definition
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.
End Entity(ies)	Subscribers and Authorized Relying Parties.
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 are publically disclosed and independently audited with publically available reports. They are contractually bound to other obligations by the Issuing CA and bound to comply with Application Software Supplier programs.
Fully-Qualified Domain Name (FQDN)	A Domain Name that includes the 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 Legal Entity, the existence of which was established by the government of a nation or a political subdivision thereof and is owned or controlled by such government or political subdivision.
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.
Identification and Authentication (I&A)	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.
Internal Name	A string of characters (not an IP Address) in a commonName or subjectAlternativeName field of a Certificate that cannot be verified as globally unique within the public DNS at the

Term	Definition
	time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.
Internet	The Internet is a global system of interconnected computer networks that uses multiple protocols to communicate data.
Internet Protocol (IP)	The primary protocol in the Internet Layer defined by the Request for Comment 1122 (RFC 1122) - *Requirements for Internet Hosts -- Communication Layers*, Internet Engineering Task Force, R. Braden, October 1989. The IP has the task of delivering datagrams from the source host to the destination host solely based on the addresses.
IP Address or IP Addresses	A 32-bit or 128-bit label assigned to a device that uses the Internet Protocol for communication.
Issue Certificates/ Issuance	The act performed by a CA in creating a Certificate, listing itself as "Issuer," and notifying the Applicant 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 Policy.
Key	A general term used throughout this Policy to encompass any one of the defined keys mentioned in this document.
Key Generation	The process of creating a Key Pair.
Key Pair	Two mathematically related Keys (a Private Key and its corresponding Public Key), having the properties that: • 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 unfeasible 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.
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.
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 http://nvd.nist.gov/home.cfm).
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.
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.

Term	Definition
OWASP Top Ten	A list of application vulnerabilities published by the Open Web Application Security Project (see https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).
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 escorted 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).
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 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 Certificate Agreement on behalf of the Organization, and/or • Acknowledges and agrees to the Certificate Terms of Use on behalf of the Organization when the Organization is an affiliate of the CA. See 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, implementing and administering Policy decisions regarding this Policy.
Private Key	The Key of a Key Pair kept secret by its holder, used to create Digital Signatures and to decrypt messages or files that were encrypted with the corresponding Public Key.
Public Key	The Key of a Key Pair publicly disclosed by the holder of the corresponding Private Key and used by the recipient to validate Digital Signatures created with the corresponding Private Key and to encrypt messages or files to be decrypted with the corresponding Private Key.
Public Key Cryptography	A type of cryptography also known as asymmetric cryptography that uses a Key Pair to securely encrypt and decrypt messages.

Term	Definition
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based Public Key Cryptography system.
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 an 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 circumstances that were known or should have been known to the Authorized Relying Party prior to reliance. An Authorized Relying Party bears all risk of relying on a TrustID Certificate while knowing or having reason to know of any facts that would cause a person of ordinary business prudence to refrain from relying on the Certificate).
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)	An entity contractually delegated by an Issuing CA to Accept and process Certificate applications, and to verify the identity of potential End Entities and authenticate information contained in Certificate applications, in conformity with the provisions of this Policy and related agreements.
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 I&A on potential End Entities.
Repository	An online system maintained by an Issuing CA for storing and retrieving Certificates and other information relevant to Certificates, including information relating to Certificate validity or Revocation.
Relying Party	A person or Legal Entity who has received information that includes a Certificate and a Digital Signature verifiable with reference to a Public Key listed in the Certificate, and is in a position to rely on them (see section 1.3.4).
Reserved IP Address	An IPv4 or IPv6 address that the IANA has marked as reserved: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
Restricted Zones	Any one of: • An Operations Zone; • A Security Zone; and • A High Security Zone.

Term	Definition
Revocation	The act of making a Certificate permanently ineffective from a specified time forward. Revocation is effected by notation or inclusion in a set of revoked Certificates or other directory or database of revoked Certificates (e.g., inclusion in a CRL).
Root CA Certificate	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 http://www.sans.org/top25-software-errors/).
Secure Email Certificate	A Certificate issued to an email address over which the Certificate Applicant demonstrates control to the RA by the Certificate Applicant responding to a unique challenge sent during the authentication process conducted prior to Issuance. A Secure Email Certificate can be used for the purposes of email signing, email encryption, and client authentication, when installed in on 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 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."

Term	Definition
Sponsoring Organization Authorization Form	The form used to provide information about an Affiliated Individual who will be authorized by an Organization to hold a TrustID Certificate.
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
Subject Name	The specific field in a Certificate containing the unique name-identifier for the Subscriber.
Subordinate CA	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
Subordinate CA Certificate	A Certificate that is signed by the IdenTrust Root CA or other Subordinate CA's within the IdenTrust Root Chain. Subordinate CA Certificates and their corresponding Public Keys may be embedded into software obtained or downloaded by the affirmative act of an Authorized Relying Party in order to establish a certification chain within the TrustID PKI hierarchy.
Subscriber	See Certificate Holder.
Technically Constrained Subordinate CA	A Subordinate CA Certificate, which uses a combination of extended Key usage settings and name constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates. The anyExtendedKeyUsage KeyPurposeID shall not appear in the EKU extension of any publically trusted Certificates.
Token	A Cryptographic Module consisting of a hardware object (e.g., a "smart card"), often with memory and a microchip.
Trusted Agent(s)	Entity authorized to act as a representative of a Sponsoring Organization in verifying Applicant or PKI Sponsor identification during the registration process. Trusted Agents do not have automated interfaces with CAs. See Trusted Agents.
Trusted Platform Module (TPM)	An international standard for a secure crypto-processor, which is a dedicated microprocessor designed to secure hardware by integrating cryptographic keys into devices.
Trusted Role	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.
Unaffiliated Individual	An Individual not attached or associated with an Organization and wishes to obtain a TrustID Certificate to verify his/her identity and/or an email address.
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

Term	Definition
	network and the presence of vulnerabilities listed in the NVD, OWASP Top Ten, or SANS Top 25.

1.6.2 Acronyms

Acronym	Definition
AO	Authorizing Officer
ARL	Authority Revocation List
CA	Certification Authority
CAA	Certification Authority Authorization
CMA	Certificate Manufacturing Authority
CMS	Card Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
DBA	Doing Business As
DN	Distinguished Name
DSA	Digital signature algorithm
EV	Extended Validation
FATCA	Foreign Account Tax Compliance Act
FIPS	Federal Information Processing Standard (US Government)
gTLD	General Top Level Domain
I&A	Identification and Authentication
ISO	International Standards Organization
ITU	International Telecommunications Union
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number (e.g., a password)
PKCS	Public Key Cryptography Standard

Acronym	Definition
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PMA	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
SHA	Secure Hashing Algorithm
TPM	Trusted Platform Module
URL	Uniform Resource Locator
VBA	Visual Basic Application
X.500	The ITU-T (International Telecommunication Union-T) standard that establishes a distributed, hierarchical directory protocol organized by country, region, Organization, etc.
X.501	The ITU-T (International Telecommunication Union-T) standard for use of Distinguished Names in an X.500 directory.
X.509	The ITU-T (International Telecommunication Union-T) standard for Certificates. X.509, version 3, refers to Certificates containing or capable of containing extensions.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The Issuing CA will perform the role and functions of the Repository. The Issuing CA may subcontract 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

2.2 PUBLICATION OF CERTIFICATION INFORMATION

Each Issuing CA will operate or cause the operation of a secure online Repository that is available to Authorized Relying Parties and that contains:

- A CRL or OCSP
- The Issuing CA's CA Certificate for its CA Private Signing Key
- Past and current versions of the Issuing CA's CPS

- A copy of this Policy
- Other relevant information relating to TrustID Certificates.

This CP conforms with and is compliant with the latest published versions of CA/B Forum and the Mozilla Root Store Policy.

- The “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” published at https://cabforum.org
- The “CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates” published at https://cabforum.org
- The “CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates” published at https://cabforum.org
- The “Mozilla Root Store Policy” published at https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/

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

2.3 TIME OR FREQUENCY OF PUBLICATION

TrustID Certificates are published following Acceptance of the TrustID Certificate by the Subscriber, in accordance with the procedure specified in section 4.4. If the Issuing CA elects to publish CRLs, the CRLs will be published as specified in section 4.10.

2.4 ACCESS CONTROLS ON REPOSITORIES

The Issuing CA will not impose any access controls on:

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

The Issuing CA may impose 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 it 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 subjectAlternativeName extension, then the Subject Name must be an empty sequence and the subjectAlternativeName extension must include the FQDN and must be flagged as critical.

The Issuing CA is responsible for performing the I&A of End Entities prior to the Issuance of TrustID Certificates. The Issuing CA may perform I&A itself, or may designate one or more persons to act as RA. RAs may designate one or more employees or agents, to be referred to as Local Registration Agents, to perform I&A in accordance with this section 3:

Table 3 - TrustID Certificates Identity Authentication Requirements

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

Certificate Type	Identification Requirements
	Demonstration that the Applicant of the Certificate had control of the Applicant provided email address at the time of email verification, based on Secure Email Certificate.
TrustID Serve Domain Validation	Identity for Domain Validation (DV) Server Certificates are all be established by validating authorization and/or ownership by Domain Name Registrant and verification of the Subject identity information (i.e., identity, DBA/Tradename, authenticity of Certificate Request, verification of Individual Applicant, verification of country), in each case based on the applicable requirements set forth in The "CA/Browser Forum Guidelines for the Issuance and Management of Publicly-Trusted Certificates" published at https://cabforum.org.
TrustID Server Organization Validation	Identity for Organization Validation (OV) Server Certificates is established by performing the validations described above for DV Server Certificates, as well as validation of the organization as a legal entity, as well as the locality/city, state and country of the organization.
TrustID Server Extended Validation	Identity for Extended Validation (EV) Server Certificates is established by performing the validations described above for OV Server Certificates, as well as validation of the legal existence of the organization including attributes such as business category, jurisdiction, registration id, etc., as set forth in the "CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates" published at https://cabforum.org.
TrustID Extended Validation Code Signing	Identity shall be established by: Verification of the Applicant's Organization in accordance with Extended Validation Code Signing and Time-Stamping Certificates as set forth in the "CA/Browser Guidelines for the Issuance and Management Of Extended Validation Code Signing Certificates" published at https://cabforum.org
TrustID Time-Stamping	Identity shall be established by: Verification of the Applicant's Organization in accordance with Extended Validation Code Signing and Time-Stamping Certificates.
TrustID 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, applications should be submitted by first class U.S. mail or in person.

3.1.2 Need for Names to Be Meaningful

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

Certificate Type	Naming Requirements
TrustID Personal	The DN must include an authenticated commonName must be a combination of first name, surname, and optional initials.

Certificate Type	Naming Requirements
TrustID Medium Assurance Hardware Unaffiliated	
TrustID Business	In addition to the authenticated commonName (as described above), the DN must also include the authenticated legal Subscribing Organization name in organizationName. Optionally, the organizationUnitName may be used to name the Subscribing Organization unit/department that is associated with the subscriber, if provided by the Subscriber.
Administrative CA for Administrators and Registration Authorities	Same as TrustID Business.
Administrative CA for Authorized Relying Parties	Same as TrustID Business.
TrustID FATCA Organization	Same as TrustID Business.
TrustID 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.
TrustID Device	The DN for a must include a unique name populated in commonName that identifies the electronic Device that will contain the associated Cryptographic Module.
TrustID Server Domain Validation	It is allowable for the DN to be empty. CA/B Forum discourages, but does not prohibit the use of DN. Where the DN is empty then the FQDN or a single IP Address must be named in the subjectAlternativeName and must be flagged as critical. In the case where the DN is not empty, then the validated FQDN must be included in the commonName.
TrustID Server Organization Validation	It is allowable for the DN to be empty. CA/B Forum discourages, but does not prohibit the use of DN. Where the DN is empty then the FQDN must be named in the subjectAlternativeName and must be flagged as critical. In the case where the DN is not empty, then the validated FQDN must be included in the commonName.
TrustID Server Extended Validation	It is allowable for the DN to be empty. CA/B Forum discourages, but does not prohibit the use of DN. If present, this field 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 CA/B Forum Baseline Requirements
TrustID Extended Validation Code Signing	The DN must include the authenticated legal Subscribing Organization name in commonName.

Certificate Type	Naming Requirements
	The DN must also include the authenticated legal Subscribing Organization name in organizationName. Optionally, the organizationUnitName may be used to name the Subscribing Organization unit/department that is associated with the subscriber, if provided by the Subscriber.
TrustID Time-Stamping Authority	Time Stamping Authority Certificates are issued to IdenTrust and used in conjunction with the Timestamping 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".
TrustID Card Authentication	TrustID Card Authentication Certificates must include a unique name for identifying the associated Cryptographic Module.

3.1.3 Anonymity or Pseudonymity of Subscribers

For human subscribers, CA Certificates shall not contain anonymous or pseudonymous identities.

DV SSL/TLS, 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.

3.1.5 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 are

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

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 appropriate 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).

3.2.2 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 I&A 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 I&A is performed by an RA, the RA will conduct I&A in accordance with its “Know Your Customer” Policy or other similar procedures, which may include a review of official government records 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
- Type of entity
- Year of formation
- Names of directors and officers
- Address
- Telephone number and
- Proof of good standing in the jurisdiction where the Applicant is incorporated or otherwise organized.

Organization information should also be verified by cross-checking it with trusted information in a data base 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 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.

3.2.3 Authentication of Individual Identity

The Issuance of a TrustID Certificate will be based on I&A performed by the CA or 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 4 - TrustID Certificates Individual Identity Authentication Requirements

Certificate Type	Description
TrustID 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 I&A; or Contemporaneous in-person identification consisting 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.
TrustID Medium Assurance Hardware Unaffiliated	Identity shall be established by: Contemporaneous in-person identification consisting 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.
TrustID Business	Sponsoring Organization confirms the Affiliated Individual's affiliation with the Sponsoring Organization.

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 to an Organization is confirmed as explained below in section 3.2.3. For those cases where there are several Individuals acting in one capacity, a Certificate may be issued in the Organization's name. In these cases, such Organizational Certificate may only be issued after the Issuing CA has performed I&A 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 I&A process as explained above

3.2.3.1 Acceptable Forms of Identification Documents

All Individuals seeking Issuance of a TrustID Certificate who apply in person must present satisfactory proof of identity.

- The following are considered by this Policy to be acceptable "Government-issued photo IDs" for in-person I&A (all photo IDs must be currently valid (i.e., unexpired) at the time of presentment by the Applicant for in-person identification):

  - 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

- 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 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 Performance of In-Person Identification

In-person identification may 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.)

All information submitted by the Applicant for in-person identification 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 a signed communication (in writing or digitally) indicating that the Applicant was properly identified.

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

3.2.3.3 Attestation 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.

3.2.3.4 Performance of 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 high-correlation of an identity-proofing algorithm, and they are completed automatically. No paper forms are necessary in this case.

To meet the requirements for completing the identity-proofing algorithm an Applicant must provide at least one of 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 I&A

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 I&A 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

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.

3.2.4 Non-verified Subscriber Information

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

3.2.5 Validation of Authority and Other Attributes

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.

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 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 from 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 data base 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 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 Verification of Email address

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

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 Authentication of Device Identity

A TrustID Certificate request identifying an Electronic Device as the Subject of a Certificate may only be made by a human sponsor of an approved End Entity for whom the Electronic Device's signature is attributable for the purposes of accountability and responsibility. When issuing a TrustID Certificate identifying an Electronic Device as the Subject of the Certificate, the Issuing CA shall conform with the applicable provisions in the “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” published at https://cabforum.org ; provided, however, when such Certificate is an Extended Validation SSL/TLS Certificate, the Issuing CA shall conform with the applicable provisions of the “CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates” published at https://cabforum.org.

A TrustID Certificate identifying an Electronic Device as the Subject of the Certificate can only be issued by an Issuing CA that can ensure accomplishment of the I&A required by this section.

For Server Certificates, Domain or IP Address validation must not be delegated to third parties and after July 31, 2019, the Issuing CA shall maintain a record of which of the domain or IP Address validation methods below, including the relevant CA/B Forum Baseline Requirements version number used to validate every domain or IP Address.

3.2.10.1 Secure Email Certificate

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 and can only be issued after the CA or RA confirms that the Applicant can demonstrate control of the email address, which is to be contained in the Certificate, at the time that email verification is performed by the Issuing CA or RA.

Control of the email address shall be demonstrated via a process that:

- Is conducted in an automated fashion, in which a system generated email is sent to the Certificate Applicant, using the email address to be included in the Certificate
- Such email shall contain a unique, system generated code that will be used for email confirmation and the URL of an email confirmation website
- That the recipient of such automated email shall confirm receipt of the email by visiting the aforementioned URL and by supplying the unique, system-generated code provided in automated email and the Applicant provided Account Password supplied during the Certificate Application and
- Successful verification of the unique, system generated code and the Applicant provided Account Password against the CA database.

Confirmation of the Applicant's identity is not performed for this type of Certificate.

3.2.10.2 TrustID Card Authentication Certificate

The TrustID Card Authentication Certificate can be used for the purposes of identifying a Cryptographic Module and can only be issued after the CA or RA assigns a unique name-identifier to the relevant Cryptographic Module and such unique name-identifier is at a minimum to be contained in Subject Name of the TrustID Card Authentication Certificate issued to the Cryptographic Module.

3.2.10.3 TrustID Device Certificate

The TrustID Device Certificate can be used for the purposes of identifying an Electronic Device containing a Cryptographic Module, encrypting data to and from the Electronic Device, encrypting data residing on the Electronic Device, and detecting changes to data residing on the Electronic Device. A TrustID Device Certificate can only be issued after the CA or RA or Applicant authenticates an Electronic Device and assigns it a unique name-identifier. Such unique name-identifier is to be contained in the Subject Name of the TrustID Device Certificate issued to the Electronic Device containing the Cryptographic Module storing the corresponding Key Pair.

3.2.11 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.

3.2.12 Authentication of Other Certificates

3.2.12.1 Extended Validation Code Signing and Time-Stamping Certificates

A TrustID Extended Validation Code Signing Certificate or TrustID Time-Stamping Certificate identifies an Organization as the Subject of a Certificate and such Organization is attributable for the purposes of accountability and responsibility for signatures created by the Organization to be used to verify the integrity of its code. When issuing either TrustID Extended Validation Code Signing Certificate or TrustID Time-Stamping Certificate, the Issuing CA shall conform with the applicable provisions set forth in the "CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates" published at https://cabforum.org. .

3.2.13 Authorized Relying Parties

I&A 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.

3.3 IDENTIFICATION AND AUTHENTICATION

3.3.1 Identification and Authentication for Routine Re-Key

3.3.1.1 Certificate Re-key

As long as an End Entity's TrustID Certificate has not been revoked, the End Entity may, within three months prior to 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.

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 an 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 I&A 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 on the basis of 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 Policy is not intended to impose implementation requirements on the Issuing CA or End Entities. However, this Policy does identify the required information and procedures that constitute assurance and support trust in the 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) establish identity of Subject (per section 3); (ii) obtain a Key Pair for each TrustID Certificate required; (iii) prove to the Issuing CA that the Public Key forms a functioning Key Pair with the Private Key held by the End Entity; and (iv) provide a point of contact for verification of any roles or authorizations requested.

4.1.1 Who Can Submit a Certificate Application

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

4.1.1.2 Business Certificates

4.1.2 Enrollment Process and Responsibilities

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

4.1.3 Enrollment Process / Bulk Loading

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.

4.1.4 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 a LRA to responsible to approve 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.

Effective September 8, 2017, 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 for each dNSName in the subjectAlternativeName extension of the Certificate to be issued, as specified in RFC 6844 as amended by Errata 5065 (Appendix A).

4.2.1 Performing Identification and Authentication Functions

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 Certificate 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.

For Server Certificates, effective March 1, 2018, 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 825 days 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 a LRA to responsible to approve Certificate applications.

The Issuing CA and RAs approve an Applicant/PKI Sponsor Certificate application if the I&A processes described in section 3.2 and 3.3 are completed successfully.

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 and
- Make the TrustID Certificate available to the Applicant for Acceptance.

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 in 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 that 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 I&A 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 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 Certificate 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 I&A 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 Certificate 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 TrustID CP and only in a manner consistent with this TrustID CP;
- 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 other compromise of the Private Key, or, in the case of Business Representative, whenever the Subscriber is no longer affiliated with the Sponsoring Organization; and
- Responds as required to notices issued by 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 Certificate Agreement online or in paper copy; or, by undergoing a full registration process prior to receiving the Certificate. Additional information concerning the rights and obligations of Subscribers 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 TrustID CP or by the 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 TrustID CP or the 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 authorizations 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[1] 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.

[1] Effective March 1, 2018, Server Certificates had a maximum Validity Period of 825 days and effective April 20, 2018, must not exceed 815 days.

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

Three months prior to the expiration period, the Issuing CA or the RA's system will automatically notify the Subscriber that he or she must Re-key and re-establish identity by presenting his or her valid TrustID Certificate.

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 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 Identification and Authentication and Who can submit a Certificate application 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 replaces the Certificate and records all of the Certificate replacement transaction data.

4.8.4 Notification of New Certificate Issuance to Subscriber

Upon successful completion of the Subscriber I&A process explained in section 3.2.3, and prior to 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 records 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 I&A 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 publication of the TrustID Certificate in a recognized Repository.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

Prior to revoking a 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 one or more of the following events take place:

- The Subscriber requests written Revocation.
- The Subscriber notifies the Issuing CA that the original Certificate request was not authorized.
- The Issuing CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate it was compromised.
  The Issuing CA obtains evidence that the validation of domain authorization or control for any FQDN or IP Address in the Certificate should not be relied upon.

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

- The Certificate no longer complies with the requirements in the relevant section of the CA/B Forum Baseline Requirements.
- The Issuing CA obtains evidence that the Certificate was misused.
- The Subscriber or the cross-certified CA breached a material obligation under this CP, the TrustID CPS, or the relevant agreement.

- For Server Certificates, the Issuing CA confirms any circumstance indicating that use of a FQDN or IP Address in the Certificate is no longer legally permitted.
- For Server Certificates the Issuing CA confirms that a wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN.
- For Extended Validation Code Signing Certificates, the Certificate has been used to sign, publish or distribute malware, downloaded without user consent or other malicious purpose.
- The Issuing CA confirms a material change in the information contained in the Certificate.
- The Issuing CA confirms that the Certificate was not issued in accordance with the CA/B Forum Baseline Requirements, this CP or IdenTrust TrustID CPS.
- The Issuing CA determines or confirms that any of the information appearing in the Certificate is inaccurate.
- The Issuing CA's right to issue Certificates under the CA/B Forum Baseline Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository.
- Revocation is required by the Issuing CA CP or CPS.
- The Issuing CA confirms a demonstrated or proven method that exposes the Subscriber's Private Key to compromised methods or if there is clear evidence that the specific method used to generate the Private Key was flawed.

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

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

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

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

- The Subordinate CA requests Revocation in writing.
- The Subordinate CA notifies the Issuing CA that the original Certificate request was not authorized and does not retroactively grant authorization.
- 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 Baseline Requirements.
- The Issuing CA obtains evidence that the CA Certificate was misused.
- 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.

- The Issuing CA determines that any of the information appearing in the CA Certificate is inaccurate or misleading.
- 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.
- The Issuing CA or the Subordinate CA's right to issue Certificates under the CA/B Forum Baseline Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository.
- Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.
- The technical content or format of the CA Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

4.9.2 Who Can Request Revocation

Different parties may request Certificate Revocation as follows:

- The Issuing CA may summarily revoke Certificates within its domain.
- An RA can request the Revocation of an End Entity's TrustID Certificate on behalf of the End Entity, the Sponsoring Organization, or other authorized party, or on its own behalf.
- An End Entity is authorized to request the Revocation of his, her, or its own 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

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-SSL/TLS Certificate prior to making a determination on whether to revoke it. Promptly following 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 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 SSL/TLS Certificates, under other circumstances specified in the applicable CA/B Forum Baseline Requirements 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 information contained in the Certificate has changed; or if the Subordinate Certificate can issue SSL/TLS Certificates, under other circumstances specified in the applicable CA/B Forum Baseline Requirements. 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 Baseline Requirements section.

4.9.6 Revocation Checking Requirement for Relying Parties

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

CRLs will be issued at least weekly, even if there are no changes or updates to be made, to ensure timeliness of information. If there are circumstances under which the Issuing CA will post early updates, these will be spelled out in a CPS or in the Authorized Relying Party Agreements used by the Issuing CA. The Issuing CA will ensure that superseded CRLs are removed from the directory system upon posting of the latest CRL.

4.9.7.1 CRL Checking Requirements

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

4.9.8 Maximum Latency for CRLs

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 TrustID Certificates, the Issuing CA will validate online, near-real-time the status of the TrustID Certificate indicated in a Certificate validation request message.

4.9.10 Online Revocation Checking Requirements

When an Issuing CA provides an online Certificate status database as a method of verifying the validity and status of TrustID Certificates, the Authorized Relying Parties who rely on an online Certificate status database must:

- Validate a TrustID Certificate with such database before relying on the Certificate and
- Log the validation request.

Failure to do so negates the ability of the Authorized Relying Party to claim that it acted on the TrustID Certificate with Reasonable Reliance.

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 Re-Key Compromise

When either an Issuing CA's or External CA's (i.e., Subordinate or Root) Certificate or Subscriber's Certificate is revoked because of compromise, or suspected compromise, of a Private Key, a CRL will be issued as soon as possible. Practices followed in the case of a CA Private Key compromised are explained in section 5.7.6 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. This risk evaluation is at the discretion of the LRA (for Human Certificates) based on the situation and information available at the time.

Suspension shall not be available for SSL/TLS or FATCA Organization Certificates and the Repository must not include these Certificate types in 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 TrustID 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. In order to effect a suspension, minimal identity validation may be required depending upon the circumstances (source of the request, circumstances for the request, etc.) and when completed, 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 uses 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 EV Code Signing Certificates, which shall remain on the CRL for at least 10 years after 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

TrustID Certificates issued by the Issuing CA shall contain pointers to locations where Certificate-related information is published including CRLs, as specified in CRL Issuance Frequency for the frequency of publication of the Issuing CA Repository. CRLs are available only for Subordinate CA Certificates and Root CA Certificates issued prior to March 1, 2014.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

4.11.1 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 SECURITY 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 those 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 plain 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.

A security check to the facility housing Issuing CA equipment will occur at least once every 24 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 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 practice. 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 practice. 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 so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit archive, 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, prior to disposal.

5.1.8 Offsite Backup

System backups, sufficient to recover from system failure, will be made on a periodic schedule, described in the CPS. At least one backup copy will be stored at an offsite location (separate from the Issuing CA equipment). Only the latest backup need 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 *CA-Browser-Forum-Network-Security-Controls-v1.3* found at: https://cabforum.org/wp-content/uploads/CA-Browser-Forum-Network-Security-Controls-v1.3.pdf

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 maintains strict separation-of-duties/multi-party controls for its Trusted Roles.

5.3 PERSONNEL SECURITY 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 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 (prior to 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.

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 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 Physical Access.

5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role will be provided to the personnel filling 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 Issuing CA equipment will be able to record events related to the server (installation, modification, accesses), and the application (requests, responses, actions, publications, and error conditions). Events may be attributable to human action (in any role) or automatically invoked by the equipment. At a minimum, the information recorded will include the type of event, and the time the event occurred. In addition, for some types it will be appropriate to record the success or failure, the source and destination of a message, or the disposition of a created object (e.g., a filename). Where possible, the audit data will be automatically collected; when this is not possible a logbook, paper form, or other physical mechanism will be used. The auditing capabilities of the underlying equipment operating system will be enabled during installation. A record will be kept of file manipulation and account management. These events will also be recorded during normal operation of the Issuing CA equipment.

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 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 or Delegated Third Party Trusted Roles 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 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

Issuing CA archive records will be detailed enough to establish the validity of a signature and of the proper operation of the PKI. At a minimum, the following data will be recorded and archived:

Table 5 - TrustID Certificates Data to Be Archived

AUDITABLE EVENT			
SECURITY AUDIT	**CA**	**CSA**	**RA**

AUDITABLE EVENT			
Any changes to the audit parameters (e.g., audit frequency, type of event audited)	X	X	X
Any attempt to delete or modify the audit logs	X	X	X
Obtaining a third-party time-stamping	N/A	N/A	N/A
IDENTITY PROOFING	**CA**	**CSA**	**RA**
Successful and unsuccessful attempts to assume a role	X	X	X
The value of maximum number of authentication attempts is changed	X	X	X
Maximum number of authentication attempts occur during user log in	X	X	X
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X	X
An administrator changes the type of authenticator (e.g., from a password to a biometric)	X	X	X
LOCAL DATA ENTRY	**CA**	**CSA**	**RA**
All security-relevant data that is entered in the system	X	X	X
REMOTE DATA ENTRY	**CA**	**CSA**	**RA**
All security-relevant messages that are received by the system	X	X	X
DATA EXPORT AND OUTPUT	**CA**	**CSA**	**RA**
All successful and unsuccessful requests for confidential and security-relevant information	X	X	X
KEY GENERATION	**CA**	**CSA**	**RA**
Whenever the component generates a Key (not mandatory for single session or one-time use symmetric Keys)	X	X	X
PRIVATE KEY LOAD AND STORAGE	**CA**	**CSA**	**RA**
The loading of Component Private Keys	X	X	X
All access to Certificate Subject Private Keys retained within the CA for Key recovery purposes	X	N/A	N/A
TRUSTED PUBLIC KEY ENTRY, DELETION, AND STORAGE	**CA**	**CSA**	**RA**
All changes to the trusted component Public Keys, including additions and deletions	X	X	X
SECRET KEY STORAGE	**CA**	**CSA**	**RA**
The manual entry of secret Keys used for authentication	X	X	X
PRIVATE AND SECRET KEY EXPORT	**CA**	**CSA**	**RA**

AUDITABLE EVENT			
The export of private and secret Keys (Keys used for a single session or message are excluded)	X	X	X
CERTIFICATE REGISTRATION	**CA**	**CSA**	**RA**
All Certificate requests: Issuance; validation and renewal	X	N/A	X
CERTIFICATE REVOCATION	**CA**	**CSA**	**RA**
All Certificate Revocation requests	X	N/A	X
CERTIFICATE STATUS CHANGE APPROVAL	**CA**	**CSA**	**RA**
The approval or rejection of a Certificate status change request	X	N/A	N/A
COMPONENT CONFIGURATION	**CA**	**CSA**	**RA**
Any security-relevant changes to the configuration of a component system	X	X	X
ACCOUNT ADMINISTRATION	**CA**	**CSA**	**RA**
Roles and users are added or deleted	X	-	-
The access control privileges of a user account or a role are modified	X	-	-
CERTIFICATE PROFILE MANAGEMENT	**CA**	**CSA**	**RA**
All changes to the Certificate Profile	X	N/A	N/A
CERTIFICATE STATUS AUTHORITY MANAGEMENT	**CA**	**CSA**	**RA**
All changes to CSA profile (e.g., OCSP profile)	N/A	X	N/A
REVOCATION PROFILE MANAGEMENT	**CA**	**CSA**	**RA**
All changes to the Revocation profile	X	N/A	N/A
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT	**CA**	**CSA**	**RA**
All changes to the Certificate Revocation List profile	X	N/A	N/A
MISCELLANEOUS	**CA**	**CSA**	**RA**
A message from any source received by the CA requesting an action related to the operational state of the CA	X	-	-
Appointment of an Individual to a Trusted Role	X	X	X
Appointment of an Individual to a multi-person Role	X	-	N/A
Installation of the Operating System	X	X	X
Installation of the PKI Application	X	X	X
Installation of Hardware KSMs	X	X	X
Removal of KSMs	X	X	X

AUDITABLE EVENT			
System Startup	X	X	X
Logon attempts to PKI application	X	X	X
Receipt of hardware / software	X	X	X
Attempts to set passwords	X	X	X
Attempts to modify passwords	X	X	X
Back up of the internal CA database	X	-	-
Restoration from back up of the internal CA database	X	-	-
File manipulation (e.g., creation, renaming, moving)	X	-	-
Posting of any material to a Repository	X	-	-
Access to the internal CA database	X	X	-
All Certificate compromise notification requests	X	N/A	X
Loading KSMs with Certificates	X	N/A	X
Shipment of KSMs	X	N/A	X
Zeroizing KSMs	X	N/A	X
Re-Key of the Component	X	X	X
CONFIGURATION CHANGES	**CA**	**CSA**	**RA**
Hardware	X	X	-
Software	X	X	X
Operating System	X	X	X
Patches	X	X	-
Security Profiles	X	X	X
PHYSICAL ACCESS / SITE SECURITY	**CA**	**CSA**	**RA**
Personnel Access to room housing to component	X	-	-
Access to a component – logged through a combination of automatic and manual logs based on the type of component and type of access	X	X	-
Known or suspected violations of physical security	X	X	X
ANOMALIES	**CA**	**CSA**	**RA**
Software error conditions	X	X	X
Software check integrity failures	X	X	X
Receipt of improper messages	X	X	X

AUDITABLE EVENT			
Misrouted messages	X	X	X
Network attacks (suspected or confirmed)	X	X	X
Equipment failure	X	-	-
Electrical power outages	X	-	-
Uninterruptible Power Supply (UPS) failure	X	-	-
Obvious and significant network service or access failures	X	-	-
Violations of Certificate Policy	X	X	X
Violations of Certification Practice Statement	X	X	X
Resetting Operations System clock	X	X	X

5.5.2 Retention Period for Archive

Archive records will be kept for a period of at least seven years, six months without any loss of data. 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 archive retention period, 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 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 prior to 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 other 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 prior to 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

The Issuing CA shall 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 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 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 its own 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 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.

5.7.7 Entity Private Key is Downgraded

In the event of the need for the downgrade of an Issuing CA's CA Certificate, the Issuing CA must immediately notify all interested parties including the PMA, other CAs with whom it cross-certified, all RAs and all Subscribers.

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.

6.1.2 Private Key Delivery to Subscriber

In most cases, a Private Key will be generated and remain within the crypto boundary of the Cryptographic Module. If the owner of the Cryptographic Module generates the Key, then there is no need to deliver the Private Key. If a Key is not generated by the intended Key holder, then the person generating the Key in the Cryptographic Module (e.g., “smart card”) must securely deliver the Cryptographic Module to the intended Key holder. Accountability for the location and state of the Cryptographic Module must be maintained until delivery and possession occurs. The recipient will acknowledge receipt of the Cryptographic Module to the Issuing CA or the RA. If the End Entity generates the Key, and the Key will be stored by and used by the application that generated it, or on a hardware Token in the possession of the End Entity, no further action is required. If the Key must be extracted for use by other applications or in other locations, a protected data structure (such as defined in [PKCS#12]) will be used. The resulting file may be kept on a magnetic medium or transported electronically. See Activation Data Generation and Installation.

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 Certificate 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 prior to 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 IETF PKIX Part 3, or other appropriate mechanism.

6.1.5 Key Sizes

Minimum Key length for other than elliptic curve base algorithm is 2048 bits. Minimum Key length for elliptic curve group algorithm is 256 bits.

6.1.6 Public Key Parameters Generation and Quality Checking

6.1.6.1 Public Key Parameters Generation

The Issuing CA that utilizes the DSA must generate parameters in accordance with the current FIPS 186 version. ECDSA must be utilized in accordance with ANSI Standard X9.62.

6.1.6.2 Parameter Quality Checking

Parameters for DSA will be checked as specified in the current FIPS 186 version

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 PKIX-1 Certificate and CRL Profile. One of the following Key Usage values must be present in all Certificates: (i) Digital Signature; or (ii) Non-Repudiation. One 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 use of protocols (like the Secure Sockets Layer) that provide authenticated connections using Key management Certificates.

6.1.8 Hardware/Software Key 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.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Each PKI Service Provider must protect its Private Key(s) in accordance with the provisions of this Policy.

6.2.1 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), TrustID Extended Validation Code Signing, TrustID Time-Stamping and Signing Authority Certificates shall be issued on hardware Cryptographic Modules validated to meet at minimum the 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.

6.2.2 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.

6.2.3 Private Key Escrow

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

6.2.4 Private Key Backup

A Participant may optionally back-up his, her, or its own Private Key. If so, the Key must be copied and stored in encrypted form and protected at a level no lower than stipulated for the primary version of the Key.

6.2.5 Private Key Archival

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.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

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 one Cryptographic Module to another, the Private Key must be encrypted during transport. Private Keys must never exist in plain text form outside the Cryptographic Module boundary.

6.2.7 Private Key Storage on Cryptographic Module

The Issuing CA and CSA Private Keys must be stored in FIPS 140-1/2 level 3 Modules.

6.2.8 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.

6.2.9 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.

6.2.10 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.

6.2.11 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 one 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 and Key Pair Usage Periods

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

Table 6 - TrustID Certificates Validity Periods

Key Type	Private Key Usage Period	Certificate Lifetime
Root CA Certificate	20 years	20 years
Subordinate CA Certificate	Up to 15 years	Up to 15 years
End Entity Certificates – Human	Up to 3 years	Up to 3 years

End Entity Certificates – SSL/TLS Server	Up to 815 days	Up to 815 days
Extended Validation Code Signing	Up to 39 months	Up to 39 months
Time-Stamping	End Entity: Up to 15 months	Subordinate CA: Up to 135 months
FATCA Organization	Up to 39 months	Up to 39 months
End Entity Certificates - Other Devices	Up to 7 years	Up to 7 years

Certificates and Keys must not be used after the expiration of the Validity Periods as defined in this section.

6.3.3 Restrictions on CA's Private Key Use

The Private Key used by the Issuing CA for issuing Certificates will 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 will 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 will be used only for communications relating to the approval or Revocation of such Certificates.

6.3.4 Certificate Periods for the Public and Private Keys

The Key usage periods for keying material are described in section 6.3.2.

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 Certificate Agreements.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

All Issuing CA servers must include the following functionality either provided by the operating system or through a combination of 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 I&A; and (vi) a protected audit record.

6.6 LIFE CYCLE TECHNICAL SECURITY 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 prior to 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 prior to 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 on-going 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 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 prior to 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 two network domains at a time. Issuing CA equipment intended to connect to more than one network classification domain will have procedures defined in a CPS, or other document made available to its auditors, that prevent information from one 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.

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 will contain Public Keys used for authenticating the sender of an 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 Policy 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

Version of X.509 Certificate, version 3(2).

7.1.1.2 Serial Number

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

Issuing CA signature to authenticate Certificate.

7.1.1.4 Issuer

Name of Issuing CA.

7.1.1.5 Validity Period

Activation and expiry date for Certificate.

7.1.1.6 Subject

End Entity's DN

7.1.1.7 Subject Public Key Information

End Entity's Public Key.

7.1.2 Certificate Extensions

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

7.1.2.1 Certificate Policies

7.1.2.2 Policy Constraints

- Critical Extensions: all Participant PKI software must correctly process extensions that are identified as "critical" in the applicable Certificate profile found in appendices to this Policy.
- Supported Extensions: The CPS or other publicly available document must define the use of any extensions supported by the Issuing CA, its RAs, and End Entities.
- Basic Constraints: This extension shall be included in all issuing CA Certificates; this extension may be included in all End Entity Certificates.

7.1.3 Algorithm Object Identifiers

Table 7 - TrustID Certificates Algorithm Object Identifiers

Algorithm	OID
Algorithms and OIDs for Signatures:	
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-Sha1	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) sha1(1)}
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 }
Algorithms and OIDs for Identifying Subject Public Key Information:	
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 one of the following named curves:

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 CPS.

7.1.8 Policy Qualifiers Syntax and Semantics

The Issuing CA must 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.

7.2 CRL PROFILE

If utilized, CRLs will be issued in the X.509 version 2 format. The 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 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 request and responses shall be version one.

7.3.2 OCSP Extensions

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

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

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.

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

Inspections will be substantially similar to: (i) AICPA/CPA Canada SSAE 18 SOC 2; (ii) AICPA CPA Canada WebTrust for Certification Authorities; and/or (iii) any other appropriate standards as determined by the PMA.

SOC2 and CA WebTrust are performed by an accredited public accountant or nationally recognized accounting firm and any Auditing Standard audit must be performed by a Certified Information Systems Auditor or a Certified Information Systems Security Professional.

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 thirty (30) days pending correction of any problems prior to 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 prior to 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.

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 I&A, 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

See Section 9.8.

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 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 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.

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

Confidential information about a Subscriber and their Subscribing Organization that is not publicly available in the contents of a Certificate, CRL or in the LDAP Directory shall be considered private.

9.4.3 Information Not Deemed Private

Certificates, CRLs and OCSP Responses, and personal or corporate information appearing in them and in the LDAP Directory, are not considered private.

9.4.3.1 Publication of Server Certificates

Effective April 20, 2018, the Issuing CA shall comply with Certificate Transparency (CT) by publishing new, renewed and replaced TrustID Server Certificates into 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.

9.4.5 Notice and Consent to Use Private Information

PKI Service Providers will not disclose any information deemed confidential under this section, to any third party, except when: (i) authorized by this Policy; (ii) required to disclose by law, governmental rule or regulation, or court order; or (iii) when necessary to effect an appropriate use of a TrustID Certificate. All requests for disclosure of information considered confidential under this section must be made in writing. The Issuing CA may choose to further define or restrict its disclosure of Certificate-related information. Unless prohibited by law, a PKI Service Provider will give all interested persons or parties reasonable prior written notice before disclosing any information considered confidential under this section. Non-disclosure of confidential information will remain an obligation notwithstanding the status of a TrustID Certificate (current or revoked) or the status of the Issuing CA.

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 9.4.6.

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 Issuing CA is responsible for all aspects of the Issuance and management of a TrustID Certificate including: (i) the application and enrollment process; (ii) the Identification and Authentication process; (iii) the actual Certificate manufacturing process; (iv) publication of the Certificate; (v) Revocation of the Certificate; (vi) renewal of the Certificate; and (vii) ensuring that all aspects of the Issuing CA services and CA operations and infrastructure related to Certificates issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy.

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 Certificate Agreement (and in accordance with this Policy and any applicable CPS, if this Policy has been incorporated by reference in the Certificate 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 Certificate 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 one 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 Certificate 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 Certificate 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 Certificate 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 I&A;
- Any restrictions on the use of TrustID Certificates and the corresponding Keys;

- Procedures, rights and responsibilities governing (a) notification of changes in Certificate information, and (b) Revocation of TrustID Certificates;
- Procedures, rights and responsibilities governing renewal of TrustID Certificates;
- Any obligation of the Subscriber to indemnify any other Participant;
- Provisions regarding fees;
- The rights and responsibilities of any RA that is party to the agreement;
- Any warranties made by the Issuing CA and any limitations on warranties or liability of the Issuing CA and/or an RA;
- Provisions regarding the protection of privacy and confidential information; and
- Provisions regarding Alternative Dispute Resolution.

Nothing in the Certificate Agreements may waive or otherwise lessen the obligations of the Subscriber as provided in section 9.6.3 of 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 sections 4 and 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) its 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 perform the Key Pair generation on an approved Cryptographic Module in accordance with section 6.2.1.

9.6.3 Subscriber Representations and Warranties

The responsibilities of each Applicant/Subscriber are to:

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 I&A 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 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 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 Certificate Agreement between the Subscriber and the Issuing CA.

9.6.4 Relying Party Representations and Warranties

Prior to 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 of this Policy.

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 obligations 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.

9.7 DISCLAIMERS OF WARRANTIES

EXCEPT FOR THOSE WARRANTIES EXPRESSLY PROVIDED IN THIS CPS OR THAT MAY BE EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT BY IDENTRUST, IDENTRUST: (I) DISCLAIMS ANY AND ALL OTHER WARRANTIES OF ANY TYPE, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY, CORRECTNESS OR ACCURACY OF INFORMATION PROVIDED, OR FITNESS FOR A PARTICULAR PURPOSE; AND (II) THAT ITS SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR FREE, OR

THAT DEFECTS WILL BE CORRECTED. IDENTRUST MAKES NO WARRANTY THAT ANY IDENTRUST SERVICES WILL MEET ANY EXPECTATIONS.

The foregoing provisions of this section shall not form any limitation on any limitations or disclaimers of IdenTrust, set forth under this TrustID CP, other provisions of the 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 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.

Except with respect to TrustID Extended Validation SSL/TLS Certificates and unless otherwise provided in a separate writing or contract, the total, maximum, aggregate liability of an Issuing CA or RA for all TrustID Certificates issued under this Policy and for all transactions relying on TrustID Certificates is $10,000,000

Except with respect to the TrustID Secure Email Certificate, TrustID Card Authentication Certificate, TrustID Device Certificate, TrustID Code Signing Certificate and TrustID Extended Validation SS/TLS Certificate and unless otherwise provided in a separate contract executed by an officer of IdenTrust Services, LLC, the maximum potential liability for an Issuing CA or RA to any Authorized Relying Party with respect to any one TrustID Certificate upon which the Authorized Relying Party relies will be limited to: (a) $100,000 per transaction; and (b) $250,000 for all transactions in which the Authorized Relying Party relies on the TrustID Certificate.

With respect to the Secure Email Certificate type of TrustID Certificate, the maximum potential liability for an Issuing CA or RA to any Authorized Relying Party with respect to any one Secure Email Certificate upon which the Authorized Replying Party relies will be limited to: (a) $100 per transaction; and (b) $250 for all transactions in which the Authorized Relying Party relies on the Secure Email Certificate.

With respect to the TrustID Card Authentication Certificate type of TrustID Certificate, the maximum potential liability for an Issuing CA or RA to any Authorized Relying Party with respect to any one TrustID Card Authentication Certificate upon which the Authorized Replying Party relies will be limited to: (a) $10 per transaction; and (b) $25 for all transactions in which the Authorized Relying Party relies on the TrustID Card Authentication Certificate.

With respect to the TrustID Device Certificate type of TrustID Certificate, the maximum potential liability for an Issuing CA or RA to any Authorized Relying Party with respect to any one TrustID Device Certificate upon which the Authorized Replying Party relies will be limited to: (a) $10 per transaction; and (b) $25 for all transactions in which the Authorized Relying Party relies on the TrustID Device Certificate.

With respect to the Extended Validation Code Signing Certificate type of TrustID Certificate, the maximum potential liability for an Issuing CA or RA to any Authorized Relying Party with respect to any one Extended Validation Code Signing Certificate upon which the Authorized Replying Party relies will be limited to: (a) $2,000 per transaction; and

(b) $10,000 for all transactions in which the Authorized Relying Party relies on the Extended Validation Code Signing Certificate.

With respect to relying on any single TrustID Extended Validation SSL/TLS Certificate, the maximum aggregate liability for an Issuing CA or RA to any Relying Party or Subscriber will be limited to $2,000 per Subscriber or Relying Party per TrustID Extended Validation SSL/TLS Certificate.

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 Certificate Agreement shall indemnify IdenTrust under the applicable terms and conditions of any indemnification provision therein.

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

9.10 TERM AND TERMINATION

9.10.1 Term

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

9.10.3 Effect of Termination and Survival

The conditions and effect 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 one of the following methods, with the choice between methods to be made by the Participant:

i. 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

ii. by written communication sent from the Participant to IdenTrust via internationally recognized overnight courier to IdenTrust Registration, 5225 Wiley Post Way, Suite 450, Salt Lake City, UT 84116, which such communication will be deemed effective when delivered as evidenced by written confirmation of receipt as recorded by the courier.

9.11.2 Notices by IdenTrust to Individual Participants

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

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 of this CP. 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 TrustID CP. Changes that may materially affect Subscribers or Relying Parties are subject to a public comment period prior to consideration by the IdenTrust PMA. Other amendments such as editorial or typographical corrections, changes to the contact details, or other such minor changes will not be submitted to the TrustID Policy Authority and no comment period will be necessary.

After the PMA accepts changes, IdenTrust's PMA Chair will submit the document for final preparation and publication. Before publication, the document is redacted for sensitive information that can post security risks. The redacted document is the Public version 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 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 is available in electronic form on the Internet at:
https://secure.identrust.com/certificates/policy/ts/

9.12.3 Circumstances Under Which OID Must Be Changed

OIDs will be changed in this 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 two 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 one 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 that a clause or provision of this CP is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CP shall remain valid.

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. 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.

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 four months after termination of the applicable Authorized Relying Party Agreement or two (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 of this CP, 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