TrustID® Certificate Policy

Version 2.0
September 15, 2016

Revision History

Version	Date	Summary of Changes/Comments
2.0	Sept 15, 2016	Incorporate language to support Secure Email Certificates. Updated format for ease of use.

1 INTRODUCTION

1.1 GENERAL INFORMATION

1.1.1 Overview

This TrustID® Certificate Policy contains the rules governing the use of TrustID Certificates among those parties authorized to participate in the Public Key Infrastructure described by this Policy, namely: (i) PKI Service Providers, consisting of (a) the Policy Management Authority; (b) Issuing Certification Authorities; (c) Registration Authorities; (d) Certificate Manufacturing Authorities, and (e) Repositories; and (ii) End Entities, consisting of (a) Certificate Holders and (b) Authorized Relying Parties. 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.

1.1.2 General Definitions

1.1.2.1 Terms Capitalized terms used in this Policy have the following meanings:

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: (i) using the TrustID Certificate (after issuance); (ii) failing to notify the Issuing CA of any problems with the TrustID Certificate within a reasonable time after receiving it, or (iii) 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 Cryptomodules (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.

Authority Revocation List (ARL)	A list of revoked CA Certificates. An ARL is a CRL for CA Certificates.
Authorized Relying Party	An Individual or Organization that has entered into an Authorized Relying Party Agreement.
Authorized Relying Party Agreement	A contract between an Individual or an Organization and an Issuing CA allowing the party to rely on TrustID Certificates in accordance with this Policy.
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: (i) identifies the Certification Authority issuing it; (ii) names or identifies a Certificate Holder, Authorized Relying Party or Electronic Device; (iii) contains the Public Key of the Certificate Holder, Authorized Relying Party or Electronic Device; (iv) identifies the Certificate's Validity Period; (v) is digitally signed by a Certification Authority; and (vi) 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 Certificate Holder 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 Certificate Holder.
Certificate Holder	An Individual or Organization that: (i) is named or identified in a TrustID Certificate, or is responsible for the Electronic Device named, as the subject of the TrustID Certificate; and (ii) 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.
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 Profile	The protocol used in Section 7 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.
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.
Cross-Certificate	A Certificate used to establish a trust relationship between two Certification Authorities.
Cryptomodule	Secure software, device or utility that: (i) generates Key Pairs, (ii) stores cryptographic information, and/or (iii) performs cryptographic functions.
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: (i) whether the transformation was created using the Private Key that corresponds to the Public Key; and (ii) whether the record has been altered since the transformation was made.
Distinguished Name (DN)	The unique identifier for a Certificate Holder so that he, she or it can be located in a directory (e.g., the DN for a Certificate Holder might contain the following attributes: common name (cn), email address (mail), Organization name (o), Organizational unit (ou), locality (l), state (st) and country (c)).
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)	Certificate Holders and Authorized Relying Parties.
External CA	An independent entity that is not affiliated to IdenTrust 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

	linked to on www.IdenTrust.com) and independently audited with publically available reports. They are contractually bound to other obligations by IdenTrust and also bound to comply with application software supplier programs.
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	A natural person and not a juridical person or legal entity.
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.
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 General Definitions section.
Key Generation	The process of creating a Key Pair.
Key Pair	Two mathematically related Keys (a Private Key and its corresponding Public Key), having the properties that: (i) one Key can be used to encrypt a communication that can only be decrypted using the other Key; and (ii) even knowing one Key it is computationally infeasible to discover the other Key.
Lightweight Directory Access Protocol (LDAP)	A client-server protocol used for accessing an X.500 directory service over the Internet.
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.

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. An Online Status Check involving a CRL consists of checking the most recently issued CRL (e.g., not involving a cached CRL).
Operational Period	A Certificate's actual term of validity, beginning with the start of the Validity Period and ending on the earlier of (i) the end of the Validity Period disclosed in the Certificate, or (ii) 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	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.
PKI Service Providers	The PMA, Issuing CAs, RAs, CMAs, and Repositories participating in the PKI defined by this Policy.
PMA Charter	The document adopted by the PMA that identifies the policies and procedures for administering this Policy.
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.

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; and • 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.
Restricted Zones	Any one of: (i) an Operations Zone; (ii) a Security Zone; and (iii) a High Security Zone.
Revocation	The act of making a Certificate permanently ineffective from a specified time forward. Revocation is effected by notation or inclusion

	in a set of revoked Certificates or other directory or database of revoked Certificates (e.g., inclusion in a CRL).
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 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 Certificate Holder, a Shared Secret may consist of an account PIN or online banking password shared solely between the RA and the Certificate Holder, but not the Issuing CA. For purposes of establishing identity between the Certificate Holder and the Issuing CA necessary for Certificate issuance, a Shared Secret consists of different Activation Data, which is shared among the RA, Certificate Holder and Issuing CA.
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.
Sponsoring Organization	An Organization that has an affiliation with an Individual and has permitted the Individual to hold a TrustID Certificate that identifies the Organization and the fact of the Individual's affiliation with the Organization. See "Affiliated Individual."
Sponsoring Organization Authorization Form	The form used to provide information about an Affiliated Individual who will be authorized by an Organization to hold a TrustID Certificate.
Subject Name	The specific field in a Certificate containing the unique name-identifier for the Certificate Holder.
Token	A Cryptomodule consisting of a hardware object (e.g., a "smart card"), often with memory and a microchip.
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: (i) are reasonably secure from intrusion and misuse; (ii) provide a reasonable level of availability; and (iii) 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).

1.1.2.2

Acronyms	**Definition**
ARL	Authority Revocation List
CA	Certification Authority
CMA	Certificate Manufacturing Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DSA	Digital signature algorithm
I&A	Identification and Authentication
LDAP	Lightweight Directory Access Protocol
ISO	International Standards Organization
OID	Object Identifier
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
VBA	Visual Basic Application
X.500	The ITU-T (International Telecommunication Union-T) standard that establishes a distributed, hierarchical directory protocol organized by country, region, Organization, etc.
X.501	The ITU-T (International Telecommunication Union-T) standard for use of Distinguished Names in an X.500 directory.
X.509	The ITU-T (International Telecommunication Union-T) standard for Certificates. X.509, version 3, refers to Certificates containing or capable of containing extensions.

1.1.3 Monetary Amounts

All monetary values used in this Policy are in United States Dollars.

1.2 IDENTIFICATION

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)}.

1.2.1 Certificate Types

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 Certificate Holder (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:

Certificate Type	OID	Description
TrustID Personal	2.16.840.1.113839.0.6.1	Issued in a software Cryptomodule to Unaffiliated Individuals in accordance with Section 3.1.6;
TrustID Personal Hardware	2.16.840.1.113839.0.6.10.1	Issued on an approved hardware Cryptomodule to Unaffiliated Individuals in accordance with the sections appropriate to the certificate type and in accordance with section 6.2.1.
TrustID Business	2.16.840.1.113839.0.6.2	Issued in a software Cryptomodule to Individuals who are affiliated with a Sponsoring Organization and issued in accordance with Sections 3.1.4, 3.1.5 and 3.1.6
TrustID Business Hardware	2.16.840.1.113839.0.6.10.2	Issued on an approved hardware Cryptomodule to an Individual who is affiliated with a Sponsoring Organization and issued in accordance with section 6.2.1.
TrustID Server	2.23.140.1.2.2 2.16.840.1.113839.0.6.3	Issued to SSL-enabled Electronic Devices in accordance with Section 3.1.8
TrustID Code Signing	2.16.840.1.113839.0.6.6 (arc)	Not currently issuing these certificate types
TrustID Business for VBA Code Signing	2.16.840.1.113839.0.6.6.1	Issued to Affiliated Individuals for signing software. It requires authentication of the organization, the individual and his/her affiliation to the organization in accordance with Sections 3.1.1, 3.1.4, 3.1.5 and 3.1.6.
TrustID Organization for VBA Code Signing	2.16.840.1.113839.0.6.6.2	Issued to Organizations for signing software. It requires the authentication of the organization, the human sponsor and his/her authority to request in

		accordance with Sections 3.1.1, 3.1.4, 3.1.5 and 3.1.6 and issued to Organizations for signing software. It requires the authentication of the organization, the human sponsor and his/her authority to request in accordance with Sections 3.1.1, 3.1.4, 3.1.5 and 3.1.6.
TrustID FATCA Organization	2.16.840.1.113839.0.6.8	Issued to Organizations operating within the United States Internal Revenue Service (IRS) Foreign Account Tax Compliance Act (FATCA) framework in accordance with Sections 3.1.4;
Administrative CA	2.16.840.1.113839.0.7 (arc)	Used solely for the management and operation of the PKI, including the three following certificate types:
Administrators	2.16.840.1.113839.0.7.1	Issued to CA Administrators
Registration Authorities	2.16.840.1.113839.0.7.2	Issued to Registration Authorities
Authorized Relying Parties	2.16.840.1.113839.0.7.3	Issued to Relying Parties
TrustID Secure Email Software	2.16.840.1.113839.0.6.11.1	Issued in a software Crytomodule in accordance with Section 3.1.8.1 to Unaffiliated Individuals for the purpose of email signing, email encryption, and client authentication.
TrustID Secure Email Hardware	2.16.840.1.113839.0.6.11.2	Issued in a hardware Crytomodule in accordance with Section 3.1.8.1 and 6.2.1 to Unaffiliated Individuals for the purpose of email signing, email encryption, and client authentication.

1.3 COMMUNITY AND APPLICABILITY

This Policy 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, Certificate Holder and Authorized Relying Party.

1.3.1 PKI Service Providers

1.3.1.1 The 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.

1.3.1.2 Issuing 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, 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.
1.3.1.3	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.
1.3.1.4	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.
1.3.1.5	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.
1.3.1.6	External Certificate Authorities	External CAs are independent entities that are not affiliated to IdenTrust that issue Certificates from a Subordinate CA Certificate. That Subordinate CA Certificate is issued and managed according to this Policy. IdenTrust will be ultimately responsible for the Subordinate CA Certificate it issues contractually to the External CA. The External CA will be responsible for the Certificates it issues and will produce and publish a separate CP and CPS that they will be bound to adhere to its terms (each are publically disclosed and linked to on www.IdenTrust.com) and independently audited with publically available reports. They are contractually bound to other obligations by IdenTrust and also bound to comply with application software supplier programs.

1.3.2 End Entities

1.3.2.1	Certificate Holders	The Issuing CA may issue TrustID Certificates to the following classes of Certificate Holders: Individuals and Organizations.
1.3.2.2	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.

1.3.3 1.3.3 PKI Applicability and Applications

1.3.3.1	Purpose	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.
1.3.3.2	Approved Applications	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 Certificate Holder'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.
1.3.3.3	Prohibited Applications	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.

1.3.4 Cross-Certification

The PMA may approve cross-certification between an Issuing CA and other Certification Authorities, and 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.

1.4 CONTACT DETAILS

This Policy is owned and administered by IdenTrust Services LLC.

1.4.1 Specification / Policy Administration Organization

The PMA can be reached at:

IdenTrust Policy Management Authority

55 Hawthorne St, Suite 400

San Francisco, CA 94105

1.4.2 Contact Person

Questions regarding the implementation and administration of this Policy should be directed to:

IdenTrust PMA Co-Chairperson

55 Hawthorne St, Suite 400

San Francisco, CA 94105

Or via email to helpdesk@IdenTrust.com.

1.4.3 Person Determining CPS Suitability

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

2 GENERAL PROVISIONS

2.1 APPORTIONING LEGAL RESPONSIBILITIES AMONG PARTIES

2.1.1 PKI Service Provider Obligations, Representations and Liability

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 Certificate Holders 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 Certificate Holder 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.

2.1.2 Issuing CA Obligations, Representations and Liability

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, including the following:

2.1.2.1 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.

2.1.2.2 Certificate Holder Warranties

Issuing CAs must provide the following warranties, in separate writing or in contract, to all Certificate Holders 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 Section 2.1.2.7)); 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 Section 2.1.2.7)).

Such warranties shall be made as of: (i) the time of the Certificate Holder's Acceptance of the TrustID Certificate; and (ii) the time that the Certificate Holder's TrustID Certificate is used during its Operational Period.

2.1.2.3 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 Certificate Holder;
- 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 Certificate Holder'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.

2.1.2.4	Warranty Limitations	The warranties offered to both Certificate Holders 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 2.1.2.3.
2.1.2.5	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.
2.1.2.6	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.

2.1.2.7 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 Certificate Holder'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 Certificate Holders 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 Certificate Holder's duties to provide accurate information during the application process;
- The Certificate Holder'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 Certificate Holder 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 Certificate Holder as provided in Section 2.1.4 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 2.1.5 of this Policy.
2.1.2.8	Protection of Private Keys	The Issuing CA must ensure that its Private Keys and Activation Data are protected in accordance with Parts 4 and 6 of this Policy.
2.1.2.9	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.
2.1.2.10	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 Part 3.
2.1.2.11	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 2.1.1 and other provisions of this Policy.

2.1.3 RA Obligations and Liability

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 Sections 2.1.1.

2.1.3.1	Notification of Certificate Issuance and Revocation	Unless otherwise provided by contract, there are no requirements that an RA notify a Certificate Holder or Authorized Relying Party of the issuance or revocation of a TrustID Certificate.
2.1.3.2	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 Parts 3 and 4 of this Policy.
2.1.3.3	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 Parts 5 and 6 of this Policy.
2.1.3.4	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.

2.1.3.5	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.
2.1.3.6	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 2.1.1 and other provisions of this Policy.

2.1.4 Applicant/Certificate Holder Obligations, Representations and Liability

The responsibilities of each Applicant/Certificate Holder are to:

2.1.4.1	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 Certificate Holder, review the Certificate to ensure that all Certificate Holder information included in it is accurate, and to Accept or reject the Certificate in accordance with Section 4.4;
2.1.4.2	Protection of Certificate Holder 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;
2.1.4.3	Restrictions on Certificate Holder 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,
2.1.4.4	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 3.1.5, whenever the Affiliated Individual is no longer affiliated with the Sponsoring Organization.
2.1.4.5	Consequences of Breach	A Certificate Holder 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.
2.1.4.6	Other Agreements	A Certificate Holder's obligations will be governed by the Certificate Agreement between the Certificate Holder and the Issuing CA.

2.1.5 Authorized Relying Party Obligations, Representations and Liability

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

2.1.5.1	Use of Certificates For Appropriate Purpose	Ensure that the TrustID Certificate and intended use are appropriate under the provisions of this Policy;

2.1.5.2	Verification Responsibilities	Use the TrustID Certificate only in accordance with the certification path validation procedure specified in X.509 and PKIX; and
2.1.5.3	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.
2.1.5.4	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 1.1.2.1 of this Policy.
2.1.5.5	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.
2.1.5.6	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.
2.1.5.7	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.
2.1.6	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.

2.2 LIMITATION ON 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.

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.

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 Secure Email Certificate type of TrustID Certificate and unless otherwise provided in a separate writing or contract, 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.

Notwithstanding the foregoing provisions of this Section 2.2, the Issuing CA and RAs may limit their liability to a Certificate Holder with respect to the Certificate Holder's TrustID Certificate to the amount received by the Issuing CA and/or RA from the Certificate Holder with respect to such TrustID Certificate.

2.3 FINANCIAL RESPONSIBILITY

2.3.1 Administrative Processes (ADR)

Participants may be required to participate in, and bear financial responsibility for, a centrally-administrated Alternative Dispute Resolution (ADR) process established under Section 2.4.3.

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 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.

2.4.2 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.

2.4.3 Dispute Resolution Procedures

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.

2.5 FEES

Notice of any fee charged to a Certificate Holder or Authorized Relying Party must be brought to the attention of that entity.

2.5.1 Certificate Issuance, Renewal, and Revocation 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.

2.5.2 Certificate Access Fees

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

2.5.3 Revocation Status Information Access Fees (Certificate Validation Services)

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

2.5.4 Fees for Other Services such as Policy Information

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.

2.5.5 Refund Policy

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

2.6 NOTICE AND PUBLICATION

2.6.1 Publication of CA 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: (i) issued TrustID Certificates; (ii) a CRL or online Certificate status database (or both); (iii) the Issuing CA's CA Certificate for its CA Private Signing Key; (iv) past and current versions of the Issuing CA's CPS; (v) a copy of this Policy; and (vi) other relevant information relating to TrustID Certificates.

2.6.2 Frequency of Publication

TrustID Certificates are published following Acceptance by the Certificate Holder in accordance with the procedure specified in Section 4.3. If the Issuing CA elects to publish CRLs, the CRLs will be published as specified in Section 4.10.

2.6.3 Access Controls

The Issuing CA will not impose any access controls on: (i) this Policy; (ii) the Issuing CA's CA Certificate; and (iii) 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.

2.6.4 Location

The location of publication will be one appropriate to the Certificate-using community, in accordance with the total security requirements, and will identify an X.500 directory and an LDAP interface.

2.6.5 Revocation Information

The sole source of information regarding the validity or revocation of a TrustID Certificate will be that provided by the Issuing CA pursuant to an Authorized Relying Party contract. Revocation reason codes should be provided through revocation mechanisms (e.g., the reason Code in an X.509 Version 2 CRL). In order to preserve trust in the PKI, the dissemination of information concerning the events leading up to an investigation of a revocation should be limited to those involved.

2.7 COMPLIANCE INSPECTION

2.7.1 Frequency

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.

2.7.2 Identity and Qualifications of Inspector

Subject to further qualifications identified in Section 2.7.4, Compliance Inspectors must: (i) have qualifications in accord with best commercial practice; (ii) perform CA or Information System Security inspections as their primary responsibility; and (iii) be familiar with the Issuing CA's practices.

2.7.3 Inspector's Neutrality

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.

2.7.4 Scope of Audit/Inspection

Inspections will be substantially similar to: (i) the Common Criteria Protection Profile for Commercial Security 2 published by the National Institute of Standards and Technology (CS2); (ii) a Report of Policies and Procedures in Operation and Test of Operational Effectiveness conducted pursuant to the guidance provided in the American Institute of Certified Public Accountants' ("AICPA's") Statement on Auditing Standards (SAS) Number 70, Reports on the Processing of Transactions by Service Organizations, Type Two Review (SAS70); (iii) AICPA/CICA WebTrust for Certification Authorities (CA WebTrust); and/or (iv) any other appropriate standards as determined by the PMA.

SAS 70 and CA WebTrust are performed by an accredited public accountant or nationally-recognized accounting firm and any CS2 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.

2.7.5 Actions Taken as a Result of Audit/Inspection

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 assurance level 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 Certificate Holders, Authorized Relying Parties and RAs. The manner and extent of the publication will be defined by the Issuing CA.

2.8 PRIVACY AND DATA PROTECTION POLICY

2.8.1 Sensitivity of Information

2.8.1.1	Non-Private 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 emailings, junk email, spam, etc.). A TrustID Certificate should only contain information that is relevant and necessary to effect transactions with the Certificate.
2.8.1.2	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 Cryptomodule.
2.8.1.3	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.

2.8.2 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). But 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.

2.8.3 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.

2.8.4 Release of Information to Third Parties

PKI Service Providers will not disclose any information deemed confidential under this Section 2.8, 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 2.8 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 2.8. 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.

2.9 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 the express written permission of the owner is expressly prohibited.

2.10 LEGAL VALIDITY OF CERTIFICATES

2.10.1 Issuance

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

2.10.2 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.

2.10.3 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.

2.10.4 Rule 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.

3 IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

3.1.1 Identification and Authentication

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 Part 3.

Certificate Type	Identification Requirements
TrustID Personal	Identity shall be established by: Verification of the identity of the Unaffiliated Applicant based on section: 3.1.6.
TrustID Business	Identity shall be established by: Verification of the identity of the affiliated Applicant based on section: 3.1.5. Verification of the Organization based on section 3.1.4.
TrustID Server	Identity shall be established by: 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 annex A.
Administrative CA (Administrators and Registration Authorities)	Identity shall be established by: Verification of the identity of the affiliated Applicant based on section: 3.1.5 Verification of the Organization based on section 3.1.4
Administrative CA (Authorized Relying Parties)	Identity shall be established by: Verification of the identity of the Relying Party based on section 3.1.7
TrustID FATCA Organization	Identity shall be established by: Verification of the Organization based on section 3.1.4.
TrustID Secure Email Software	Identity shall be established by: Demonstration that the Applicant of the certificate had control of the Applicant provided email address at the time of email verification, based on section 3.1.8.1
TrustID Secure Email Hardware	Identity shall be established by: Demonstration that the Applicant of the certificate had control of the Applicant provided email address at the time of email verification, based on section 3.1.8.1

If applications are transmitted electronically, via email or a web-site, the transmissions must be secure (e.g., SSL or similar protocol); otherwise, applications should be submitted by first class U.S. mail or in person.

3.1.2 Types of Names

The Subject Name used for TrustID Certificates shall be the End Entity's authenticated common name. 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 DN must be in the form of an X.501 printable string and must not be blank.

3.1.2.1	Need for Names to be Meaningful	The contents of each Certificate Subject and Name fields must have an association with the authenticated name of the End Entity. • In the case of Individuals, the authenticated common name should be a combination of first name, surname, and optionally initials. • For Affiliated Individuals, the DN may also include an Organization position or role. • In the case of End Entities that are Organizations, the DN will reflect the authenticated legal name of the End Entity. • Where a Certificate refers to a role or position, the Certificate must also contain the identity of the person who holds that role or position. • A Certificate issued for an Electronic Device must include the authenticated name of the Electronic Device and, if applicable, the name of the responsible Individual or Organization.
3.1.2.2	Rules for Interpreting Various Name Forms	The Issuing CA may defer to a naming authority for guidance on name interpretation and subordination.
3.1.2.3	Uniqueness Of Names	The Subject Name listed in a TrustID Certificate shall be unambiguous for Certificates issued by the Issuing CA and conform to X.500 standards for name uniqueness. If necessary, additional numbers or letters may be appended to the real name to ensure the name's uniqueness within the domain of TrustID Certificates issued by the Issuing CA. Each name shall be unique for a single Certificate Holder. A CA may issue more than one Certificate with the same unique name to the same Certificate Holder. Wildcard forms are allowed, subject to the restrictions imposed by Application Software Suppliers programs.
3.1.2.4	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.
3.1.2.5	Use of Names and 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.

3.1.3 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 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 Section 6.1.2).

3.1.4 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: (i) the Organization legally exists and has conducted business from the address listed in the Certificate application; and (ii) 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: (i) legal company name; (ii) type of entity; (iii) year of formation; (iv) names of directors and officers; (v) address; (vi) telephone number; and (vii) 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.

3.1.5 Certificates for Affiliated Individuals

An Organization's Certificates may be issued to Affiliated Individuals after Authentication of Organization Identity outlined in Section 3.1.4 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 3.1.6. 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

3.1.6 Identification and 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:

Certificate Type	Identification Requirements
TrustID Personal Certificate	Identity shall be established by: Verification and validation of identity information provided by the Applicant, including out-of-band confirmation, performed in accordance with Section 3.1.6.3; Maintenance of an ongoing, trusted business relationship in accordance with Section 3.1.6.5; 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 3.1.6.1 below), performed in accordance with Section 3.1.6.2.
TrustID Business Certificate	Sponsoring Organization confirms the Affiliated Individual's affiliation with the Sponsoring Organization.

3.1.6.1 Acceptable Forms of Identification Documents (IDs)

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

(i) 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.

(ii) 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.

3.1.6.2 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 (i) internally consistent; and (ii) consistent with the information contained in the application for the certificate. Identity established in this manner shall be communicated to the CA by a signed communication (in writing or digitally) indicating that the Applicant was properly identified.

Documentation that in-person identification was performed may be submitted electronically in accordance with Section 3.1.6.4.

3.1.6.3 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 (i) delivery of a Shared Secret to a confirmed and trusted data point (e.g., street address, telephone number or email address), (ii) delivery in-person of a Shared Secret upon presentment of at least two Acceptable Forms of ID in accordance with Sections 3.1.6.1 and 3.1.6.2, (iii) use of a Shared Secret between the Individual identified in the application and the CA or RA pursuant to an antecedent identification and ongoing relationship, (iv) 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 (v) another equivalent process.

3.1.6.4	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 3.1.4, 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.
3.1.6.5	Know Your Customer I&A	If (i) the RA has previously established the identity of an Individual, and (ii) the RA and the Individual have an ongoing, trusted business relationship (e.g., commercial, banking or employment) sufficient to satisfy the RA of the Individual's identity, then the RA may rely on such prior identification and ongoing relationship to satisfy the 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.
3.1.6.6	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

3.1.7 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.

3.1.8 Electronic Devices

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 this type of Certificate, the Issuing CA shall conform to “the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” available in annex A and published at http://www.cabforum.org. In the event of any inconsistency between this CP and those requirements set forth in annex takes precedence over this document. This type of Certificate can only be issued by an Issuing CA that can ensure accomplishment of the I&A required by this Section.

3.1.8.1 Secure Email Certificate

The Secure Email Certificate can be used for the purposes of email signing, email encryption, and client authentication 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: (i) 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; (ii) such email shall contain a unique, system generated code that will be used for email confirmation and the URL of an email confirmation website; (iii) 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 (iv) 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 CERTIFICATE RE-KEY, RENEWAL, AND UPDATE

3.2.1 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.

3.2.2 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 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.

3.2.3 Certificate Update

Updating a TrustID Certificate means creating a new TrustID Certificate that: (i) has the same or a different Public Key, (ii) has a different serial number, and (iii) 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 Certificate Holder who gains an authorization. The old Certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

3.2.4 Re-Key, Renewal or Update of Affiliated Individual's Certificate

Re-key, renewal or update 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.

3.3 RE-KEY AFTER REVOCATION OR EXPIRATION

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 REVOCATION REQUEST

An End Entity may request revocation 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 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 REQUEST

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 Request a Certificate

The Certificate application process may be initiated by Individuals or Organizations.

4.2 Certificate Request Processing

4.2.1 Certificate Request Process

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.

4.2.2 Time to Process a Certificate Request

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

4.3 CERTIFICATE ISSUANCE

After all application and approval processes identified in this Policy are completed, the Issuing CA will: (i) issue the requested TrustID Certificate; (ii) notify the Applicant of the TrustID Certificate's issuance; and (iii) make the TrustID Certificate available to the Applicant for Acceptance. 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.

4.5 NOTIFICATION OF CERTIFICATE ISSUANCE TO OTHERS

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

4.6 CERTIFICATE USAGE

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

4.7 PROCESSING A REQUEST FOR A NEW KEY

4.7.1 Circumstances for Request of a New Key Certification

A request for new Key certification may be made to expedite certification of a new Key Pair to (i) replace an existing Certificate revoked for a reason other than Key compromise, (ii) replace an existing Certificate revoked for Key compromise, pursuant to Section 4.7.3; or (iii) obtain a second Certificate with a different Distinguished Name, attribute or assurance level.

4.7.2 Who Can Request

Only the End Entity may request certification of a new Key.

4.7.3 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

4.7.4 Notification of Certification Request for a New Key to End Entity

The notification procedures used by the Issuing CA or RA should be the same as with a new End Entity request.

4.8 CERTIFICATE MODIFICATIONS

The Issuing CA may allow for Certificate modification for any of the following changes during the Certificate's Operational Period: (i) legal name due to marriage, divorce or court petition; (ii) Organizational affiliation; (iii) location information; (iv) email address; or (v) any attribute/extension of a Certificate.

4.9 CERTIFICATE REVOCATION

4.9.1 Circumstances for Revocation

4.9.1.1	Permissive Revocation	An End Entity may request revocation of his, her or its TrustID Certificate at any time for any reason. A Sponsoring Organization may request revocation of a TrustID Certificate issued to an Affiliated Individual and/or human sponsor, of the Sponsoring Organization, at any time for any reason. The Issuing CA may revoke a TrustID Certificate for any reason, including without limitation the failure of the End Entity (or any Sponsoring Organization, where applicable) to meet its obligations under this Policy, the applicable CPS, or any other agreement, regulation, or law applicable to the TrustID Certificate that may be in force. This includes revoking a TrustID Certificate when the Issuing CA suspects that a compromise of the corresponding Private Key has occurred.
4.9.1.2	Required Revocation	An End Entity or a Sponsoring Organization (where applicable) will promptly request revocation of a TrustID Certificate whenever: (i) any of the information in the TrustID Certificate changes or becomes obsolete; (ii) the Private Key, or the media holding the Private Key, associated with the TrustID Certificate is known or suspected of being

compromised; or (iii) an Affiliated Individual is no longer affiliated with a Sponsoring Organization. The Issuing CA will revoke a TrustID Certificate: (i) upon request of the End Entity (or Sponsoring Organization, where applicable); (ii) upon failure of the End Entity (or the Sponsoring Organization, where applicable) to meet its material obligations under this Policy, any applicable CPS, or any other agreement, regulation, or law that may be in force that is applicable to the TrustID Certificate; (iii) if knowledge or reasonable suspicion of compromise is obtained; (iv) if the Issuing CA determines that the TrustID Certificate was not properly issued in accordance with this Policy and/or any applicable CPS; (v) if knowledge or reasonable suspicion of misuse is obtained (i.e., use of Code Signing Certificate to sign malicious code).

4.9.2 Who Can Request Revocation

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 Certificate Holder's Sponsoring Organization. In any case, notice should be provided to the End Entity 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 Time to Process a Revocation

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 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.

4.9.5 Revocation Checking Requirements

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.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Certificate Status Checking Methods

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 (i) CRLs, and/or (ii) an online Certificate status database. 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 Certificate Revocation Lists

When an Issuing CA provides CRLs as a method of verifying the validity and status of TrustID Certificates, the following requirements will apply:

4.10.2.1	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.
4.10.2.2	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.
4.10.2.3	CRL Latency	Authorized Relying Parties who rely on a CRL must (i) check for an interim CRL before relying on a TrustID Certificate, and (ii) 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.

4.10.3 Online Status Checking

When an Issuing CA provides an online Certificate status database as a method of verifying the validity and status of TrustID Certificates, the following requirements will apply:

4.10.3.1	Online Revocation/Status Checking Availability	The Issuing CA will validate online, near-real-time the status of the TrustID Certificate indicated in a Certificate validation request message.
4.10.3.2	Online Revocation Checking Requirements	Authorized Relying Parties who rely on an online Certificate status database must (i) validate a TrustID Certificate with such database before relying on the Certificate, and (ii) 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.

4.10.4 Other Forms of Revocation Advertisements Available

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

4.11 END OF SUBSCRIPTION

No stipulation.

4.12 PRIVATE KEY RECOVERY

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.

5 CA FACILITY AND MANAGEMENT CONTROLS

5.1 PHYSICAL CONTROLS

The Issuing CA, and all RAs, CMAs and Repositories, will implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or Tokens) 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: (i) be manually or electronically monitored for unauthorized intrusion at all times; (ii) 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; (iii) ensure personnel not on the access list are properly escorted and supervised; (iv) ensure a site access log is maintained and inspected periodically; and (v) 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: (i) a Security Zone; or (ii) 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 Cryptomodule, all system software and Private Keys. For example, the Cryptomodule 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 Cryptomodules 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 Cryptomodule is installed and activated. The RA will implement physical access controls to reduce the risk of equipment tampering even when the Cryptomodule 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 Cryptomodules 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 Cryptomodule 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 Cryptomodules 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 person 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, which 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 2.8 will be destroyed, such that the information is unrecoverable, prior to disposal.

5.1.8 Off-Site 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.

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 identity and authorization verified before they are: (i) included in the access list for the Issuing CA site; (ii) included in the access list for physical access to the Issuing CA system; (iii) given a Certificate for the performance of their CA role; or (iv) given an account on the PKI system. Each of these Certificates and accounts (with the exception of CA signing Certificates) must: (i) be directly attributable to an individual; (ii) not be shared; and (iii) 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.

5.3 PERSONNEL CONTROLS

5.3.1 Background 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: (i) the Issuing CA/RA security principles and mechanisms; (ii) security awareness; (iii) all PKI software versions in use on the Issuing CA system; (iv) all duties they are expected to perform; and (v) 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. Local policies, which do impose requirements, will provide for continuity and integrity of the PKI service.

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 Contracting Personnel Requirements

The Issuing CA must ensure that contractor access to the Issuing CA site is in accordance with Section 5.1.1.

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 SECURITY AUDIT PROCEDURES

5.4.1 Types of Event 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

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 Event Recorded

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:

5.5.1.1 Certificate Issuance

- Applicant's name when it appears in the Certificate's "Common Name" field
- Method of application (i.e., online, in-person, etc.)
    1. For each data element accepted for proofing, including electronic forms:Name of document presented for identity proofing
    2. Issuing authority
    3. Date of issuance
    4. Date of expiration
    5. All fields verified
    6. Source of verification (i.e., which databases used)
    7. Method of verification (i.e., online, in-person)
    8. Date/time of verification
- Name of the RA
- All associated error messages and codes
- Date/time of process completion
- Date/time of Certificate download/Acceptance

5.5.1.2	Certificate Validation	• Certificate serial number • Certificate status with reason code • All associated error messages and codes • Date/time of all Certificate validation requests • Date/time of transmission of Certificate status request responses
5.5.1.3	Certificate Revocation	• Date/time • Name of the RA • End Entity's common name • Reason code for revocation request • Certificate serial number • All associated verification request and revocation data
5.5.1.4	Certificate Renewal	• Certificate serial number • Certificate common name • New Validity Period dates • Date/time of completion of renewal process • All associated renewal data

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

Certificate validations and witnessed document signing (notarization) will be time-stamped.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

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 inspector will verify the integrity of the archives.

5.5.8 Long Term Information Preservation

No stipulation.

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 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 forty eight (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.

5.7.2 Secure Facility after a Natural or Other Type of 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.

5.7.3 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: (i) the PMA; (ii) all CAs to whom it has issued cross-certificates; (iii) all of its RAs; (iv) all Certificate Holders; and (v) all Individuals or Organizations who are responsible for a Certificate used to an Electronic Device. The Issuing CA must also: (i) publish the CA Certificate serial number on an appropriate CRL; and (ii) revoke all cross-Certificates signed with the revoked CA Certificate. After addressing the factors that led to revocation, 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 Section 4.9.

5.7.4 Entity Private Key is Compromised

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 Section 5.7.3). After addressing the factors that led to 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.

5.7.5 Entity Public 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 Certificate Holders.

5.8 CA TERMINATION

In the event that the Issuing CA ceases operation, all Certificate Holders, 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.

5.9 CUSTOMER SERVICE

As described in this Policy, the Issuing CA will implement and maintain a Customer Service Center to provide assistance and services to Certificate Holders 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.

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 Cryptomodules.

6.1.2 Private Key Delivery

In most cases, a Private Key will be generated and remain within the crypto boundary of the Cryptomodule. If the owner of the Cryptomodule 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 Cryptomodule (e.g., Smart Card) must securely deliver the Cryptomodule to the intended Key holder. Accountability for the location and state of the Cryptomodule must be maintained until delivery and possession occurs. The recipient will acknowledge receipt of the Cryptomodule to the Issuing CA or the RA. If the End Entity generates the Key, and the Key will be stored by and used by the application that generated it, or on a hardware Token in the possession of the End Entity, no further action is required. If the Key must be extracted for use by other applications or in other locations, a protected data structure (such as defined in [PKCS#12]) will be used. The resulting file may be kept on a magnetic medium or transported electronically. See Section 6.4.1.

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 Certificate Holders

The Public Key corresponding to the Issuing CA's CA Private Signing Key may be delivered to End Entities 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 224 bits.

6.1.6 Public Key Parameters Generation

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

6.1.7 Parameter Quality Checking

Parameters for DSA will be checked as specified in [FIPS186].

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 an FIPS approved method.

6.1.9 Key Usage Purposes (As Per X.509 V3 Key Usage Field)

Keys may be used for authentication, non-repudiation and message integrity. 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.

6.2 CA PRIVATE KEY PROTECTION

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

6.2.1 Standards for Cryptomodule

The relevant standard for Cryptomodules 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. Cryptomodules 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.

End Entities will use Cryptomodules that meet at least the criteria specified for Level 1. RAs require at least Level 2 hardware Cryptomodules. A higher level may be used if available or desired. RAs and Issuing CAs should provide the option of using any acceptable Cryptomodule, to facilitate the management of Certificates. The Issuing CA may use hardware or software Cryptomodules for CA key generation and protection, validated at Level 2. Certificates will be signed using a hardware Cryptomodule that meets Level 2.

End Entity Certificates with a policy OID within the arch for hardware (i.e., 2.16.840.1.113839.0.6.10.x) shall be issued on hardware Cryptomodules validated to meet the criteria specified in the FIPS 140-2 Level 2 standard.

6.2.2 Private Key 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.

6.2.6 Private Key Entry into Cryptomodule

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

6.2.7 Method of Activating Private Key

An End Entity must be authenticated to the Cryptomodule 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.

6.2.8 Method of Deactivating Private Key

Cryptomodules 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 Cryptomodules should be removed and stored, unless they are within the End Entity's sole control.

6.2.9 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 Cryptomodules, 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.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The Issuing CA must retain all verification Public Keys.

6.3.2 Validity Periods

All Certificates and corresponding Keys shall have maximum Validity Periods not to exceed the following: (i) CA public verification Key and Certificate - twenty years; (ii) CA Private Signing Key and Certificate - eight years; (iii) End-Entity public verification Key and Certificate - twelve years; (iv) End-Entity signing Key - three years. Certificates and Keys must not be used after the expiration of the Validity Periods indicated 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 Usage Periods for the Public and Private Keys

The Key usage periods for keying material are described in Section 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 Cryptomodule. 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 Cryptomodule and Activation Data. In addition, End Entities should also receive (and acknowledge receipt of) information regarding the use and control of the Cryptomodule. See Section 6.1.2.

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 Cryptomodule is used to protect, and will not be stored with the Cryptomodule. 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 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.

6.7 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 CRYPTOMODULE ENGINEERING CONTROLS

Requirements for Cryptomodules are as stated above in Section 6.2.

7 CERTIFICATE AND CRL 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 and Base Fields

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 as well as the Certificate extensions defined 7.1.2
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

No extension will modify or undermine the use of X.509 base fields. Additionally:

7.1.2.1	Certificate Policies	No stipulation.
7.1.2.2	Policy Constraints	No stipulation.
7.1.2.3	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.
7.1.2.4	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.
7.1.2.5	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

TrustID Certificates under this Policy will use the following OIDs for signatures: id-dsa-with-sha1 {iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}. Certificates under this Policy will use the following OIDs for identifying the algorithm the subject key was generated for: Encryption {iso(1) member-body(2) us(840) (113549) pkcs(1) pkcs-1(1) 1} publicnumber {iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}. Certificates containing keys generated for use with DSA or for use with KEA will be signed with id-dsa-with-sha1. Keys generated for use with RSA will be signed using sha-1WithRSAEncryption. For alternate algorithms, only PMA-approved algorithms may be used.

7.1.4 Name Forms

Every DN must be in the form of an X.501 printable string.

7.1.5 Name Constraints

Subject and Issuer DNs must comply with PKIX standards and be present in all 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 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 https://secure.identrust.com/certificates/policy/ts."

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 Numbers

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.

8 POLICY ADMINISTRATION

8.1 POLICY CHANGE PROCEDURES

This Policy will be reviewed on a yearly basis. Errors, updates, or suggested changes to this document should be communicated to the contact in Section 1.4. Such communication must include a description of the change, a change justification, and contact information for the person requesting the change. All policy changes under consideration by the PMA will be disseminated to interested parties (see Section 8.2) for a period of at least one month. The PMA will accept, with modifications, or reject the proposed change after completion of the review period.

8.1.1 List of Items That Can Change Without Notification

Editorial and typographical corrections, changes to contact details and other minor changes that do not materially impact Participants may be changed without notice and are not subject to the notification requirements herein.

8.1.2 List of Items Subject to Notification Requirement

All changes to this Policy that may materially affect Participants are subject to the notification requirement. Prior to making any such changes to this Policy, the PMA will notify all CAs that are directly cross-certified with the PMA.

8.1.3 Comment Period, Process and Procedure

Affected Participants may file comments with the PMA within 30 days of original notice. If the proposed change is modified as a result of such comments, a new notice of the modified proposed change would be given.

8.2 PUBLICATION AND NOTIFICATION POLICIES

8.2.1 Copy of Policy

A copy of this Policy is available in electronic form on the Internet at https://secure.identrust.com/certificates/policy/ts., and via email from helpdesk@Identrust.com. Approved Issuing CAs will post copies of, or links to, this Policy in their Repositories.

8.2.2 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 Certificate Holders of the proposed changes. The PMA will also post a notice of the proposal on the PMA World Wide Web site.

8.2.2.1	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.
8.2.2.2	Final Change Notice	The PMA will determine the period for final change notice.

8.2.3 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 assig a new OID for the modified policy.

8.3 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.

8.4 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 ANNEX A: CA/B Forum Baseline Requirements Version 1.1.9

CA/Browser Forum
Baseline Requirements
for the
Issuance and Management
of
Publicly-Trusted Certificates, v.1.1.9

(Current through adoption of Ballot 129 on 4 August 2014)

Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v. 1.1.9

This version 1.1.9 represents the Baseline Requirements, as adopted by the CA/Browser Forum as of Ballot 129, passed by the Forum on 4 August 2014.

These Baseline Requirements describe an integrated set of technologies, protocols, identity-proofing, lifecycle management, and auditing requirements that are necessary (but not sufficient) for the issuance and management of Publicly-Trusted Certificates; Certificates that are trusted by virtue of the fact that their corresponding Root Certificate is distributed in widely-available application software. The Requirements are not mandatory for Certification Authorities unless and until they become adopted and enforced by relying–party Application Software Suppliers.

Notice to Readers

This version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates present criteria established by the CA/Browser Forum for use by Certification Authorities when issuing, maintaining, and revoking publicly-trusted Certificates. The Requirements may be revised from time to time, as appropriate, in accordance with procedures adopted by the CA/Browser Forum. Because one of the primary beneficiaries of these Requirements is the end user, the Forum openly invites anyone to make recommendations and suggestions by email to the CA/Browser Forum at questions@cabforum.org. The Forum members value all input, regardless of source, and will seriously consider all such input.

The CA/Browser Forum

The CA/Browser Forum is a voluntary organization of Certification Authorities and suppliers of Internet browser and other relying-party software applications. Membership as of August 2014 is as follows:

Certification Authorities

- Actalis
- ANF Autoridad de Certificación
- AS Sertifitseerimiskeskus
- Buypass AS
- Camerfirma
- Certinomis
- certSIGN
- Certum
- Chunghwa Telecom Co., Ltd.
- Comodo CA Ltd
- D-TRUST GmbH
- DanID A/S
- DigiCert, Inc.
- Digidentity BV
- E-TUGRA Inc.
- GlobalSign
- GoDaddy.com, Inc.
- Izenpe S.A.
- Japan Certification Services, Inc.
- Kamu Sertifikasyon Merkezi
- KPN Corporate Market BV
- Logius PKIoverheid
- Network Solutions, LLC
- Open Access Technology International
- OpenTrust
- Prvni certifikacni autorita, a.s.
- QuoVadis Ltd.
- SECOM Trust Systems CO., Ltd.
- Shanghai Electronic CA Center Co. Ltd
- Skaitmeninio sertifikavimo centras (SSC)
- StartCom Certification Authority
- Swisscom (Switzerland) Ltd
- SwissSign AG
- Symantec Corporation
- Taiwan CA (TWCA)
- TrendMicro
- Trustis Limited
- Trustwave
- TURKTRUST
- Visa
- Wells Fargo Bank, N.A.
- WoSign

Relying-Party Application Software Suppliers

- Apple
- Google Inc.
- Microsoft Corporation
- Opera Software ASA
- The Mozilla Foundation

Other groups that have participated in the development of these Requirements include the AICPA/CICA WebTrust for Certification Authorities task force and ETSI ESI. Participation by such groups does not imply their endorsement, recommendation, or approval of the final product.

Document History

Ver.	Ballot	Description	Adopted	Effective*
1.0.0	62	Version 1.0 of the Baseline Requirements Adopted	22-Nov-11	01-Jul-12
1.0.1	71	Revised Auditor Qualifications	08-May-12	01-Jan-13
1.0.2	75	Non-critical Name Constraints allowed as exception to RFC 5280	08-Jun-12	08-Jun-12
1.0.3	78	Revised Domain/IP Address Validation, High Risk Requests, and Data Sources	22-Jun-12	22-Jun-12
1.0.4	80	OCSP responses for non-issued certificates	02-Aug-12	01-Feb-13 01-Aug-13
--	83	Network and Certificate System Security Requirements adopted	03-Aug-13	01-Jan-13
1.0.5	88	User-assigned country code of XX allowed	12-Sep-12	12-Sep-12
1.1.0	--	Published as Version 1.1 with no changes from 1.0.5	14-Sep-12	14-Sep-12
1.1.1	93	Reasons for Revocation and Public Key Parameter checking	07-Nov-12	07-Nov-12 01-Jan-13
1.1.2	96	Wildcard certificates and new gTLDs	20-Feb-13	20-Feb-13 01-Sep-13
1.1.3	97	Prevention of Unknown Certificate Contents	21-Feb-13	21-Feb-13
1.1.4	99	Add DSA Keys (BR v.1.1.4)	3-May-2013	3-May-2013
1.1.5	102	Revision to subject domainComponent language in section 9.2.3	31-May-2013	31-May-2013
1.1.6	105	Technical Constraints for Subordinate Certificate Authorities	29-July-2013	29-July-2013
1.1.7	112	Replace Definition of "Internal Server Name" with “Internal Name”	3-April-2014	3-April-2014
1.1.8	120	Affiliate Authority to Verify Domain	5-June-2014	5-June-2014
1.1.9	129	Clarification of PSL mentioned in section 11.1.3	4-Aug-2014	4-Aug-2014

* Effective Date and Additionally Relevant Compliance Date(s)

Implementers’ Note: Version 1.1 of these SSL Baseline Requirements was published on September 14, 2012. Version 1.1 of WebTrust’s SSL Baseline Audit Criteria and ETSI Technical Standard Electronic Signatures and Infrastructures (ESI) 102 042 version 2.3.1 incorporate version 1.1 of these Baseline Requirements. The CA/Browser Forum continues to improve the Baseline Requirements, and we encourage all CAs to conform to each revision on the date specified without awaiting a corresponding update to an applicable audit criterion. In the event of a conflict between an existing audit criterion and a guideline revision, we will communicate with the audit community and attempt to resolve any uncertainty, and we will respond to implementation questions directed to questions@cabforum.org. Our coordination with compliance auditors will continue as we develop guideline revision cycles that harmonize with the revision cycles for audit criteria, the compliance auditing periods and cycles of CAs, and the CA/Browser Forum’s guideline implementation dates**.**

Relevant Compliance Dates

Compliance	Summary Description (See Full Text for Details)
2013-01-01	For RSA public keys, CAs SHALL confirm that the value of the public exponent is an odd number equal to 3 or more. (Appendix A – (4) General Requirements for Public Keys)
2013-01-01	CAs SHALL support an OCSP capability using the GET method.
2013-01-01	CAs SHALL comply with the Network and Certificate System Security Requirements.
2013-08-01	OCSP Responders SHALL NOT respond "Good" for Unissued Certificates.
2013-09-01	CAs SHALL revoke any certificate where wildcard character occurs in the first label position immediately to the left of a "registry-controlled" label or "public suffix".
2013-12-31	CAs SHALL confirm that the RSA Public Key is at least 2048 bits or that one of the following ECC curves is used: P-256, P-384, or P-521. A Root CA Certificate issued prior to 31 Dec. 2010 with an RSA key size less than 2048 bits MAY still serve as a trust anchor.
2015-04-01	CAs SHALL NOT issue certificates with validity periods longer than 39 months.
2015-11-01	Issuance of Certificates with Reserved IP Address or Internal Server Name prohibited.
2016-10-01	All Certificates with Reserved IP Address or Internal Server Name must be revoked.

1 Scope

The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates describe a subset of the requirements that a Certification Authority must meet in order to issue Publicly Trusted Certificates. Except where explicitly stated otherwise, these requirements apply only to relevant events that occur on or after the Effective Date.

These Requirements do not address all of the issues relevant to the issuance and management of Publicly-Trusted Certificates. The CA/Browser Forum may update the Requirements from time to time, in order to address both existing and emerging threats to online security. In particular, it is expected that a future version will contain more formal and comprehensive audit requirements for delegated functions.

This version of the Requirements only addresses Certificates intended to be used for authenticating servers accessible through the Internet. Similar requirements for code signing, S/MIME, time-stamping, VoIP, IM, Web services, etc. may be covered in future versions.

These Requirements do not address the issuance, or management of Certificates by enterprises that operate their own Public Key Infrastructure for internal purposes only, and for which the Root Certificate is not distributed by any Application Software Supplier.

These Requirements are applicable to all Certification Authorities within a chain of trust. They are to be flowed down from the Root Certification Authority through successive Subordinate Certification Authorities.

2 Purpose

The primary goal of these Requirements is to enable efficient and secure electronic communication, while addressing user concerns about the trustworthiness of Certificates. The Requirements also serve to inform users and help them to make informed decisions when relying on Certificates.

3 References

ETSI TS 119 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - General Requirements and Guidance

ETSI TS 102 042, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates

FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001

ISO 21188:2006, Public key infrastructure for financial services -- Practices and policy framework

NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications
http://csrc.nist.gov/publications/nistpubs/800-89/SP-800-89_November2006.pdf

RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997

RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999

RFC2560, Request for Comments: 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP M. Myers, et al, June 1999

RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003

RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006

RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007

RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008

WebTrust for Certification Authorities Version 2.0, available at http://www.webtrust.org/homepagedocuments/item27839.aspx

X.509v3, ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

4 Definitions

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

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

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA.

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

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

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

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

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

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Control: "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such

entity; (2) control the election of a majority of the directors; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country: Either a member of the United Nations OR a geographic region recognized as a sovereign nation by at least two UN member nations.

Cross Certificate: A certificate that is used to establish a trust relationship between two Root CAs.

Delegated Third Party: A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

Domain Name: The label assigned to a node in the Domain Name System.

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

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Effective Date: These Requirements come into force on 1 July 2012.

Enterprise RA: An employee or agent of an organization Unaffiliated with the CA who authorizes issuance of Certificates to that organization.

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys) or if there is clear evidence that the specific method used to generate the Private Key was flawed.

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

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

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

Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Parent Company: A company that Controls a Subsidiary Company.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 17.6 (Auditor Qualifications).

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Requirements: This document.

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

Root CA: 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.

Sovereign State: A state or country that administers its own government, and is not dependent upon, or subject to, another power.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

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

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

Subsidiary Company: A company that is controlled by a Parent Company.

Technically Constrained Subordinate CA Certificate: 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.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialists: Someone who performs the information verification duties specified by these Requirements.

Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date.

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

5 Abbreviations and Acronyms

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As

DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VOIP	Voice Over Internet Protocol

6 Conventions

Terms not otherwise defined in these Requirements shall be as defined in applicable agreements, user manuals, Certificate Policies and Certification Practice Statements, of the CA.

The key words “MUST”, “MUST NOT”, "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in these Requirements shall be interpreted in accordance with RFC 2119.

7 Certificate Warranties and Representations

7.1 By the CA

By issuing a Certificate, the CA makes the Certificate Warranties listed in Section 7.1.2 to the Certificate Beneficiaries listed in 7.1.1.

7.1.1 Certificate Beneficiaries

Certificate Beneficiaries include, but are not limited to, the following:

1. The Subscriber that is a party to the Subscriber or Terms of Use Agreement for the Certificate;

2. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and

3. All Relying Parties who reasonably rely on a Valid Certificate.

7.1.2 Certificate Warranties

The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with these Requirements and its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

1. **Right to Use Domain Name or IP Address:** That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;

2. **Authorization for Certificate:** That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;

3. **Accuracy of Information:** That, at the time of issuance, the CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject: organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;

4. **No Misleading Information:** That, at the time of issuance, the CA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;

5. **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 9.2.4 and 11.2; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;

6. **Subscriber Agreement:** That, if the CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are Affiliated, the Applicant Representative acknowledged and accepted the Terms of Use;

7. **Status:** That the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and

8. **Revocation:** That the CA will revoke the Certificate for any of the reasons specified in these Requirements.

7.2 By the Applicant

The CA SHALL require, as part of the Subscriber or Terms of Use Agreement, that the Applicant make the commitments and warranties set forth in Section 10.3.2 of these Requirements, for the benefit of the CA and the Certificate Beneficiaries.

8 Community and Applicability

The CA SHALL at all times:

1. Issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates;
2. Comply with these Requirements;
3. Comply with the audit requirements set forth in Section 17; and
4. Be licensed as a CA in each jurisdiction where it operates, if licensing is required by the law of such jurisdiction for the issuance of Certificates.

If a court or government body with jurisdiction over the activities covered by these Requirements determines that the performance of any mandatory requirement is illegal, then such requirement is considered reformed to the minimum extent necessary to make the requirement valid and legal. This applies only to operations or certificate issuances that

are subject to the laws of that jurisdiction. The parties involved SHALL notify the CA / Browser Forum of the facts, circumstances, and law(s) involved, so that the CA/Browser Forum may revise these Requirements accordingly.

8.1 Certificate Policies

8.1.1 Implementation

The CA SHALL develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements.

8.1.2 Disclosure

The CA SHALL publicly disclose its Certificate Policy and/or Certification Practice Statement through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA SHALL publicly disclose its CA business practices to the extent required by the CA's selected audit scheme (see Section 17.1). The disclosures MUST include all the material required by RFC 2527 or RFC 3647, and MUST be structured in accordance with either RFC 2527 or RFC 3647.

8.2 Commitment to Comply

The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version. The CA MAY fulfill this requirement by incorporating these Requirements directly into its Certificate Policy and/or Certification Practice Statements or by incorporating them by reference using a clause such as the following (which MUST include a link to the official version of these Requirements):

> [Name of CA] conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

8.3 Trust model

The CA SHALL disclose all Cross Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue).

9 Certificate Content and Profile

9.1 Issuer Information

An Issuing CA SHALL populate the issuer field of each Certificate issued after the adoption of these Requirements in accordance with the following subsections.

9.1.1 Issuer Common Name Field

Certificate Field: issuer:commonName (OID 2.5.4.3)

Required/Optional: Optional

Contents: If present in a Certificate, the Common Name field MUST include a name that accurately identifies the Issuing CA.

9.1.2 Issuer Domain Component Field

Certificate Field: issuer:domainComponent (OID 0.9.2342.19200300.100.1.25)

Required/Optional: Optional.

Contents: If present in a Certificate, the Domain Component field MUST include all components of the Issuing CA's Registered Domain Name in ordered sequence, with the most significant component, closest to the root of the namespace, written last.

9.1.3 Issuer Organization Name Field

Certificate Field: issuer:organizationName (OID 2.5.4.10)

Required/Optional: Required

Contents: This field MUST contain the name (or abbreviation thereof), trademark, or other meaningful identifier for the CA, provided that they accurately identify the CA. The field MUST NOT contain a generic designation such as “Root” or “CA1”.

9.1.4 Issuer Country Name Field

Certificate Field: issuer:countryName (OID 2.5.4.6)

Required/Optional: Required

Contents: This field MUST contain the two-letter ISO 3166-1 country code for the country in which the issuer’s place of business is located.

9.2 Subject Information

By issuing the Certificate, the CA represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate’s issuance date, all of the Subject Information was accurate. CAs SHALL NOT include a Domain Name in a Subject attribute except as specified in Sections 9.2.1 and 9.2.2 below

9.2.1 Subject Alternative Name Extension

Certificate Field: extensions:subjectAltName

Required/Optional: Required

Contents: This extension MUST contain at least one entry. Each entry MUST be either a dNSName containing the Fully-Qualified Domain Name or an iPAddress containing the IP address of a server. The CA MUST confirm that the Applicant controls the Fully-Qualified Domain Name or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate. Wildcard FQDNs are permitted.

As of the Effective Date of these Requirements, prior to the issuance of a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name, the CA SHALL notify the Applicant that the use of such Certificates has been deprecated by the CA / Browser Forum and that the practice will be eliminated by October 2016. Also as of the Effective Date, the CA SHALL NOT issue a certificate with an Expiry Date later than 1 November 2015 with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name. Effective 1 October 2016, CAs SHALL revoke all unexpired Certificates whose subjectAlternativeName extension or Subject commonName field contains a Reserved IP Address or Internal Server Name.

9.2.2 Subject Common Name Field

Certificate Field: subject:commonName (OID 2.5.4.3)

Required/Optional: Deprecated (Discouraged, but not prohibited)

Contents: If present, this field MUST contain a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate’s subjectAltName extension (see Section 9.2.1).

9.2.3 Subject Domain Component Field

Certificate Field: subject:domainComponent (OID 0.9.2342.19200300.100.1.25)

Required/Optional: Optional.

Contents: If present, this field MUST contain a label from a Domain Name.

The domainComponent fields for each Domain Name MUST be in a single ordered sequence containing all labels from the Domain name. The labels MUST be encoded in the reverse order to the on-wire representation of domain names in the DNS protocol, so that the label closest to the root is encoded first.

The CA MUST ensure that the certificate is issued with the consent of, and according to procedures established by, the owner of each Domain Name.

9.2.4 Subject Distinguished Name Fields

a. Certificate Field: subject:organizationName (OID 2.5.4.10)

Optional.

Contents: If present, the subject:organizationName field MUST contain either the Subject's name or DBA as verified under Section 11.2. The CA may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if theofficial record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name". Because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, the CA MAY use the subject:organizationName field to convey a natural person Subject's name or DBA.

b. Certificate Field: Number and street: subject:streetAddress (OID: 2.5.4.9)

Optional if the subject:organizationName field is present.

Prohibited if the subject:organizationName field is absent.

Contents: If present, the subject:streetAddress field MUST contain the Subject's street address information as verified under Section 11.2.

c. Certificate Field: subject:localityName (OID: 2.5.4.7)

Required if the subject:organizationName field is present and the subject:stateOrProvinceName field is absent.

Optional if the subject:organizationName and subject:stateOrProvinceName fields are present.

Prohibited if the subject:organizationName field is absent.

Contents: If present, the subject:localityName field MUST contain the Subject's locality information as verified under Section 11.2. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 9.2.5, the localityName field MAY contain the Subject's locality and/or state or province information as verified under Section 11.2.

d. Certificate Field: subject:stateOrProvinceName (OID: 2.5.4.8)

Required if the subject:organizationName field is present and subject:localityName field is absent.

Optional if subject:organizationName and subject:localityName fields are present.

Prohibited if the subject:organizationName field is absent.

Contents: If present, the subject:stateOrProvinceName field MUST contain the Subject's state or province information as verified under Section 11.2. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 9.2.5, the subject:stateOrProvinceName field MAY contain the full name of the Subject's country information as verified under Section 11.2.5.

e. Certificate Field: subject:postalCode (OID: 2.5.4.17)

Optional if the subject:organizationName field is present.

Prohibited if the subject:organizationName field is absent.

Contents: If present, the subject:postalCode field MUST contain the Subject's zip or postal information as verified under Section 11.2

9.2.5 Subject Country Name Field

Certificate Field: subject:countryName (OID: 2.5.4.6)

Required if the subject:organizationName field is present.

Optional if the subject:organizationName field is absent.

Contents: If the subject:organizationName field is present, the subject:countryName MUST contain the two-letter ISO 3166-1 country code associated with the location of the Subject verified under Section 11.2. If the subject:organizationName field is absent, the subject:countryName field MAY contain the two-letter ISO 3166-1 country code associated with the Subject as verified in accordance with Section 11.2.5. If a Country is not represented by an official ISO 3166-1 country code, the CA MAY specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

9.2.6 Subject Organizational Unit Field

Certificate Field: subject:organizationalUnitName

Optional

The CA SHALL implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with Section 11.2 and the Certificate also contains subject:organizationName, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 11.2.

9.2.7 Other Subject Attributes

All other optional attributes, when present within the subject field, MUST contain information that has been verified by the CA. Optional attributes MUST NOT contain metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

9.3 Certificate Policy Identification

This section describes the content requirements for the Root CA, Subordinate CA, and Subscriber Certificates, as they relate to the identification of Certificate Policy.

9.3.1 Reserved Certificate Policy Identifiers

The following Certificate Policy identifiers are reserved for use by CAs as an optional means of asserting compliance with these Requirements as follows:

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) domain-validated(1)} (2.23.140.1.2.1), if the Certificate complies with these Requirements but lacks Subject Identity Information that is verified in accordance with Section 11.2.

If the Certificate asserts the policy identifier of 2.23.140.1.2.1, then it MUST NOT include organizationName, streetAddress, localityName, stateOrProvinceName, or postalCode in the Subject field.

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) subject-identity-validated(2)} (2.23.140.1.2.2), if the Certificate complies with these Requirements and includes Subject Identity Information that is verified in accordance with Section 11.2.

If the Certificate asserts the policy identifier of 2.23.140.1.2.2, then it MUST also include organizationName, localityName, stateOrProvinceName (if applicable), and countryName in the Subject field.

9.3.2 Root CA Certificates

A Root CA Certificate SHOULD NOT contain the certificatePolicies extension.

9.3.3 Subordinate CA Certificates

A Certificate issued after the Effective Date to a Subordinate CA that is not an Affiliate of the Issuing CA:

1. MUST include one or more explicit policy identifiers that indicates the Subordinate CA's adherence to and compliance with these Requirements (i.e. either the CA/Browser Forum reserved identifiers or identifiers defined by the CA in its Certificate Policy and/or Certification Practice Statement) and

2. MUST NOT contain the "anyPolicy" identifier (2.5.29.32.0).

A Certificate issued after the Effective Date to a Subordinate CA that is an affiliate of the Issuing CA:

1. MAY include the CA/Browser Forum reserved identifiers or an identifier defined by the CA in its Certificate Policy and/or Certification Practice Statement to indicate the Subordinate CA's compliance with these Requirements and

2. MAY contain the "anyPolicy" identifier (2.5.29.32.0) in place of an explicit policy identifier.

A Subordinate CA SHALL represent, in its Certificate Policy and/or Certification Practice Statement, that all Certificates containing a policy identifier indicating compliance with these Requirements are issued and managed in accordance with these Requirements.

9.3.4 Subscriber Certificates

A Certificate issued to a Subscriber MUST contain one or more policy identifier(s), defined by the Issuing CA, in the Certificate's certificatePolicies extension that indicates adherence to and compliance with these Requirements. CAs complying with these Requirements MAY also assert one of the reserved policy OIDs in such Certificates.

The issuing CA SHALL document in its Certificate Policy or Certification Practice Statement that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with these Requirements.

9.4 Validity Period

9.4.1 Subscriber Certificates

Subscriber Certificates issued after the Effective Date MUST have a Validity Period no greater than 60 months.

Except as provided for below, Subscriber Certificates issued after 1 April 2015 MUST have a Validity Period no greater than 39 months.

Beyond 1 April 2015, CAs MAY continue to issue Subscriber Certificates with a Validity Period greater than 39 months but not greater than 60 months provided that the CA documents that the Certificate is for a system or software that:

(a) was in use prior to the Effective Date;

(b) is currently in use by either the Applicant or a substantial number of Relying Parties;

(c) fails to operate if the Validity Period is shorter than 60 months;

(d) does not contain known security risks to Relying Parties; and

(e) is difficult to patch or replace without substantial economic outlay.

9.5 Public Key

The CA SHALL reject a certificate request if the requested Public Key does not meet the requirements set forth in Appendix A or if it has a known weak Private Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys).

9.6 Certificate Serial Number

CAs SHOULD generate non-sequential Certificate serial numbers that exhibit at least 20 bits of entropy.

9.7 Technical Constraints in Subordinate CA Certificates via Name Constraints and EKU

For a Subordinate CA Certificate to be considered Technically Constrained, the certificate MUST include an Extended Key Usage (EKU) extension specifying all extended key usages that the Subordinate CA Certificate is authorized to issue certificates for. The anyExtendedKeyUsage KeyPurposeId MUST NOT appear within this extension.

If the Subordinate CA Certificate includes the id-kp-serverAuth extended key usage, then the Subordinate CA Certificate MUST include the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:-

(a) For each dNSName in permittedSubtrees, the CA MUST confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of section 11.1.

(b) For each iPAddress range in permittedSubtrees, the CA MUST confirm that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf.

(c) For each DirectoryName in permittedSubtrees the CA MUST confirm the Applicants and/or Subsidiary's Organizational name and location such that End Entity certificates issued from the subordinate CA Certificate will be in compliancy with section 9.2.4 and 9.2.5.

If the Subordinate CA Certificate is not allowed to issue certificates with an iPAddress, then the Subordinate CA Certificate MUST specify the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Subordinate CA Certificate MUST include within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4 address range of 0.0.0.0/0). The Subordinate CA Certificate MUST also include within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0). Otherwise, the Subordinate CA Certificate MUST include at least one iPAddress in permittedSubtrees.

A decoded example for issuance to the domain and sub domains of example.com by organization :- Example LLC, Boston, Massachusetts, US would be:-

X509v3 Name Constraints:

Permitted:

DNS:example.com

DirName: C=US, ST=MA, L=Boston, O=Example LLC

Excluded:

IP:0.0.0.0/0.0.0.0

IP:0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0

If the Subordinate CA is not allowed to issue certificates with dNSNames, then the Subordinate CA Certificate MUST include a zero-length dNSName in excludedSubtrees. Otherwise, the Subordinate CA Certificate MUST include at least one dNSName in permittedSubtrees.

9.8 Additional Technical Requirements

The CA SHALL meet the technical requirements set forth in Appendix A - Cryptographic Algorithm and Key Requirements, and

Appendix B – Certificate Extensions, and Appendix C – User Agent Verification.

10 Certificate Application

10.1 Documentation Requirements

Prior to the issuance of a Certificate, the CA SHALL obtain the following documentation from the Applicant:

1. A certificate request, which may be electronic; and
2. An executed Subscriber or Terms of Use Agreement, which may be electronic.

The CA SHOULD obtain any additional documentation the CA determines necessary to meet these Requirements.

10.2 Certificate Request

10.2.1 General

Prior to the issuance of a Certificate, the CA SHALL obtain from the Applicant a certificate request in a form prescribed by the CA and that complies with these Requirements. One certificate request MAY suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in Section 11.3, provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. The certificate request MAY be made, submitted and/or signed electronically.

10.2.2 Request and Certification

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

10.2.3 Information Requirements

The certificate request MAY include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for the CA to obtain from the Applicant in order to comply with these Requirements and the CA's Certificate Policy and/or Certification Practice Statement. In cases where the certificate request does not contain all the necessary information about the Applicant, the CA SHALL obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. The CA SHALL establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

Applicant information MUST include, but not be limited to, at least one Fully-Qualified Domain Name or IP address to be included in the Certificate's SubjectAltName extension.

10.2.4 Subscriber Private Key

Parties other than the Subscriber SHALL NOT archive the Subscriber Private Key.

If the CA or any of its designated RAs generated the Private Key on behalf of the Subscriber, then the CA SHALL encrypt the Private Key for transport to the Subscriber.

If the CA or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then the CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

10.2.5 Subordinate CA Private Key

Parties other than the Subordinate CA SHALL NOT archive the Subordinate CA Private Keys. If the Issuing CA generated the Private Key on behalf of the Subordinate CA, then the Issuing CA SHALL encrypt the Private Key for transport to the Subordinate CA. If the Issuing CA becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then the Issuing

CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

10.3 Subscriber and Terms of Use Agreement

10.3.1 General

Prior to the issuance of a Certificate, the CA SHALL obtain, for the express benefit of the CA and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with the CA, or
2. The Applicant's agreement to the Terms of Use agreement.

The CA SHALL implement a process to ensure that each Subscriber or Terms of Use Agreement is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. The CA MAY use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each certificate request, or a

single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber or Terms of Use Agreement.

10.3.2 Agreement Requirements

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

1. **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;

2. **Protection of Private Key:** An obligation and warranty by the Applicant to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);

3. **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;

4. **Use of Certificate:** An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber or Terms of Use Agreement;

5. **Reporting and Revocation:** An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request the CA to revoke the Certificate, in the event that: (a) any information in the Certificate is, or becomes, incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate;

6. **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.

7. Responsiveness: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.

8. **Acknowledgment and Acceptance:** An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Agreement or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

11 Verification Practices

11.1 Authorization

11.1.1 Authorization by Domain Name Registrant

For each Fully-Qualified Domain Name listed in a Certificate, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant (or the Applicant's Parent Company, Subsidiary Company, or Affiliate, collectively referred to as "Applicant" for the purposes of this section) either is the Domain Name Registrant or has control over the FQDN by:

1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar;

2. Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar;

3. Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field;

4. Communicating with the Domain's administrator using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN;

5. Relying upon a Domain Authorization Document;

6. Having the Applicant demonstrate practical control over the FQDN by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the FQDN; or

7. Using any other method of confirmation, provided that the CA maintains documented evidence that the method of confirmation establishes that the Applicant is the Domain Name Registrant or has control over the FQDN to at least the same level of assurance as those methods previously described.

Note: For purposes of determining the appropriate domain name level or Domain Namespace, the registerable Domain Name is the second-level domain for generic top-level domains (gTLD) such as .com, .net, or .org, or, if the Fully Qualified Domain Name contains a 2 letter Country Code Top-Level Domain (ccTLD), then the domain level is whatever is allowed for registration according to the rules of that ccTLD.

If the CA relies upon a Domain Authorization Document to confirm the Applicant's control over a FQDN, then the Domain Authorization Document MUST substantiate that the communication came from either the Domain Name Registrant (including any private, anonymous, or proxy registration service) or the Domain Name Registrar listed in the WHOIS. The CA MUST verify that the Domain Authorization Document was either (i) dated on or after the certificate request date or (ii) used by the CA to verify a previously issued certificate and that the Domain Name's WHOIS record has not been modified since the previous certificate's issuance.

11.1.2 Authorization for an IP Address

For each IP Address listed in a Certificate, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant has control over the IP Address by:

1. Having the Applicant demonstrate practical control over the IP Address by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the IPAddress;

2. Obtaining documentation of IP address assignment from the Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC);

3. Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name under Section 11.1.1; or

4. Using any other method of confirmation, provided that the CA maintains documented evidence that the method of confirmation establishes that the Applicant has control over the IP Address to at least the same level of assurance as the methods previously described.

Note: IPAddresses may be listed in Subscriber Certificates using IPAddress in the subjectAltName extension or in Subordinate CA Certificates via IPAddress in permittedSubtrees within the Name Constraints extension.

11.1.3 Wildcard Domain Validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, the CA MUST establish and follow a documented procedure† that determines if the wildcard character occurs in the first label position to the left of a "registry-controlled" label or "public suffix" (e.g. "*.com", "*.co.uk", see RFC 6454 Section 8.2 for further explanation).

If a wildcard would fall within the label immediately to the left of a registry-controlled† or public suffix, CAs MUST refuse issuance unless the applicant proves its rightful control of the entire Domain Namespace. (e.g. CAs MUST NOT issue "*.co.uk" or "*.local", but MAY issue "*.example.com" to Example Co.).

Prior to September 1, 2013, each CA MUST revoke any valid certificate that does not comply with this section of the Requirements.

†Determination of what is “registry-controlled” versus the registerable portion of a Country Code Top-Level

Domain Namespace is not standardized at the time of writing and is not a property of the DNS itself. Current best practice is to consult a “public suffix list” such as http://publicsuffix.org/ (PSL), and to retrieve a fresh copy regularly. If using the PSL, a CA SHOULD consult the "ICANN DOMAINS" section only, not the "PRIVATE DOMAINS" section. The PSL is updated regularly to contain new gTLDs delegated by ICANN, which are listed in the "ICANN DOMAINS" section. A CA is not prohibited from issuing a Wildcard Certificate to the Registrant of an entire gTLD, provided that control of the entire namespace is demonstrated in an appropriate way.

11.1.4 New gTLD Domains

CAs SHOULD NOT issue Certificates containing a new gTLD under consideration by ICANN. Prior to issuing a Certificate containing an Internal Server Name with a gTLD that ICANN has announced as under consideration to make operational, the CA MUST provide a warning to the applicant that the gTLD may soon become resolvable and that, at that time, the CA will revoke the Certificate unless the applicant promptly registers the domain name.

Within 30 days after ICANN has approved a new gTLD for operation, as evidenced by publication of a contract with the gTLD operator on [www.ICANN.org] each CA MUST (1) compare the new gTLD against the CA’s records of valid certificates and (2) cease issuing Certificates containing a Domain Name that includes the new gTLD until after the CA has first verified the Subscriber's control over or exclusive right to use the Domain Name in accordance with Section 11.1.

Within 120 days after the publication of a contract for a new gTLD is published on [www.icann.org], CAs MUST revoke each Certificate containing a Domain Name that includes the new gTLD unless the Subscriber is either thE Domain Name Registrant or can demonstrate control over the Domain Name.

11.2 Verification of Subject Identity Information

If the Applicant requests a Certificate that will contain Subject Identity Information comprised only of the countryName field, then the CA SHALL verify the country associated with the Subject using a verification process meeting the requirements of Section 11.2.5 and that is described in the CA’s Certificate Policy and/or Certification Practice Statement. If the Applicant requests a Certificate that will contain the countryName field and other Subject Identity Information, then the CA SHALL verify the identity of the Applicant, and the authenticity of the Applicant Representative’s certificate request using a verification process meeting the requirements of this Section 11.2 and that is described in the CA’s Certificate Policy and/or Certification Practice Statement. The CA SHALL inspect any document relied upon under this Section for alteration or falsification.

11.2.1 Identity

If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the identity and address of the organization and that the address is the Applicant’s address of existence or operation. The CA SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Applicant’s legal creation, existence, or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation Letter.

The CA MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant’s identity and address.

Alternatively, the CA MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

11.2.2 11.2.2 DBA/Tradename

If the Subject Identity Information is to include a DBA or tradename, the CA SHALL verify the Applicant’s right to use the DBA/tradename using at least one of the following:

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;

2. A Reliable Data Source;

3. Communication with a government agency responsible for the management of such DBAs or tradenames;

4. An Attestation Letter accompanied by documentary support; or

5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

11.2.3 Authenticity of Certificate Request

If the Applicant for a Certificate containing Subject Identity Information is an organization, the CA SHALL use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request.

The CA MAY use the sources listed in section 11.2.1 to verify the Reliable Method of Communication. Provided that the CA uses a Reliable Method of Communication, the CA MAY establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate.

In addition, the CA SHALL establish a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then the CA SHALL NOT accept any certificate requests that are outside this specification. The CA SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

11.2.4 Verification of Individual Applicant

If an Applicant subject to this Section 11.2 is a natural person, then the CA SHALL verify the Applicant's name, Applicant's address, and the authenticity of the certificate request.

The CA SHALL verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). The CA SHALL inspect the copy for any indication of alteration or falsification.

The CA SHALL verify the Applicant's address using a form of identification that the CA determines to be reliable, such as a government ID, utility bill, or bank or credit card statement. The CA MAY rely on the same government issued ID that was used to verify the Applicant's name.

The CA SHALL verify the certificate request with the Applicant using a Reliable Method of Communication.

11.2.5 Verification of Country

If the subject:countryName field is present, then the CA SHALL verify the country associated with the Subject using one of the following: (a) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address; (b) the ccTLD of the requested Domain Name; (c) information provided by the Domain Name Registrar; or (d) a method identified in Section 11.2.1. The CA SHOULD implement a process to screen proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.

11.3 Age of Certificate Data

Section 9.4 limits the validity period of Subscriber Certificates. The CA MAY use the documents and data provided in Section 11 to verify certificate information, provide that the CA obtained the data or document from a source specified under Section 11 no more than thirty-nine (39) months prior to issuing the Certificate.

11.4 Denied List

In accordance with Section 15.3.2, the CA SHALL maintain an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. The CA SHALL use this information to identify subsequent suspicious certificate requests.

11.5 High Risk Requests

The CA SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements.

11.6 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the CA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The CA SHOULD consider the following during its evaluation:

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

Databases maintained by the CA, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under Section 11.

12 Certificate Issuance by a Root CA

Certificate issuance by the Root CA SHALL require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

Root CA Private Keys MUST NOT be used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates, and OCSP Response verification Certificates);
4. Certificates issued solely for the purpose of testing products with Certificates issued by a Root CA; and
5. Subscriber Certificates, provided that:
    a. The Root CA uses a 1024-bit RSA signing key that was created prior to the Effective Date;
    b. The Applicant's application was deployed prior to the Effective Date;
    c. The Applicant's application is in active use by the Applicant or the CA uses a documented process to establish that the Certificate's use is required by a substantial number of Relying Parties;
    d. The CA follows a documented process to determine that the Applicant's application poses no known security risks to Relying Parties; and
    e. The CA documents that the Applicant's application cannot be patched or replaced without substantial economic outlay.

13 Certificate Revocation and Status Checking

13.1 Revocation

13.1.1 Revocation Request

The CA SHALL provide a process for Subscribers to request revocation of their own Certificates. The process MUST be described in the CA's Certificate Policy or Certification Practice Statement. The CA SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and related inquiries.

13.1.2 Certificate Problem Reporting

The CA SHALL provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA SHALL publicly disclose the instructions through a readily accessible online means.

13.1.3 Investigation

The CA SHALL begin investigation of a Certificate Problem Report within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

1. The nature of the alleged problem;

2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;

3. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and

4. Relevant legislation.

13.1.4 Response

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

13.1.5 Reasons for Revoking a Subscriber Certificate

The CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate;

2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;

3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (also see Section 10.2.4) or no longer complies with the requirements of Appendix A;

4. The CA obtains evidence that the Certificate was misused;

5. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber or Terms of Use Agreement;

6. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);

7. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;

8. The CA is made aware of a material change in the information contained in the Certificate;

9. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;

10. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;

11. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;

12. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;

13. The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;

14. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or

15. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

13.1.6 Reasons for Revoking a Subordinate CA Certificate

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

1. The Subordinate CA requests revocation in writing;

2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;

3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Appendix A,

4. The Issuing CA obtains evidence that the Certificate was misused;

5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with these Baseline Requirements or the applicable Certificate Policy or Certification Practice Statement;

6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;

7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;

8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;

9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement; or

10. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

13.2 Certificate Status Checking

13.2.1 Mechanisms

The CA SHALL make revocation information for Subordinate Certificates and Subscriber Certificates available in accordance with Appendix B.

If the Subscriber Certificate is for a high-traffic FQDN, the CA MAY rely on stapling, in accordance with [RFC4366], to distribute its OCSP responses. In this case, the CA SHALL ensure that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshake. The CA SHALL enforce this requirement on the Subscriber either contractually, through the Subscriber or Terms of Use Agreement, or by technical review measures implement by the CA.

13.2.2 Repository

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

For the status of Subscriber Certificates:

1. If the CA publishes a CRL, then the CA SHALL update and reissue CRLs at least once every seven days, and the value of the nextUpdate field MUST NOT be more than ten days beyond the value of the thisUpdate field; and

2. The CA SHALL update information provided via an Online Certificate Status Protocol at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days.

For the status of Subordinate CA Certificates:

1. The CA SHALL update and reissue CRLs at least (i) once every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field MUST NOT be more than twelve months beyond the value of the thisUpdate field; and

2. The CA SHALL update information provided via an Online Certificate Status Protocol at least (i) every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate.

Effective 1 January 2013, the CA SHALL support an OCSP capability using the GET method for Certificates issued in accordance with these Requirements.

13.2.3 Response Time

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

13.2.4 Deletion of Entries

Revocation entries on a CRL or OCSP Response MUST NOT be removed until after the Expiry Date of the revoked Certificate.

13.2.5 OCSP Signing

OCSP responses MUST conform to RFC2560 and/or RFC5019. OCSP responses MUST either:

1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or

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

In the latter case, the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC2560.

13.2.6 Response for non-issued certificates

If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder SHOULD NOT respond with a "good" status. The CA SHOULD monitor the responder for such requests as part of its security response procedures.

Effective 1 August 2013, OCSP responders for CAs which are not Technically Constrained in line with Section 9.7 MUST NOT respond with a "good" status for such certificates.

13.2.7 Certificate Suspension

The Repository MUST NOT include entries that indicate that a Certificate is suspended.

14 Employees and Third Parties

14.1 Trustworthiness and Competence

14.1.1 Identity and Background Verification

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

14.1.2 Training and Skill Level

The CA SHALL provide all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements.

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

Validation Specialists engaged in Certificate issuance SHALL maintain skill levels consistent with the CA's training and performance programs.

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

The CA SHALL require all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in these Requirements.

14.2 Delegation of Functions

14.2.1 General

The CA MAY delegate the performance of all, or any part, of Section 11 of these Requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of Section 11.

Before the CA authorizes a Delegated Third Party to perform a delegated function, the CA SHALL contractually require the Delegated Third Party to:

1) Meet the qualification requirements of Section 14.1, when applicable to the delegated function;

2) Retain documentation in accordance with Section 15.3.2;

3) Abide by the other provisions of these Requirements that are applicable to the delegated function; and

4) Comply with (a) the CA's Certificate Policy/Certification Practice Statement or (b) the Delegated Third Party's practice statement that the CA has verified complies with these Requirements.

The CA SHALL verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 14 and the document retention and event logging requirements of Section 15.

If a Delegated Third Party fulfills any of the CA's obligations under Section 11.5 (High Risk Requests), the CA SHALL verify that the process used by the Delegated Third Party to identify and further verify High Risk Certificate Requests provides at least the same level of assurance as the CA's own processes

14.2.2 Compliance Obligation

The CA SHALL internally audit each Delegated Third Party's compliance with these Requirements on an annual basis.

14.2.3 Allocation of Liability

For delegated tasks, the CA and any Delegated Third Party MAY allocate liability between themselves contractually as they determine, but the CA SHALL remain fully responsible for the performance of all parties in accordance with these Requirements, as if the tasks had not been delegated.

14.2.4 Enterprise RAs

The CA MAY designate an Enterprise RA to verify certificate requests from the Enterprise RA's own organization.

The CA SHALL NOT accept certificate requests authorized by an Enterprise RA unless the following requirements are satisfied:

1. The CA SHALL confirm that the requested Fully-Qualified Domain Name(s) are within the Enterprise RA's verified Domain Namespace (see Section 7.1.2 para 1).

2. If the certificate request includes a Subject name of a type other than a Fully-Qualified Domain Name, the CA SHALL confirm that the name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject. For example, the CA SHALL NOT issue a Certificate containing the Subject name "XYZ Co." on the authority of Enterprise RA "ABC Co.", unless the two companies are affiliated (see Section 11.1) or "ABC Co." is the agent of "XYZ Co". This requirement applies regardless of whether the accompanying requested Subject FQDN falls within the Domain Namespace of ABC Co.'s Registered Domain Name.

The CA SHALL impose these limitations as a contractual requirement on the Enterprise RA and monitor compliance by the Enterprise RA.

15 Data Records

15.1 Documentation and Event Logging

The CA and each Delegated Third Party SHALL record details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. The CA SHALL make these records available to its Qualified Auditor as proof of the CA's compliance with these Requirements.

15.2 Events and Actions

The CA SHALL record at least the following events:

1. CA key lifecycle management events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction; and
    b. Cryptographic device lifecycle management events.
2. CA and Subscriber Certificate lifecycle management events, including:
    a. Certificate requests, renewal, and re-key requests, and revocation;
    b. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
    c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    d. Acceptance and rejection of certificate requests;
    e. Issuance of Certificates; and
    f. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
    a. Successful and unsuccessful PKI system access attempts;
    b. PKI and security system actions performed;

c. Security profile changes;

d. System crashes, hardware failures, and other anomalies;

e. Firewall and router activities; and

f. Entries to and exits from the CA facility.

Log entries MUST include the following elements:

1. Date and time of entry;

2. Identity of the person making the journal entry; and

3. Description of the entry.

15.3 Retention

15.3.1 Audit Log Retention

The CA SHALL retain any audit logs generated after the Effective Date for at least seven years. The CA SHALL make these audit logs available to its Qualified Auditor upon request.

15.3.2 Documentation Retention

The CA SHALL retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid.

16 Data Security

16.1 Objectives

The CA SHALL develop, implement, and maintain a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;

2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;

3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;

4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and

5. Comply with all other security requirements applicable to the CA by law.

16.2 Risk Assessment

The CA's security program MUST include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;

2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and

3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

16.3 Security Plan

Based on the Risk Assessment, the CA SHALL develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate

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

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

16.4 Business Continuity

In addition, the CA SHALL document a business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. The CA is not required to publicly disclose its business continuity plans but SHALL make the business continuity plan and security plan of Section 15.3 available to the CA's auditors upon request. The CA SHALL annually test, review, and update these procedures.

The business continuity plan MUST include:

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

16.5 System Security

The Certificate Management Process MUST include:

1. physical security and environmental controls;
2. system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
3. network security and firewall management, including port restrictions and IP address filtering;
4. user management, separate trusted-role assignments, education, awareness, and training; and
5. logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

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

16.6 Private Key Protection

The CA SHALL protect its Private Key in a system or device that has been validated as meeting at least FIPS 140 level 3 or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats. The CA SHALL implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the Private Key outside the validated system or device specified above MUST consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Key. The CA SHALL encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part. The Private Key SHALL be backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

17 Audit

Certificates that are capable of being used to issue new certificates MUST either be Technically Constrained in line with section 9.7 and audited in line with section 17.9 only, or Unconstrained and fully audited in line with all remaining requirements from section 17. A Certificate is deemed as capable of being used to issue new certificates if it contains an X.509v3 basicConstraints extension, with the cA boolean set to true and is therefore by definition a Root CA Certificate or a Subordinate CA Certificate.

17.1 Eligible Audit Schemes

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

1. WebTrust for Certification Authorities v2.0;
2. A national scheme that audits conformance to ETSI TS 102 042;
3. A scheme that audits conformance to ISO 21188:2006; or
4. If a Government CA is required by its Certificate Policy to use a different internal audit scheme, it MAY use such scheme provided that the audit either (a) encompasses all requirements of one of the above schemes or (b) consists of comparable criteria that are available for public review.

Whichever scheme is chosen, it MUST incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit MUST be conducted by a Qualified Auditor, as specified in Section 17.6.

17.2 Audit Period

The period during which the CA issues Certificates SHALL be divided into an unbroken sequence of audit periods.

An audit period MUST NOT exceed one year in duration.

17.3 Audit Report

The Audit Report SHALL state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in Section 9.3.1. The CA SHALL make the Audit Report publicly available. The CA is not required to make publicly available any general audit findings that do not impact the overall audit opinion. For both government and commercial CAs, the CA SHOULD make its Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, and if so requested by an Application Software Supplier, the CA SHALL provide an explanatory letter signed by the Qualified Auditor.

17.4 Pre-Issuance Readiness Audit

If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 17.1, then no pre-issuance readiness assessment is necessary.

If the CA does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in Section 17.1, then, before issuing Publicly-Trusted Certificates, the CA SHALL successfully complete a point-in time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in

Section 17.1. The point-in-time readiness assessment SHALL be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.

17.5 Audit of Delegated Functions

If a Delegated Third Party is not currently audited in accordance with Section 17 and is not an Enterprise RA, then prior to certificate issuance the CA SHALL ensure that the domain control validation process required under Section 11.1 has been properly performed by the Delegated Third Party by either (1) using an out-of-band mechanism involving at least one human who is acting either on behalf of the CA or on behalf of the Delegated Third Party to confirm the authenticity of the certificate request or the information supporting the certificate request or (2) performing the domain control validation process itself.

If the CA is not using one of the above procedures and the Delegated Third Party is not an Enterprise RA, then the CA SHALL obtain an audit report, issued under the auditing standards that underlie the accepted audit schemes found in Section 17.1, that provides an opinion whether the Delegated Third Party's performance complies with either the Delegated Third Party's practice statement or the CA's Certificate Policy and/or Certification Practice Statement. If the opinion is that the Delegated Third Party does not comply, then the CA SHALL not allow the Delegated Third Party to continue performing delegated functions.

The audit period for the Delegated Third Party SHALL NOT exceed one year (ideally aligned with the CA's audit). However, if the CA or Delegated Third Party is under the operation, control, or supervision of a Government Entity and the audit scheme is completed over multiple years, then the annual audit MUST cover at least the core controls that are required to be audited annually by such scheme plus that portion of all non-core controls that are allowed to be conducted less frequently, but in no case may any non-core control be audited less often than once every three years.

17.6 Auditor Qualifications

The CA's audit SHALL be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;

2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 17.1);

3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;

4. (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ETSI TS 119 403, or accredited to conduct such audits under an equivalent national scheme, or accredited by a national accreditation body in line with ISO 27006 to carry out ISO 27001 audits;

5. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;

6. Bound by law, government regulation, or professional code of ethics; and

7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

17.7 Key Generation Ceremony

For Root CA Key Pairs created after the Effective Date that are either (i) used as Root CA Key Pairs or (ii) Key Pairs generated for a subordinate CA that is not the operator of the Root CA or an Affiliate of the Root CA, the CA SHALL:

1. prepare and follow a Key Generation Script,

2. have a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process, and

3. have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

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

1. prepare and follow a Key Generation Script and

2. have a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process.

In all cases, the CA SHALL:

1. generate the keys in a physically secured environment as described in the CA's Certificate Policy and/or Certification Practice Statement;

2. generate the CA keys using personnel in trusted roles under the principles of multiple person control and split knowledge;

3. generate the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's Certificate Policy and/or Certification Practice Statement;

4. log its CA key generation activities; and

5. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

17.8 Regular Quality Assessment Self Audits

During the period in which the CA issues Certificates, the CA SHALL monitor adherence to its Certificate Policy, Certification Practice Statement and these Requirements and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken. Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in Section 16.3, the CA SHALL strictly control the service quality of Certificates issued or containing information verified by a Delegated Third Party by having a Validation Specialist employed by the CA perform ongoing quarterly audits against a randomly selected sample of at least the greater of one certificate or three percent of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last sample was taken. The CA SHALL review each Delegated Third Party's practices and procedures to ensure that the Delegated Third Party is in compliance with these Requirements and the relevant Certificate Policy and/or Certification Practice Statement.

17.9 Regular Quality Assessment of Technically Constrained Subordinate CAs

During the period in which a Technically Constrained Subordinate CA issues Certificates, the CA which signed the Subordinate CA SHALL monitor adherence to the CA's Certificate Policy and the Subordinate CA's Certification Practice Statement. On at least a quarterly basis, against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by the Subordinate CA, during the period commencing immediately after the previous audit sample was taken, the CA shall ensure all applicable Baseline Requirements are met.

18 Liability and Indemnification

18.1 Liability to Subscribers and Relying Parties

If the CA has issued and managed the Certificate in compliance with these Requirements and its Certificate Policy and/or Certification Practice Statement, the CA MAY disclaim liability to the Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such Certificate beyond those specified in the CA's Certificate Policy and/or Certification Practice Statement. If the CA has not issued or managed the Certificate in compliance with these Requirements and its Certificate Policy and/or Certification Practice Statement, the CA MAY seek to limit its liability to the Subscriber and to Relying Parties, regardless of the cause of action or legal theory involved, for any and all claims, losses or damages suffered as a result of the use or reliance on such Certificate by

any appropriate means that the CA desires. If the CA chooses to limit its liability for Certificates that are not issued or managed in compliance with these Requirements or its Certificate Policy and/or Certification Practice Statement, then the CA SHALL include the limitations on liability in the CA's Certificate Policy and/or Certification Practice Statement.

18.2 Indemnification of Application Software Suppliers

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Root CA do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, except in the case where the CA is a government entity, the CA SHALL 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 Certificate issued by the CA, 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 Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

18.3 Root CA Obligations

The Root CA SHALL be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with these Requirements, and for all liabilities and indemnification obligations of the Subordinat CA under these Requirements, as if the Root CA were the Subordinate CA issuing the Certificates.

19 Appendix A - Cryptographic Algorithm and Key Requirements (Normative)

Certificates MUST meet the following requirements for algorithm type and key size.

(1) Root CA Certificates

	Validity period beginning on or before 31 Dec 2010	Validity period beginning after 31 Dec 2010
Digest algorithm	MD5 (NOT RECOMMENDED), SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048**	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits)	L= 2048, N= 224 or L= 2048, N= 256, L= 2048, N= 224 or L= 2048, N= 256	L= 2048, N= 224 or L= 2048, N= 256, L= 2048, N= 224 or L= 2048, N= 256

(2) Subordinate CA Certificates

	Validity period beginning on or before 31 Dec 2010 and ending on or before 31 Dec 2013	Validity period beginning after 31 Dec 2010 or ending after 31 Dec 2013
Digest algorithm	SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits)	L= 2048, N= 224 or L= 2048, N= 256, L= 2048, N= 224 or L= 2048, N= 256	L= 2048, N= 224 or L= 2048, N= 256, L= 2048, N= 224 or L= 2048, N= 256

(3) Subscriber Certificates

	Validity period ending on or before 31 Dec 2013	Validity period ending after 31 Dec 2013
Digest algorithm	SHA1*, SHA-256, SHA-384 or SHA-512	SHA1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus	1024	2048

size (bits)		
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits)	L= 2048, N= 224 or L= 2048, N= 256, L= 2048, N= 224 or L= 2048, N= 256	L= 2048, N= 224 or L= 2048, N= 256, L= 2048, N= 224 or L= 2048, N= 256

* SHA-1 MAY be used with RSA keys until SHA-256 is supported widely by browsers used by a substantial portion of relying-parties worldwide.

** A Root CA Certificate issued prior to 31 Dec. 2010 with an RSA key size less than 2048 bits MAY still serve as a trust anchor for Subscriber Certificates issued in accordance with these Requirements. L and N (the bit lengths of modulus p and divisor q, respectively) are described in the Digital Signature Standard, FIPS 186-3 (http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf).

(4) General requirements for public keys

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

DSA: Although FIPS 800-57 says that domain parameters may be made available at some accessible site, compliant DSA certificates MUST include all domain parameters. This is to insure maximum interoperability among relying party software. The CA MUST confirm that the value of the public key has the unique correct representation and range in the field, and that the key has the correct order in the subgroup. [Source: Section 5.3.1, NIST SP 800-89].

ECC: The CA SHOULD confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.5 and 5.6.2.6, respectively, NIST SP 800-56A].

20 Appendix B – Certificate Extensions (Normative)

This appendix specifies the requirements for Certificate extensions for Certificates generated after the Effective Date.

(1) Root CA Certificate

Root Certificates MUST be of type X.509 v3.

A. basicConstraints

This extension MUST appear as a critical extension.

The cA field MUST be set true.

The pathLenConstraint field SHOULD NOT be present.

B. keyUsage

This extension MUST be present and MUST be marked critical.

Bit positions for keyCertSign and cRLSign MUST be set.

If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.

C. certificatePolicies

This extension SHOULD NOT be present.

D. extendedKeyUsage

This extension MUST NOT be present.

(2) Subordinate CA Certificate

Subordinate CA Certificates MUST be of type X.509 v3.

A. certificatePolicies

This extension MUST be present and SHOULD NOT be marked critical.

certificatePolicies:policyIdentifier (Required)

The following fields MAY be present if the Subordinate CA is not an Affiliate of the entity that controls the Root CA.

certificatePolicies:policyQualifiers:policyQualifierId (Optional)

☐ id-qt 1 [RFC 5280].

certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

☐ HTTP URL for the Root CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the CA.

B. cRLDistributionPoints

This extension MUST be present and MUST NOT be marked critical.

It MUST contain the HTTP URL of the CA’s CRL service.

C. authorityInformationAccess

With the exception of stapling, which is noted below, this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA’s OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

It SHOULD also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). See Section 13.2.1 for details.

The HTTP URL of the Issuing CA's OCSP responder MAY be omitted, provided that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshakes [RFC4366].

D. basicConstraints

This extension MUST be present and MUST be marked critical.

The cA field MUST be set true.

The pathLenConstraint field MAY be present.

E. keyUsage

This extension MUST be present and MUST be marked critical.

Bit positions for keyCertSign and cRLSign MUST be set.

If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.

F. **nameConstraints** (optional)

If present, this extension SHOULD be marked critical*.

* Non-critical Name Constraints are an exception to RFC 5280 that MAY be used until the Name

Constraints extension is supported by Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide.

G. **extkeyUsage** (optional)

For Subordinate CA Certificates to be Technically constrained in line with section 9.8, then either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present**.

Other values MAY be present.

If present, this extension SHOULD be marked non-critical.

** Generally Extended Key Usage will only appear within end entity certificates (as highlighted in RFC 5280 (4.2.1.12)), however, Subordinate CAs MAY include the extension to further protect relying parties until the use of the extension is consistent between Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide.

(3) Subscriber Certificate

A. certificatePolicies

This extension MUST be present and SHOULD NOT be marked critical.

certificatePolicies:policyIdentifier (Required)

☐ A Policy Identifier, defined by the issuing CA, that indicates a Certificate Policy asserting the issuing CA's adherence to and compliance with these Requirements.

The following extensions MAY be present:

certificatePolicies:policyQualifiers:policyQualifierId (Recommended)

☐ id-qt 1 [RFC 5280].

certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

☐ HTTP URL for the Subordinate CA's Certification Practice Statement, Relying Party Agreement or other pointer to online information provided by the CA.

B. cRLDistributionPoints

This extension MAY be present. If present, it MUST NOT be marked critical, and it MUST contain the HTTP URL of the CA's CRL service. See Section 13.2.1 for details.

C. authorityInformationAccess

With the exception of stapling, which is noted below, this extension MUST be present.

It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

It SHOULD also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). See Section 13.2.1 for details.

The HTTP URL of the Issuing CA's OCSP responder MAY be omitted provided that the Subscriber "staples" OCSP responses for the Certificate in its TLS handshakes [RFC4366].

D. basicConstraints (optional)

If present, the cA field MUST be set false.

E. keyUsage (optional)

If present, bit positions for keyCertSign and cRLSign MUST NOT be set.

F. extKeyUsage (required)

Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present. id-kp-emailProtection [RFC5280] MAY be present.

Other values SHOULD NOT be present.

(4) All Certificates

All other fields and extensions MUST be set in accordance with RFC 5280. The CA SHALL NOT issue a Certificate that contains a keyUsage flag, extendedKeyUsage value, Certificate extension, or other data not specified in this Appendix B unless the CA is aware of a reason for including the data in the Certificate.

CAs SHALL NOT issue a Certificate with:

(a) Extensions that do not apply in the context of the public Internet (such as an extendedKeyUsage value for a service that is only valid in the context of a privately managed network), unless:

i. such value falls within an OID arc for which the Applicant demonstrates ownership, or

ii. the Applicant can otherwise demonstrate the right to assert the data in a public context; or

(b) semantics that, if included, will mislead a Relying Party about the certificate information verified by the CA (such as including extendedKeyUsage value for a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

21 Appendix C - User Agent Verification (Normative)

The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired.