# CA/Browser Forum

# Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates

**CA/Browser Forum.**
Version 1.4.0~~3.9~~
August 29, 2016
cabforum.org

**TABLE OF CONTENTS**

# 1. INTRODUCTION

## *1.1. OVERVIEW*

This CP describes 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**

The CP 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. This document serves two purposes: to specify Baseline Requirements and to provide guidance and requirements for what a CA should include in its CPS. 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. In accordance with RFC 3647 and to facilitate a comparison of other certificate policies and CPSs (e.g. for policy mapping), this CP includes all sections of the RFC 3647 framework. However, rather than beginning with a "no stipulation" comment in all empty sections, the CA/Browser Forum is leaving such sections initially blank until a decision of "no stipulation" is made. The CA/Browser Forum may update these 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.

These Requirements only address 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.

## *1.2. DOCUMENT NAME AND IDENTIFICATION*

This certificate policy (CP) contains the requirements for the issuance and management of publicly-trusted SSL certificates, as adopted by the CA/Browser Forum.

The following Certificate Policy identifiers are reserved for use by CAs as an optional means of asserting compliance with this CP (OID arc 2.23.140.1.2) as follows:

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1);
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2); and
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) individual-validated(3)} (2.23.140.1.2.3).

### 1.2.1. Revisions

| 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<br>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<br>01-Jan-13 |
| 1.1.2 | 96 | Wildcard certificates and new gTLDs | 20-Feb-13 | 20-Feb-13<br>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 |
| 1.2.0 | 125 | CAA Records | 14-Oct-2014 | 15-Apr-2015 |
| 1.2.1 | 118 | SHA-1 Sunset | 16-Oct-2014 | 16-Jan-2015<br>1-Jan-2016<br>1-Jan-2017 |
| 1.2.2 | 134 | Application of RFC 5280 to Pre-certificates | 16-Oct-2014 | 16-Oct-2014 |
| 1.2.3 | 135 | ETSI Auditor Qualifications | 16-Oct-2014 | 16-Oct-2014 |
| 1.2.4 | 144 | Validation Rules for .onion Names | 18-Feb-2015 | 18-Feb-2015 |
| 1.2.5 | 148 | Issuer Field Correction | 2-April-2015 | 2-April-2015 |
| 1.3.0 | 146 | Convert Baseline Requirements to RFC 3647 Framework | 16-Apr-2015 | 16-Apr-2015 |
| 1.3.1 | 151 | Addition of Optional OIDs for Indicating Level of Validation | 28-Sep-2015 | 28-Sep-2015 |
| 1.3.2 | 156 | Amend Sections 1 and 2 of Baseline Requirements | 3-Dec-2015 | 3-Dec-2016 |
| 1.3.3 | 160 | Amend Section 4 of Baseline Requirements | 4-Feb-2016 | 4-Feb-2016 |
| 1.3.4 | 162 | Sunset of Exceptions | 15-Mar-2016 | 15-Mar-2016 |
| 1.3.5 | 168 | Baseline Requirements Corrections (Revised) | 10-May-2016 | 10-May-2016 |
| 1.3.6 | 171 | Updating ETSI Standards in CABF documents | 1-July-2016 | 1-July-2016 |
| 1.3.7 | 164 | Certificate Serial Number Entropy | 8-July-2016 | 30-Sep-2016 |
| 1.3.8 | 169 | Revised Validation Requirements | 5-Aug-2016 | 1-Mar-2017 |
| 1.3.9 | 174 | Reform of Requirements Relating to Conflicts with Local Law | 29-Aug-2016 | 27-Nov-2016 |
| 1.4.0 | 173 | Removal of requirement to cease use of public key due to incorrect info | 28-July-2016 | 11-Sep-2016 |

* Effective Date and Additionally Relevant Compliance Date(s)

### 1.2.2. Relevant Dates

| Compliance | Section(s) | Summary Description (See Full Text for Details) |
|---|---|---|
| 2013-01-01 | 6.1.6 | For RSA public keys, CAs SHALL confirm that the value of the public exponent is an odd number equal to 3 or more. |

| | | |
|---|---|---|
| 2013-01-01 | 4.9.10 | CAs SHALL support an OCSP capability using the GET method. |
| 2013-01-01 | 5 | CAs SHALL comply with the Network and Certificate System Security Requirements. |
| 2013-08-01 | 4.9.10 | OCSP Responders SHALL NOT respond "Good" for Unissued Certificates. |
| 2013-09-01 | 3.2.2.6 | 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 | 6.1.5 | 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. |
| 2015-01-16 | 7.1.3 | CAs SHOULD NOT issue Subscriber Certificates utilizing the SHA-1 algorithm with an Expiry Date greater than 1 January 2017. |
| 2015-04-01 | 6.3.2 | CAs SHALL NOT issue certificates with validity periods longer than 39 months, except in certain circumstances. |
| 2015-04-15 | 2.2 | A CA's CPS must state whether it reviews CAA Records, and if so, its policy or practice on processing CAA records for Fully Qualified Domain Names. |
| 2015-11-01 | 7.1.4.2.1 | Issuance of Certificates with Reserved IP Address or Internal Name prohibited. |
| 2016-01-01 | 7.1.3 | CAs MUST NOT issue any new Subscriber certificates or Subordinate CA certificates using the SHA-1 hash algorithm. |
| 2016-06-30 | 6.1.7 | CAs MUST NOT issue Subscriber Certificates directly from Root CAs. |
| 2016-06-30 | 6.3.2 | CAs MUST NOT issue Subscriber Certificates with validity periods longer than 39 months, regardless of circumstance. |
| 2016-09-30 | 7.1 | CAs SHALL generate Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG |
| 2016-10-01 | 7.1.4.2.1 | All Certificates with Reserved IP Address or Internal Name must be revoked. |
| 2016-12-03 | 1 and 2 | Ballot 156 amendments to sections 1.5.2, 2.3, and 2.4 are applicable |
| 2017-01-01 | 7.1.3 | CAs MUST NOT issue OCSP responder certificates using SHA-1 (inferred). |
| 2017-03-01 | 3.2.2.4 | CAs MUST follow revised validation requirements in section 3.2.2.4. |

## *1.3. PKI PARTICIPANTS*

The CA/Browser Forum is a voluntary organization of Certification Authorities and suppliers of Internet browser and other relying-party software applications.

### 1.3.1. Certification Authorities

Certification Authority (CA) is defined in Section 1.6, Definitions. Current CA Members of the CA/Browser Forum are listed here: https://cabforum.org/members.

### 1.3.2. Registration Authorities

The CA MAY delegate the performance of all, or any part, of Section 3.2 requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of Section 3.2.

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 5.3.1, when applicable to the delegated function;
(2) Retain documentation in accordance with Section 5.5.2;
(3) Abide by the other provisions of 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 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.

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 3.2) or "ABC Co." is the agent of "XYZ Co". This requirement applies regardless of whether the accompanying requested Subject FQDN falls within the Domain Namespace of ABC Co.'s Registered Domain Name.

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

### 1.3.3. Subscribers

As defined in Section 1.6.1 Definitions.

### 1.3.4. Relying Parties

Relying Party" and "Application Software Supplier" are defined in Section 1.6.1, Definitions. Current Members of the CA/Browser Forum who are Application Software Suppliers are listed here: https://cabforum.org/members.

### 1.3.5. Other Participants

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.

## *1.4. CERTIFICATE USAGE*

### 1.4.1. Appropriate Certificate Uses

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

### 1.4.2. Prohibited Certificate Uses

## *1.5. POLICY ADMINISTRATION*

### 1.5.1. Organization administering the document

This Certificate Policy for 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. This CP 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 this CP 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.

### 1.5.2. Contact person

Contact information for the CA/Browser Forum is available here: https://cabforum.org/leadership/

In this section of a CA's CPS, the CA shall provide a link to a web page or an email address for contacting the person or persons responsible for operation of the CA.

### 1.5.3. Person determining CPS suitability for the policy

No stipulation.

### 1.5.4. CPS approval procedures

No stipulation.

## *1.6. DEFINITIONS AND ACRONYMS*

### 1.6.1. 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 the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is 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.

**Authorization Domain Name:** The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

**Authorized Port:** One of the following ports: 80 (http), 443 (http), 115 (sftp), 25 (smtp), 22 (ssh).

**Base Domain Name:** The portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

**CAA:** From RFC 6844 (http:tools.ietf.org/html/rfc6844): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue."

**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 State by at least two UN member nations.

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

**CSPRNG:** A random number generator intended for use in cryptographic system.

**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 Contact:** The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.

**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:** 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 8.3 (Auditor Qualifications).

**Random Value:** A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

**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.

**Request Token:** A value derived in a method specified by the CA which binds this demonstration of control to the certificate request.

The Request Token SHALL incorporate the key used in the certificate request.

A Request Token MAY include a timestamp to indicate when it was created.

A Request Token MAY include other information to ensure its uniqueness.

A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation.

A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future.

A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation.

The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

**Required Website Content:** Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.

**Requirements:** The Baseline Requirements found in 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 Agreement or Terms of Use.

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

**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 or is the CA.

**Test Certificate:** A Certificate with a maximum validity period of 30 days and which: (i) includes a critical extension with the specified Test Certificate CABF OID, or (ii) is issued under a CA where there are no certificate paths/chains to a root certificate subject to these Requirements.

**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.

### 1.6.2. Acronyms

| | |
|---|---|
| AICPA | American Institute of Certified Public Accountants |
| CA | Certification Authority |
| CAA | Certification Authority Authorization |
| 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 |

### 1.6.3. References

ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

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.

Network and Certificate System Security Requirements, v.1.0, 1/1/2013.

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.

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.

RFC6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013.

WebTrust for Certification Authorities , SSL Baseline with Network Security, Version 2.0, available at http://www.webtrust.org/homepage-documents/item79806.pdf.

X.509, Recommendation ITU-T X.509 (10/2012) | ISO/IEC 9594-8:2014 (E), Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

### 1.6.4. 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.

## 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

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.

### *2.1. REPOSITORIES*

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

### *2.2. PUBLICATION OF INFORMATION*

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 8.1). 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. Effective as of 15 April 2015, section 4.2 of a CA's Certificate Policy and/or Certification Practice Statement (section 4.1 for CAs still conforming to RFC 2527) SHALL state whether the CA reviews CAA Records, and if so, the CA’s policy or practice on processing CAA Records for Fully Qualified Domain Names. The CA SHALL log all actions taken, if any, consistent with its processing practice.

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.

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.

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

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.

### *2.4. ACCESS CONTROLS ON REPOSITORIES*

The CA shall make its Repository public available in a read-only manner.

# 3. IDENTIFICATION AND AUTHENTICATION

## *3.1. NAMING*

### 3.1.1. Types of names

### 3.1.2. Need for names to be meaningful

### 3.1.3. Anonymity or pseudonymity of subscribers

### 3.1.4. Rules for interpreting various name forms

### 3.1.5. Uniqueness of names

### 3.1.6. Recognition, authentication, and role of trademarks

## *3.2. INITIAL IDENTITY VALIDATION*

### 3.2.1. Method to Prove Possession of Private Key

### 3.2.2. Authentication of Organization and Domain Identity

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 3.2.2.3 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 3.2.2.1 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.

#### *3.2.2.1. 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.

#### *3.2.2.2. 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.

#### *3.2.2.3. 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 3.2.2.1. 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.

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

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain.

The CA SHALL confirm that, as of the date the Certificate issues, either the CA or a Delegated Third Party has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below.

Completed confirmations of Applicant authority may be valid for the issuance of multiple certificates over time. In all cases, the confirmation must have been initiated within the time period specified in the relevant requirement (such as Section 3.3.1 of this document) prior to certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

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

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

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact directly with the Domain Name Registrar. This method may only be used if:

1. The CA authenticates the Applicant's identity under BR Section 3.2.2.1 and the authority of the Applicant Representative under BR Section 3.2.5, OR
2. The CA authenticates the Applicant's identity under EV Guidelines Section 11.2 and the agency of the Certificate Approver under EV Guidelines Section 11.8; OR
3. The CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

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

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

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

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

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

The CA or Delegated Third Party MAY resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

#### 3.2.2.4.3 Phone Contact with Domain Contact

Confirming the Applicant's control over the requested FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The CA or Delegated Third Party MUST place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.

Each phone call SHALL be made to a single number and MAY confirm control of multiple FQDNs, provided that the phone number is identified by the Domain Registrar as a valid contact method for every Base Domain Name being verified using the phone call.

#### 3.2.2.4.4 Constructed Email to Domain Contact

Confirming the Applicant's control over the requested FQDN by (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

Each email MAY confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed.

The Random Value SHALL be unique in each email.

The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient SHALL remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

#### 3.2.2.4.5 Domain Authorization Document

Confirming the Applicant's control over the requested FQDN by relying upon the attestation to the authority of the Applicant to request a Certificate contained in a Domain Authorization Document. The Domain Authorization Document MUST substantiate that the communication came from the Domain Contact. The CA MUST verify that the Domain Authorization Document was either (i) dated on or after the date of the domain validation request or (ii) that the WHOIS data has not materially changed since a previously provided Domain Authorization Document for the Domain Name Space.

#### 3.2.2.4.6 Agreed-Upon Change to Website

Confirming the Applicant's control over the requested FQDN by confirming one of the following under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of Domain

Validation, on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port:

1. The presence of Required Website Content contained in the content of a file or on a web page in the form of a meta tag. The entire Required Website Content MUST NOT appear in the request used to retrieve the file or web page, or
2. The presence of the Request Token or Request Value contained in the content of a file or on a webpage in the form of a meta tag where the Request Token or Random Value MUST NOT appear in the request.

If a Random Value is used, the CA or Delegated Third Party SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the certificate request, the timeframe permitted for reuse of validated information relevant to the certificate (such as in Section 3.3.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).

**Note:** Examples of Request Tokens include, but are not limited to: (i) a hash of the public key; (ii) a hash of the Subject Public Key Info [X.509]; and (iii) a hash of a PKCS#10 CSR. A Request Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests. This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR. E.g. echo date -u +%Y%m%d%H%M sha256sum <r2.csr | sed "s/[ -]//g" The script outputs: 201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f The CA should define in its CPS (or in a document referenced from the CPS) the format of Request Tokens it accepts.

**3.2.2.4.7 DNS Change**

Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value or Request Token in a DNS TXT or CAA record for an Authorization Domain Name or an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

If a Random Value is used, the CA or Delegated Third Party SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the certificate request, the timeframe permitted for reuse of validated information relevant to the certificate (such as in Section 3.3.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).

**3.2.2.4.8 IP Address**

Confirming the Applicant's control over the requested FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with section 3.2.2.5.

**3.2.2.4.9 Test Certificate**

Confirming the Applicant's control over the requested FQDN by confirming the presence of a non-expired Test Certificate issued by the CA on the Authorization Domain Name and which is accessible by the CA via TLS over an Authorized Port for the purpose of issuing a Certificate with the same Public Key as in the Test Certificate.

**3.2.2.4.10. TLS Using a Random Number**

Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value within a Certificate on the Authorization Domain Name which is accessible by the CA via TLS over an Authorized Port.

### *3.2.2.5. Authentication 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 IP Address;
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 3.2.2.4; 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.

### *3.2.2.6. 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.

### *3.2.2.7. Data Source Accuracy*

Prior to using any data source as a Reliable Data Source, the CA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The 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 this Section 3.2.

### 3.2.3. Authentication of Individual Identity

If an Applicant subject to this Section 3.2.3 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.

### 3.2.4. Non-verified Subscriber Information

### 3.2.5. Validation of Authority

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 3.2.2.1 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.

### 3.2.6. Criteria for Interoperation or Certification

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).

## *3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS*

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

### 3.3.2. Identification and Authentication for Re-key After Revocation

## *3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST*

# 4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

## *4.1. CERTIFICATE APPLICATION*

### 4.1.1. Who Can Submit a Certificate Application

In accordance with Section 5.5.2, 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.

### 4.1.2. Enrollment Process and Responsibilities

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 Agreement or Terms of Use, which may be electronic.

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

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 3.3.1, 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.

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.

## *4.2. CERTIFICATE APPLICATION PROCESSING*

### 4.2.1. Performing Identification and Authentication Functions

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.

Section 6.3.2 limits the validity period of Subscriber Certificates. The CA MAY use the documents and data provided in Section 3.2 to verify certificate information, provided that the CA obtained the data or document from a source specified under Section 3.2 no more than thirty-nine (39) months prior to issuing the Certificate.

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.

If a Delegated Third Party fulfills any of the CA's obligations under this section , 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

### 4.2.2. Approval or Rejection of Certificate Applications

CAs SHOULD NOT issue Certificates containing a new gTLD under consideration by ICANN. Prior to issuing a Certificate containing an Internal 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. When a gTLD is delegated by inclusion in the IANA Root Zone Database, the Internal Name becomes a Domain Name, and at such time, a Certificate with such gTLD, which may have complied with these Requirements at the time it was issued, will be in a violation of these Requirements, unless the CA has verified the Subscriber's rights in the Domain Name. The provisions below are intended to prevent such violation from happening.

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 3.2.2.4.

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.

#### 4.2.3. Time to Process Certificate Applications

No stipulation.

### *4.3. CERTIFICATE ISSUANCE*

#### 4.3.1. CA Actions during Certificate Issuance

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

#### 4.3.2. Notification of Certificate Issuance

No stipulation.

### *4.4. CERTIFICATE ACCEPTANCE*

#### 4.4.1. Conduct constituting certificate acceptance

No stipulation.

#### 4.4.2. Publication of the certificate by the CA

No stipulation.

#### 4.4.3. Notification of certificate issuance by the CA to other entities

No stipulation.

## *4.5. KEY PAIR AND CERTIFICATE USAGE*

### 4.5.1. Subscriber private key and certificate usage

See Section 9.6.3, provisions 2. and 4.

### 4.5.2. Relying party public key and certificate usage

No stipulation.

## *4.6. CERTIFICATE RENEWAL*

### 4.6.1. Circumstance for certificate renewal

No stipulation.

### 4.6.2. Who may request renewal

No stipulation.

### 4.6.3. Processing certificate renewal requests

No stipulation.

### 4.6.4. Notification of new certificate issuance to subscriber

No stipulation.

### 4.6.5. Conduct constituting acceptance of a renewal certificate

No stipulation.

### 4.6.6. Publication of the renewal certificate by the CA

No stipulation.

### 4.6.7. Notification of certificate issuance by the CA to other entities

No stipulation.

## *4.7. CERTIFICATE RE-KEY*

### 4.7.1. Circumstance for certificate re-key

No stipulation.

### 4.7.2. Who may request certification of a new public key

No stipulation.

### 4.7.3. Processing certificate re-keying requests

No stipulation.

### 4.7.4. Notification of new certificate issuance to subscriber

No stipulation.

### 4.7.5. Conduct constituting acceptance of a re-keyed certificate

No stipulation.

### 4.7.6. Publication of the re-keyed certificate by the CA

No stipulation.

### 4.7.7. Notification of certificate issuance by the CA to other entities

No stipulation.

## *4.8. CERTIFICATE MODIFICATION*

### 4.8.1. Circumstance for certificate modification

No stipulation.

### 4.8.2. Who may request certificate modification

No stipulation.

### 4.8.3. Processing certificate modification requests

No stipulation.

### 4.8.4. Notification of new certificate issuance to subscriber

No stipulation.

### 4.8.5. Conduct constituting acceptance of modified certificate

No stipulation.

### 4.8.6. Publication of the modified certificate by the CA

No stipulation.

### 4.8.7. Notification of certificate issuance by the CA to other entities

No stipulation.

## *4.9. CERTIFICATE REVOCATION AND SUSPENSION*

### 4.9.1. Circumstances for Revocation

#### *4.9.1.1. 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 or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;

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 Agreement or Terms of Use;

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).

#### *4.9.1.2. 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 Sections 6.1.5 and 6.1.6,

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 this CP 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).

### 4.9.2. Who Can Request Revocation

The Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.

### 4.9.3. Procedure for 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.

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.

### 4.9.4. Revocation Request Grace Period

No stipulation.

### 4.9.5. Time within which CA Must Process the Revocation Request

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.

### 4.9.6. Revocation Checking Requirement for Relying Parties

No stipulation.

(Note: Following certificate issuance, a certificate may be revoked for reasons stated in Section 4.9.1. Therefore, relying parties should check the revocation status of all certificates that contain a CDP or OCSP pointer.)

### 4.9.7. CRL Issuance Frequency

For the status of Subscriber Certificates:

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.

For the status of Subordinate CA Certificates:

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.

### 4.9.8. Maximum Latency for CRLs

No stipulation.

### 4.9.9. On-line Revocation/Status Checking Availability

OCSP responses MUST conform to RFC6960 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 RFC6960.

### 4.9.10. On-line Revocation Checking Requirements

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

For the status of Subscriber Certificates:

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:

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.

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 7.1.5 MUST NOT respond with a "good" status for such certificates.

### 4.9.11. Other Forms of Revocation Advertisements Available

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 Agreement or Terms of Use, or by technical review measures implemented by the CA.

### 4.9.12. Special Requirements Related to Key Compromise

See Section 4.9.1.

### 4.9.13. Circumstances for Suspension

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

### 4.9.14. Who Can Request Suspension

Not applicable.

### 4.9.15. Procedure for Suspension Request

Not applicable.

### 4.9.16. Limits on Suspension Period

Not applicable.

## *4.10. CERTIFICATE STATUS SERVICES*

### 4.10.1. Operational Characteristics

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

### 4.10.2. Service Availability

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

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

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

### 4.10.3. Optional Features

No stipulation.

## *4.11. END OF SUBSCRIPTION*

No stipulation.

## *4.12. KEY ESCROW AND RECOVERY*

### 4.12.1. Key escrow and recovery policy and practices

No stipulation.

### 4.12.2. Session key encapsulation and recovery policy and practices

Not applicable.

# 5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

The CA/Browser Forum's Network and Certificate System Security Requirements are incorporated by reference as if fully set forth herein.

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.

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'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.

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.

## *5.1. PHYSICAL SECURITY CONTROLS*

### 5.1.1. Site location and construction

### 5.1.2. Physical access

### 5.1.3. Power and air conditioning

### 5.1.4. Water exposures

### 5.1.5. Fire prevention and protection

### 5.1.6. Media storage

### 5.1.7. Waste disposal

#### 5.1.8. Off-site backup

### *5.2. PROCEDURAL CONTROLS*

#### 5.2.1. Trusted Roles

#### 5.2.2. Number of Individuals Required per Task

The CA 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.

#### 5.2.3. Identification and Authentication for Trusted Roles

#### 5.2.4. Roles Requiring Separation of Duties

### *5.3. PERSONNEL CONTROLS*

#### 5.3.1. Qualifications, Experience, and Clearance Requirements

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.

#### 5.3.2. Background Check Procedures

#### 5.3.3. Training Requirements and Procedures

The CA SHALL provide all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the CA's 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.

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.

#### 5.3.4. Retraining Frequency and Requirements

All personnel in Trusted Roles SHALL maintain skill levels consistent with the CA's training and performance programs.

#### 5.3.5. Job Rotation Frequency and Sequence

#### 5.3.6. Sanctions for Unauthorized Actions

#### 5.3.7. Independent Contractor Controls

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 5.3.3 and the document retention and event logging requirements of Section 5.4.1.

### 5.3.8. Documentation Supplied to Personnel

## *5.4. AUDIT LOGGING PROCEDURES*

### 5.4.1. Types of Events Recorded

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.

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.

### 5.4.2. Frequency for Processing and Archiving Audit Logs

### 5.4.3. Retention Period for Audit Logs

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

#### 5.4.4. Protection of Audit Log

#### 5.4.5. Audit Log Backup Procedures

#### 5.4.6. Audit Log Accumulation System (internal vs. external)

#### 5.4.7. Notification to Event-Causing Subject

#### 5.4.8. Vulnerability Assessments

Additionally, 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. [BR 16.2]

### *5.5. RECORDS ARCHIVAL*

#### 5.5.1. Types of Records Archived

#### 5.5.2. Retention Period for Archive

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

#### 5.5.3. Protection of Archive

#### 5.5.4. Archive Backup Procedures

#### 5.5.5. Requirements for Time-stamping of Records

#### 5.5.6. Archive Collection System (internal or external)

#### 5.5.7. Procedures to Obtain and Verify Archive Information

### *5.6. KEY CHANGEOVER*

### *5.7. COMPROMISE AND DISASTER RECOVERY*

#### 5.7.1. Incident and Compromise Handling Procedures

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

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

The business continuity plan 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.

#### 5.7.2. Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

#### 5.7.3. Recovery Procedures After Key Compromise

#### 5.7.4. Business Continuity Capabilities after a Disaster

### *5.8. CA OR RA TERMINATION*

## 6. TECHNICAL SECURITY CONTROLS

### *6.1. KEY PAIR GENERATION AND INSTALLATION*

#### 6.1.1. Key Pair Generation

#### *6.1.1.1. CA Key Pair Generation*

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.

#### *6.1.1.2. RA Key Pair Generation*

#### *6.1.1.3. Subscriber Key Pair Generation*

The CA SHALL reject a certificate request if the requested Public Key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 or if it has a known weak Private Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys).

### 6.1.2. Private Key Delivery to Subscriber

Parties other than the Subscriber SHALL NOT archive the Subscriber Private Key without authorization by the Subscriber.
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.

### 6.1.3. Public Key Delivery to Certificate Issuer

### 6.1.4. CA Public Key Delivery to Relying Parties

### 6.1.5. Key Sizes

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<br>or<br>L= 2048, N= 256, | L= 2048, N= 224<br>or<br>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<br>or<br>L= 2048, N= 256 | L= 2048, N= 224<br>Or<br>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 size (bits) | 1024 | 2048 |
| ECC curve | NIST P-256, P-384, or P-521 | NIST P-256, P-384, or P-521 |
| Minimum | L= 2048, N= 224 | L= 2048, N= 224 |

| | | |
|---|---|---|
| DSA modulus and divisor size (bits) | or<br>L= 2048, N= 256 | or<br>L= 2048, N= 256 |

* SHA-1 MAY be used with RSA keys in accordance with the criteria defined in Section 7.1.3.
** 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 186-4 (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf).

### 6.1.6. Public Key Parameters Generation and Quality Checking

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 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 56A: Revision 2].

### 6.1.7. Key Usage Purposes

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;

    e. The CA documents that the Applicant's application cannot be patched or replaced without substantial economic outlay.

    f. The CA signs the Subscriber Certificate on or before June 30, 2016; and

    g. The notBefore field in the Subscriber Certificate has a date on or before June 30, 2016.

## *6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS*

The CA SHALL implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the validated system or device specified above MUST consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA 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.

### 6.2.1. Cryptographic Module Standards and Controls

### 6.2.2. Private Key (n out of m) Multi-person Control

### 6.2.3. Private Key Escrow

### 6.2.4. Private Key Backup

See Section 5.2.2.

### 6.2.5. Private Key Archival

Parties other than the Subordinate CA SHALL NOT archive the Subordinate CA Private Keys without authorization by the Subordinate CA.

### 6.2.6. Private Key Transfer into or from a Cryptographic Module

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.

### 6.2.7. Private Key Storage on Cryptographic Module

The CA SHALL protect its Private Key in a system or device that has been validated as meeting at least FIPS 140 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.

### 6.2.8. Activating Private Keys

### 6.2.9. Deactivating Private Keys

### 6.2.10. Destroying Private Keys

### 6.2.11. Cryptographic Module Capabilities

## *6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT*

### 6.3.1. Public Key Archival

### 6.3.2. Certificate Operational Periods and Key Pair Usage Periods

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.

Until 30 June 2016, 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.

## *6.4. ACTIVATION DATA*

### 6.4.1. Activation data generation and installation

### 6.4.2. Activation data protection

### 6.4.3. Other aspects of activation data

## *6.5. COMPUTER SECURITY CONTROLS*

### 6.5.1. Specific Computer Security Technical Requirements

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

### 6.5.2. Computer Security Rating

## *6.6. LIFE CYCLE TECHNICAL CONTROLS*

### 6.6.1. System development controls

### 6.6.2. Security management controls

### 6.6.3. Life cycle security controls

## *6.7. NETWORK SECURITY CONTROLS*

### *6.8. TIME-STAMPING*

## 7. CERTIFICATE, CRL, AND OCSP PROFILES

### *7.1. CERTIFICATE PROFILE*

The CA SHALL meet the technical requirements set forth in Section 2.2 – Publication of Information, Section 6.1.5– Key Sizes, and Section 6.1.6 – Public Key Parameters Generation and Quality Checking.

Effective September 30, 2016, CAs SHALL generate non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

#### 7.1.1. Version Number(s)

Certificates MUST be of type X.509 v3.

#### 7.1.2. Certificate Content and Extensions; Application of RFC 5280

This section specifies the additional requirements for Certificate content and extensions for Certificates generated after the Effective Date.

##### *7.1.2.1. Root CA Certificate*

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.

e. Subject Information

The Certificate Subject MUST contain the following:

- countryName (OID 2.5.4.6). This field MUST contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.
- organizationName (OID 2.5.4.10): This field MUST be present and the contents MUST contain either the Subject CA's name or DBA as verified under Section 3.2.2.2. 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 the official record shows “Company Name Incorporated”, the CA MAY use “Company Name Inc.” or “Company Name”.

#### *7.1.2.2. Subordinate CA Certificate*

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).

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 (4.2.1.10), however, they 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 7.1.5, 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.

h. Subject Information

The Certificate Subject MUST contain the following:

- countryName (OID 2.5.4.6). This field MUST contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.
- organizationName (OID 2.5.4.10): This field MUST be present and the contents MUST contain either the Subject CA's name or DBA as verified under Section 3.2.2.2. 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 the official record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name".

#### *7.1.2.3. 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.

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). .

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)

The cA field MUST NOT be true.

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.

#### *7.1.2.4. 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 section 7.1.2.1, 7.1.2.2, or 7.1.2.3 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).

#### *7.1.2.5. Application of RFC 5280*

For purposes of clarification, a Precertificate, as described in RFC 6962 – Certificate Transparency, shall not be considered to be a "certificate" subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile under these Baseline Requirements.

### 7.1.3. Algorithm Object Identifiers

Effective 1 January 2016, CAs MUST NOT issue any new Subscriber certificates or Subordinate CA certificates using the SHA-1 hash algorithm. CAs MAY continue to sign certificates to verify OCSP responses using SHA1 until 1 January 2017. This Section 7.1.3 does not apply to Root CA or CA cross certificates. CAs MAY continue to use their existing SHA-1 Root Certificates. SHA-2 Subscriber certificates SHOULD NOT chain up to a SHA-1 Subordinate CA Certificate.

Effective 16 January 2015, CAs SHOULD NOT issue Subscriber Certificates utilizing the SHA-1 algorithm with an Expiry Date greater than 1 January 2017 because Application Software Providers are in the process of

deprecating and/or removing the SHA-1 algorithm from their software, and they have communicated that CAs and Subscribers using such certificates do so at their own risk.

### 7.1.4. Name Forms

#### *7.1.4.1. Issuer Information*

The content of the Certificate Issuer Distinguished Name field MUST match the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280, section 4.1.2.4.

#### *7.1.4.2. 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 or IP Address in a Subject attribute except as specified in Sections 3.2.2.4 or 3.2.2.5.

##### *7.1.4.2.1. 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 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 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 Name. Effective May 1, 2015, each CA SHALL revoke all unexpired Certificates with an Internal Name using onion as the right-most label in an entry in the subjectAltName Extension or commonName field unless such Certificate was issued in accordance with Appendix F of the EV Guidelines.

##### *7.1.4.2.2. Subject Distinguished Name Fields*

a. **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 7.1.4.2.1).
b. **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 3.2.2.2. 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 the official 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.

**c.** **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 3.2.2.1.

**d.** **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 3.2.2.1. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2(g), the localityName field MAY contain the Subject's locality and/or state or province information as verified under Section 3.2.2.1.

**e.** **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 3.2.2.1. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2(g), the subject:stateOrProvinceName field MAY contain the full name of the Subject's country information as verified under Section 3.2.2.1.

**f.** **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 3.2.2.1.

**g.** **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 3.2.2.1. 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 3.2.2.3. 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.

**h.** **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 3.2 and the Certificate

also contains subject:organizationName, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 3.2.2.1.

**i. 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.

#### *7.1.4.3. Subject Information – Subordinate CA Certificates*

By issuing a Subordinate CA 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.

### 7.1.5. Name Constraints

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 3.2.2.4.

(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 7.1.2.4 and 7.1.2.5.

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.

## 7.1.6. Certificate Policy Object Identifier

### *7.1.6.1. Reserved Certificate Policy Identifiers*

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

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) baseline-requirements(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 3.2.2.1 or Section 3.2.3.

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) baseline-requirements(2) organization-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 3.2.2.1.

> {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) individual-validated(3)} (2.23.140.1.2.3), if the Certificate complies with these Requirements and includes Subject Identity Information that is verified in accordance with Section 3.2.3.

If the Certificate asserts the policy identifier of 2.23.140.1.2.2, then it MUST also include organizationName, localityName (to the extent such field is required under Section 7.1.4.2.2), stateOrProvinceName (to the extent such field is required under Section 7.1.4.2.2), and countryName in the Subject field. If the Certificate asserts the policy identifier of 2.23.140.1.2.3, then it MUST also include (i) either organizationName or givenName and surname, (ii) localityName (to the extent such field is required under Section 7.1.4.2.2), (iii) stateOrProvinceName (to the extent required under Section 7.1.4.2.2), and (iv) countryName in the Subject field.

### *7.1.6.2. Root CA Certificates*

A Root CA Certificate SHOULD NOT contain the certificatePolicies extension.

### *7.1.6.3. 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.

#### *7.1.6.4. 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.

### 7.1.7. Usage of Policy Constraints Extension

### 7.1.8. Policy Qualifiers Syntax and Semantics

### 7.1.9. Processing Semantics for the Critical Certificate Policies Extension

## *7.2. CRL PROFILE*

### 7.2.1. Version number(s)

### 7.2.2. CRL and CRL entry extensions

## *7.3. OCSP PROFILE*

### 7.3.1. Version number(s)

### 7.3.2. OCSP extensions

## 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The CA SHALL at all times:

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

**Implementers' Note:** Version 1.1.6 of the SSL Baseline Requirements was published on July 29, 2013. Version 2.0 of WebTrust's Principles and Criteria for Certifiation Authorities - SSL Baseline with Network Security and ETSI's Electronic Signatures and Infrastructures (ESI) 102 042 incorporate version 1.1.6 of these Baseline Requirements and version 1.0 of the Network and Certificate System Security Requirements. The CA/Browser Forum continues to improve the Baseline Requirements while WebTrust and ETSI also continue to update their audit criteria. We encourage all CAs to conform to each revision herein 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.

## *8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT*

Certificates that are capable of being used to issue new certificates MUST either be Technically Constrained in line with section 7.1.5 and audited in line with section 8.7 only, or Unconstrained and fully audited in line with all remaining requirements from this section. 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.

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.

If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 8.1, 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 8.1, 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 8.1. 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.

## *8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR*

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 8.1);

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 ISO 17065 applying the requirements specified in ETSI EN 319 403;

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

## *8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY*

## *8.4. TOPICS COVERED BY ASSESSMENT*

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/ ETSI EN 319 411-1;

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 8.3.

If a Delegated Third Party is not currently audited in accordance with Section 8 and is not an Enterprise RA, then prior to certificate issuance the CA SHALL ensure that the domain control validation process required under Section 3.2.2.4 or IP address verification under 3.2.2.5 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 8.1, 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.

## *8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY*

## *8.6. COMMUNICATION OF RESULTS*

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 7.1.6.1. 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.

## *8.7. 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 8.1, 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.

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

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 CP are met.

# 9. OTHER BUSINESS AND LEGAL MATTERS

## *9.1. FEES*

### 9.1.1. Certificate issuance or renewal fees

### 9.1.2. Certificate access fees

### 9.1.3. Revocation or status information access fees

### 9.1.4. Fees for other services

### 9.1.5. Refund policy

## *9.2. FINANCIAL RESPONSIBILITY*

### 9.2.1. Insurance coverage

### 9.2.2. Other assets

### 9.2.3. Insurance or warranty coverage for end-entities

## *9.3. CONFIDENTIALITY OF BUSINESS INFORMATION*

### 9.3.1. Scope of confidential information

### 9.3.2. Information not within the scope of confidential information

### 9.3.3. Responsibility to protect confidential information

## *9.4. PRIVACY OF PERSONAL INFORMATION*

### 9.4.1. Privacy plan

### 9.4.2. Information treated as private

### 9.4.3. Information not deemed private

### 9.4.4. Responsibility to protect private information

### 9.4.5. Notice and consent to use private information

### 9.4.6. Disclosure pursuant to judicial or administrative process

### 9.4.7. Other information disclosure circumstances

## *9.5. INTELLECTUAL PROPERTY RIGHTS*

## *9.6. REPRESENTATIONS AND WARRANTIES*

### 9.6.1. CA Representations and Warranties

By issuing a Certificate, the CA makes the certificate warranties listed herein to the following Certificate Beneficiaries:

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

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 3.2 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 the same entity or are Affiliated, the Applicant Representative acknowledged 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.

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 Subordinate CA under these Requirements, as if the Root CA were the Subordinate CA issuing the Certificates

### 9.6.2. RA Representations and Warranties

### 9.6.3. Subscriber Representations and Warranties

The CA SHALL require, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.
Prior to the issuance of a Certificate, the CA SHALL obtain, for the express benefit of the CA and the Certificate Beneficiaries, either:

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

The CA SHALL implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement 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 Agreement or Terms of Use.

The Subscriber Agreement or Terms of Use 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 assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, 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 Agreement or Terms of Use;
5. **Reporting and Revocation:** An obligation and warranty to: (a) promptly request revocation of the Certificate, and cease using ~~a Certificate~~ it 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)~~ if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate~~;~~, and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.

6. **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
7. **Responsiveness:** An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. **Acknowledgment and Acceptance:** An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

### 9.6.4. Relying Party Representations and Warranties

### 9.6.5. Representations and Warranties of Other Participants

## *9.7. DISCLAIMERS OF WARRANTIES*

## *9.8. LIMITATIONS 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.

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.

## *9.9. INDEMNITIES*

### 9.9.1. Indemnification by CAs

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).

### 9.9.2. Indemnification by Subscribers

### 9.9.3. Indemnification by Relying Parties

### *9.10. TERM AND TERMINATION*

#### 9.10.1. Term

#### 9.10.2. Termination

#### 9.10.3. Effect of termination and survival

### *9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS*

### *9.12. AMENDMENTS*

#### 9.12.1. Procedure for amendment

#### 9.12.2. Notification mechanism and period

#### 9.12.3. Circumstances under which OID must be changed

### *9.13. DISPUTE RESOLUTION PROVISIONS*

### *9.14. GOVERNING LAW*

### *9.15. COMPLIANCE WITH APPLICABLE LAW*

### *9.16. MISCELLANEOUS PROVISIONS*

#### 9.16.1. Entire Agreement

#### 9.16.2. Assignment

#### 9.16.3. Severability

In the event of a conflict between these Requirements and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which a CA operates or issues certificates, a CA MAY modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law. In such event, the CA SHALL immediately (and prior to issuing a certificate under the modified requirement) include in Section 9.16.3 of the CA's CPS a detailed reference to the Law requiring a modification of these Requirements under this section, and the specific modification to these Requirements implemented by the CA.

The CA MUST also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to these Requirements accordingly.

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

#### 9.16.4. Enforcement

#### 9.16.5. Force Majeure

### *9.17. OTHER PROVISIONS*