Certificate Policy

Version 1.0.7

1 INTRODUCTION

1.1 Overview

This Certificate Policy is intended to communicate the minimum operating requirements for CAs in the Amazon PKI. By design, it closely follows the CA/Browser Forum Guidelines and Requirements and only deviates when an Application Software Supplier has requirements that are stricter than those published by the CA/Browser Forum.

This CP also includes the principles and criteria that CAs are required to follow according to the Trust Service Principles and Criteria for Certification Authorities Version 2.0.

This CP does not attempt to paraphrase or alter the requirements, rather the focus is to bring all of them into one document to enable Relying Parties and auditors to have a comprehensive view of the policies which the CA commits to follow.

Certificate Authorities following this CP may have practices which exceed the minimum requirements set forth by these policies. CAs may also describe practices that cover topics for which there is no stipulation in this CP.

1.1.1 Compliance

This Certificate Policy conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org (http:// www.cabforum.org). In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

This Certificate Policy conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

This CP conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Code Signing Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

This CP conforms to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates published at http:// www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

1.1.2 Types of Certificates

This Certificate Policy defines several different types of certificates. Each certificate issued under this policy is categorized as either a CA-certificate or an End-Entity Certificate.

All certificates issued under this policy MUST be X.509 v3 certificates.

1.1.2.1 CA-Certificates

A certificate is a CA-certificate if basicConstraints extension is present and has cA:TRUE.

CA-certificates are grouped into two categories: self-issued certificates and cross-certificates.

A self-issued certificate is a CA certificate where the subject and issuer DNs of the certificate match. Under this policy, all self-issued certificates must be self-signed certificates. A self-signed certificate is a self-issued certificate where the private key used by the CA to sign the certificate corresponds to the public key that is certified within the certificate.

A cross-certificate is a CA certificate that is not a self-issued certificate.

1.1.2.1.1 Missing Heading

1.1.2.1.2 Missing Heading

1.1.2.1.3 Terminus CA-Certificates

A certificate is a Terminus CA-certificate if it is a cross-certificate and the basicConstraints extension is present and the pathLenConstraint is present and set to 0 (zero).

1.1.2.1.4 Policy CA-Certificates

A certificate is a Policy CA-certificate if it is a cross-certificate and is not a Terminus CA-certificate.

1.1.2.1.5 Technically Constrained CA-Certificates

A certificate is a Technically Constrained CA-certificate if it is a CA-certificate and it meets the requirements in section 7.1.5.

1.1.2.1.6 Unconstrained CA-Certificates

A certificate is an Unconstrained CA-certificate if it is a CA-certificate and is not a Technically Constrained CA-certificate.

1.1.2.1.7 Root CA-Certificates

A certificate is a Root CA-certificate if the subject is designated by the CA as a Root CA in the CA's CPS and it is either a self-issued certificate or Policy CA-certificate.

1.1.2.1.8 Subordinate CA-Certificates

A certificate is a Subordinate CA-certificate if it is a cross-certificate and the subject DN of the certificate does not match the issuer name of any Root CA in the CA's CPS.

1.1.2.2 End-Entity Certificates

A certificate is an End-Entity Certificate if it is not a CA certificate.

End-Entity Certificates can be further broken down into the following categories. CAs must not issue End- Entity Certificates that simultaneously meet the criteria of multiple of the following categories.

1.1.2.2.1 Extended Validation TLS Server Authentication Certificates

An End-Entity Certificate is an Extended Validation TLS Server Authentication Certificate if it (i) has a Relative Distinguished Name of type jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3) in the Subject Distinguished Name and (ii) has a key purpose of id-kp-serverAuth (1.3.6.1.5.5.7.3.1) in the Extended Key Usage certificate extension.

1.1.2.2.2 Standard Validation TLS Server Authentication Certificates

An End-Entity Certificate is a Standard Validation TLS Server Authentication Certificate if it (i) does not have a Relative Distinguished Name of type jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3) in the Subject Distinguished Name and (ii) has a key purpose of id-kp-serverAuth (1.3.6.1.5.5.7.3.1) in the Extended Key Usage certificate extension.

1.1.2.2.3 Extended Validation Code Signing Certificates

An End-Entity Certificate is an Extended Validation Code Signing Certificate if it (i) has a Relative Distinguished Name of type jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3) in the Subject Distinguished Name and (ii) has a key purpose of id-kp-codeSigning (1.3.6.1.5.5.7.3.3) in the Extended Key Usage certificate extension.

1.1.2.2.4 Standard Validation Code Signing Certificates

An End-Entity Certificate is a Standard Validation Code Signing Certificate if it (i) does not have a Relative Distinguished Name of type jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3) in the Subject Distinguished Name and (ii) has a key purpose of id-kp-codeSigning (1.3.6.1.5.5.7.3.3) in the Extended Key Usage certificate extension.

1.1.2.2.5 Client Certificates (including Augmented Client Certificates)

An End-Entity Certificate is a Client Certificate if it has at least one of id-kp-clientAuth (1.3.6.1.5.5.7.3.2), id- kp-emailProtection (1.3.6.1.5.5.7.3.4), Document Signing (1.3.6.1.4.1.311.10.3.12), or Encrypting Filesystem Crypto (1.3.6.1.4.1.311.10.3.4) key purposes in the Extended Key Usage certificate extension and does not have the id-kp-serverAuth (1.3.6.1.5.5.7.3.1) key purpose in the Extended Key Usage certificate extension.

Under this policy, an Augmented Client Certificate is identical to a Client Certificate.

1.1.2.2.6 OCSP Signing Certificate

An End-Entity Certificate is an OCSP Signing Certificate if it has a key purpose of id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9) in the Extended Key Usage certificate extension.

1.1.2.2.7 Time Stamp Authority Certificate

An End-Entity Certificate is a Time Stamping Authority Certificate if it has a key purpose of id-kp- timeStamping (1.3.6.1.5.5.7.3.8) in the Extended Key Usage certificate extension.

1.1.2.3 Subscriber Certificates

All Extended Validation TLS Server Authentication Certificates, Standard Validation TLS Server Authentication Certificates, and Extended Validation Code Signing Certificates are Subscriber Certificates.

1.2 Document name and identification

This is the Amazon Public Key Infrastructure (PKI) Certificate Policy. It was approved for publication by the Amazon PKI Policy Management Authority (APPMA). Amendments are made only after the APPMA has reviewed and approved such amendment. This document is identified by the Object Identifier 1.3.187.16385.1.

This CP is updated at least annually to ensure that it incorporates the latest version of the CA/Browser Forum Baseline Requirements.

Date	Changes	Version
2017-01-12	Yearly update	1.0.4
2018-01-15	Yearly update	1.0.5
2018-04-13	Updated 3.2.2.4 Validation of Domain Authorization or Control, BR 1.5.6	1.0.6
2019-18-12	Updated to add Code Signing Baseline Requirements	1.0.7
2020-30-03	Updated with latest Baseline Requirements	1.0.8

1.3 PKI participants

1.3.1 Certification authorities

The Certification Authority (CA) provides services in accordance with its disclosed practices.

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.

The CA MAY contractually authorize the Subject of a specified Valid EV Certificate to perform the RA function and authorize the CA to issue Enterprise EV Certificates. In such case, the Subject SHALL be considered an Enterprise RA, and the following requirements SHALL apply:

1. An Enterprise RA SHALL NOT authorize the CA to issue an Enterprise EV Certificate at the third or higher domain levels to any Subject other than the Enterprise RA or a business that is owned or directly controlled by the Enterprise RA;
2. In all cases, the Subject of an Enterprise EV Certificate MUST be an organization verified by the CA in accordance with this Certificate Policy;
3. The CA MUST impose these limitations as a contractual requirement with the Enterprise RA and monitor compliance by the Enterprise RA;
4. The Final Cross-Correlation and Due Diligence requirements of EV Guidelines Section 11.13 MAY be performed by a single person representing the Enterprise RA; and
5. The audit requirements of EV Guidelines Section 17.1 SHALL apply to the Enterprise RA, except in the case where the CA maintains control over the Root CA Private Key or Subordinate CA Private Key used to issue the Enterprise EV Certificates, in which case, the Enterprise RA MAY be exempted from the audit requirements.

The CA MAY NOT contractually authorize the Subject of a specified Valid EV Code Signing Certificate to perform the RA function and authorize the CA to issue additional EV Code Signing Certificates.

1.3.3 Subscribers

No stipulation.

1.3.4 Relying parties

No stipulation.

1.3.5 Other participants

The CA MUST include (directly or by reference) the applicable requirements of the EV Guidelines in all contracts with Subordinate CAs, RAs, Enterprise RAs, and subcontractors that involve or relate to the issuance or maintenance of EV Certificates. The CA MUST enforce compliance with such terms.

In all cases, the CA MUST contractually obligate each Affiliate, RA, subcontractor, and Enterprise RA to comply with all applicable requirements in this CP and to perform them as required of the CA itself. The CA SHALL enforce these obligations and internally audit each Affiliate's, RA's, subcontractor's, and Enterprise RA's compliance with these Requirements on an annual basis.

The CA MUST include (directly or by reference) the applicable requirements of this Certificate Policy in all contracts that involve or relate to the issuance or maintenance of EV Code Signing Certificates. The Issuer MUST enforce compliance with such terms.

In all cases, the CA MUST contractually obligate each RA and subcontractor to comply with all applicable requirements in this Certificate Policy and to perform them as required of the CA itself. The CA SHALL enforce these obligations and internally audit each Affiliate's, RA's, and subcontractor's compliance with these Requirements on an annual basis.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

No stipulation.

1.4.2 Prohibited certificate uses

No stipulation.

1.5 Policy administration

The CA must disclose its business practices including but not limited to the topics listed in RFC 3647, RFC 2527, or WebTrust for Certification Authorities v1 CA Business Practices Disclosure Criteria in its Certification Practice Statement.

The CA must maintain controls to provide reasonable assurance that its Certification Practice Statement management processes are effective.

Each CA MUST develop, implement, enforce, display prominently on its Web site, and periodically update as necessary its own auditable EV Certificate practices, policies and procedures that:

1. Implements this policy;
2. Implements the requirements of (i) the then-current WebTrust Program for CAs, and (ii) the then- current WebTrust EV Program or ETSI TS 102 042; and
3. Specifies the CA's and its Root CA's entire root certificate hierarchy including all roots that its EV Certificates depend on for proof of those EV Certificates' authenticity.

Each Issuer MUST develop, implement, enforce, display prominently on its Web site, and periodically update as necessary its own auditable EV Code Signing Object practices, policies and procedures, such as a Certification Practice Statement and Certificate Policy that:

A. Implement the requirements of this Certificate Policy as they are revised from time-to-time;
B. Implement the requirements of (i) the then-current WebTrust Program for CAs, and (ii) the then- current WebTrust EV Program or ETSI TS 102 042 V2.1.1; and
C. Specify the Issuer's (and applicable Root CA's) entire root certificate hierarchy including all roots that its EV Code Signing Certificates depend on for proof of those EV Code Signing Certificates' authenticity.

With the exception of revocation checking for time-stamped and expired certificates, platforms are expected to validate signed code in accordance with RFC 5280. When a platform encounters a certificate that fails to validate due to revocation, the platform should reject the code. When a platform encounters a certificate that fails to validate for reasons other than revocation, the platform should treat the code as it would if it had been unsigned.

Ordinarily, a code signature created by a Subscriber may be considered valid for a period of up to thirty-nine months. However, a code signature may be treated as valid for a period of up to one hundred and twenty three months by means of one of the following methods: the "Timestamp" Method or the "Signing Authority" Method.

A. **Timestamp Method**: In this method, the Subscriber signs the code, appends its EV Code Signing Certificate (whose expiration time is less than thirty-nine months in the future) and submits it to an EV Timestamp Authority to be time-stamped. The resulting package can be considered valid up to the expiration time of the timestamp certificate (which may be up to one hundred and twenty three months in the future).
B. **Signing Authority Method**: In this method, the Subscriber submits the code, or a digest of the code, to an EV Signing Authority for signature. The resulting signature is valid up to the expiration time of the Signing Authority certificate (which may be up to one hundred and twenty three months in the future).

1.5.1 Organization administering the document

No stipulation.

1.5.2 Contact person

No stipulation.

1.5.3 Person determining CPS suitability for the policy

The CA must maintain controls to provide reasonable assurance that its Certification Practice Statement addresses the topics included in its Certificate Policy.

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 Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in section 8.1.

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these 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 Ports: One of the following ports: 80 (http), 443 (https), 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, and whose activities are not within the scope of the appropriate CA audits, to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

DNS CAA Email Contact: The email address defined in section B.1.1.

DNS CAA Phone Contact: The phone number defined in section B.1.2.

DNS TXT Record Email Contact: The email address defined in section B.2.1.

DNS TXT Record Phone Contact: The phone number defined in section B.2.2.

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 contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

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

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 assignees).

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.

IP Address: A 32-bit or 128-bit label assigned to a device that uses the Internet Protocol for communication.

IP Address Contact: The person(s) or entity(ies) registered with an IP Address Registration Authority as having the right to control how one or more IP Addresses are used.

IP Address Registration Authority: The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

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, or an unauthorized person has had access to it.

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 8.2.

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 CA SHOULD define within its CPS (or a document clearly referenced by the CPS) the format and method of Request Tokens it accepts.

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.

Note: Examples of Request Tokens include, but are not limited to: (i) a hash of the public key; or (ii) a hash of the Subject Public Key Info [X.509]; or (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.

Note: This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR. echo `date -u +%Y%m%d%H%M` `sha256sum <r2.csr` \| sed "s/[-]//g" The script outputs: 201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f

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: This term is no longer used in these Baseline 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.

WHOIS: Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

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

Wildcard Domain Name: A Domain Name consisting of a single asterisk character followed by a single full stop character ("*.") followed by a Fully-Qualified Domain Name.

1.6.2 Acronyms

Acronym	Meaning

AICPA	American Institute of Certified Public Accountants
ADN	Authorization Domain Name
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
TLS	Transport Layer Security
VoIP	Voice Over Internet Protocol

1.6.3 References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.6.4 Conventions

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 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 certification information

The Parent CA maintains controls to provide reasonable assurance that timely, complete and accurate certificate status information (including CRLs and other certificate status mechanisms) is made available to any entity in accordance with the CA’s disclosed business practices.

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 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.

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

Each CA MUST publicly disclose their EV Policies through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA is also REQUIRED to publicly disclose its CA business practices as required by both WebTrust for CAs and ETSI TS 102 042. The disclosures MUST be structured in accordance with either RFC 2527 or RFC 3647.

2.3 Time or frequency of publication

No stipulation.

2.4 Access controls on repositories

No stipulation.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

No stipulation.

3.1.2 Need for names to be meaningful

No stipulation.

3.1.3 Anonymity or pseudonymity of subscribers

No stipulation.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

No stipulation.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

An Issuer CA may use any legal means of communication or investigation to ascertain the identity of an organizational or individual Applicant. The Issuer CA may refuse to issue a Certificate in its sole discretion.

The Issuer of EV Certificates is responsible for taking all verification steps reasonably necessary to satisfy each of the Verification Requirements set forth in the EV Guidelines. In all cases, however, the Issuer is responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement.

The Issuer of EV Code Signing Certificates is responsible for taking all verification steps reasonably necessary to satisfy each of the Verification Requirements set forth in the EV Code Signing Guidelines. In all cases, however, the Issuer is responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement.

3.2.1 Method to prove possession of private key

No stipulation.

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.

If the Applicant requests an Extended Validation Certificate, then the CA shall follow the EV Guidelines.

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 Applicant's Jurisdiction of Incorporation or Jurisdiction of Registration;
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

The CA SHALL confirm that prior to issuance, the CA has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below.

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 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.

CAs SHALL maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.

3.2.2.4.1 Validating the Applicant as a Domain Contact

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

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 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 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.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.3 Phone Contact with Domain Contact

Confirming the Applicant's control over the 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 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.

CAs SHALL NOT perform validations using this method after May 31, 2019. Completed validations using this method SHALL continue to be valid for subsequent issuance per the applicable certificate data reuse periods.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.4 Constructed Email to Domain Contact

Confirm the Applicant's control over the FQDN by

1. 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; and
2. including a Random Value in the email; and
3. 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.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.5 Domain Authorization Document

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.2.4.6 Agreed-Upon Change to Website

Confirming the Applicant's control over the 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. The entire Required Website Content MUST NOT appear in the request used to retrieve the file or web page
2. The presence of the Request Token or Random Value contained in the content of a file where the Request Token or Random Value MUST NOT appear in the request.

If a Random Value is used, the CA 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 4.2.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.7 DNS Change

Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

If a Random Value is used, the CA 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.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.8 IP Address

Confirming the Applicant's control over the 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.

Note: Once the FQDN has been validated using this method, the CA MAY NOT also issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the CA performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.9 Test Certificate

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.2.4.10 TLS Using a Random Number

Confirming the Applicant's control over the 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.

3.2.2.4.11 Any Other Method

This method has been retired and MUST NOT be used.

3.2.2.4.12 Validating Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact. This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.13 Email to DNS CAA Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065 (Appendix A).

Each email MAY confirm control of multiple FQDNs, provided that each email address is a DNS CAA Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS CAA Email Contacts for each Authorization Domain Name being validated.

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(s) 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.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.14 Email to DNS TXT Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN.

Each email MAY confirm control of multiple FQDNs, provided that each email address is DNS TXT Record Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS TXT Record Email Contacts for each Authorization Domain Name being validated.

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(s) 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.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.15 Phone Contact with Domain Contact

Confirm the Applicant's control over the FQDN by calling the Domain Contact’s phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

In the event that someone other than a Domain Contact is reached, the CA MAY request to be transferred to the Domain Contact.

In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to the CA to approve the request.

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.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

Confirm the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact’s phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same DNS TXT Record Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

The CA MAY NOT knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation.

In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to the CA to approve the request.

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.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

Confirm the Applicant's control over the FQDN by calling the DNS CAA Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065 (Appendix A).

The CA MUST NOT be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation.

In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to the CA to approve the request.

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.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.5 Authentication for an IP Address

The CA SHALL confirm that prior to issuance, the CA has validated each IP Address listed in the Certificate using at least one of the methods specified in this section.

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 of this document) prior to Certificate issuance. For purposes of IP Address validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

After July 31, 2019, CAs SHALL maintain a record of which IP validation method, including the relevant BR version number, was used to validate every IP Address.

Note: IP Addresses verified in accordance with this section 3.2.5 may be listed in Subscriber Certificates as defined in section 7.1.4.2 or in Subordinate CA Certificates via iPAddress in permittedSubtrees within the Name Constraints extension. CAs are not required to verify IP Addresses listed in Subordinate CA Certificates via iPAddress in excludedSubtrees in the Name Constraints extension prior to inclusion in the Subordinate CA Certificate.

3.2.2.5.1 Agreed-Upon Change to Website

Confirming the Applicant's control over the requested IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of validating control of IP Addresses, on the IP Address that is accessible by the CA via HTTP/HTTPS over an Authorized Port. The Request Token or Random Value MUST NOT appear in the request.

If a Random Value is used, the CA 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 4.2.1 of this document).

3.2.2.5.2 Email, Fax, SMS, or Postal Mail to IP Address Contact

Confirming the Applicant's control over the IP Address 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 an IP Address Contact.

Each email, fax, SMS, or postal mail MAY confirm control of multiple IP Addresses.

The CA 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 IP Address Registration Authority as representing the IP Address Contact for every IP Address 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 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.

3.2.2.5.3 Reverse Address Lookup

Confirming the Applicant's control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under BR Section 3.2.2.4.

3.2.2.5.4 Any Other Method

Using any other method of confirmation, including variations of the methods defined in BR Section 3.2.2.5, 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 in version 1.6.2 of these Requirements.

CAs SHALL NOT perform validations using this method after July 31, 2019. Completed validations using this method SHALL NOT be re-used for certificate issuance after July 31, 2019. Any certificate issued prior to August 1, 2019 containing an IP Address that was validated using any method that was permitted under the prior version of this section 3.2.2.5 MAY continue to be used without revalidation until such certificate naturally expires.

3.2.2.5.5 Phone Contact with IP Address Contact

Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number and obtaining a response confirming the Applicant's request for validation of the IP Address. The CA MUST place the call to a phone number identified by the IP Address Registration Authority as the IP Address Contact. Each phone call SHALL be made to a single number.

In the event that someone other than an IP Address Contact is reached, the CA MAY request to be transferred to the IP Address Contact.

In the event of reaching voicemail, the CA may leave the Random Value and the IP Address(es) being validated. The Random Value MUST be returned to the CA to approve the request.

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.

3.2.2.5.6 ACME "http-01" method for IP Addresses

Confirming the Applicant's control over the IP Address by performing the procedure documented for an "http-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4.

3.2.2.5.7 ACME “tls-alpn-01” method for IP Addresses

Confirming the Applicant's control over the IP Address by performing the procedure documented for a “tls-alpn-01” challenge in draft 04 of “ACME IP Identifier Validation Extension,” available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4.

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[1] 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[1] 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.).

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 Section 3.2.

3.2.2.8 CAA Records

As part of the issuance process, the CA MUST check for CAA records and follow the processing instructions found, for each dNSName in the subjectAltName extension of the certificate to be issued, as specififed in RFC 6844 as amended by Errata 5065 (Appendix A). If the CA issues, they MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater.

This stipulation does not prevent the CA from checking CAA records at any other time.

When processing CAA records, CAs MUST process the issue, issuewild, and iodef property tags as specified in RFC 6844, although they are not required to act on the contents of the iodef property tag. Additional property tags MAY be supported, but MUST NOT conflict with or supersede the mandatory property tags set out in this document. CAs MUST respect the critical flag and not issue a certificate if they encounter an unrecognized property tag with this flag set. CAs MAY treat a non-empty CAA Resource Record Set that does not contain any issue property tags (and also does not contain any issuewild property tags when performing CAA processing for a Wildcard Domain Name) as permission to issue, provided that no records in the CAA Resource Record Set otherwise prohibit issuance.

RFC 6844 requires that CAs "MUST NOT issue a certificate unless either (1) the certificate request is consistent with the applicable CAA Resource Record set or (2) an exception specified in the relevant Certificate Policy or Certification Practices Statement applies." For issuances conforming to these Baseline Requirements, CAs MUST NOT rely on any exceptions specified in their CP or CPS unless they are one of the following:

- CAA checking is optional for certificates for which a Certificate Transparency pre-certificate was created and logged in at least two public logs, and for which CAA was checked.
- CAA checking is optional for certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Baseline Requirements section 7.1.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.
- CAA checking is optional if the CA or an Affiliate of the CA is the DNS Operator (as defined in RFC 7719) of the domain's DNS.

CAs are permitted to treat a record lookup failure as permission to issue if:

- the failure is outside the CA's infrastructure; and
- the lookup has been retried at least once; and
- the domain's zone does not have a DNSSEC validation chain to the ICANN root.

CAs MUST document potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CAB Forum on the circumstances, and SHOULD dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s), if present. CAs are not expected to support URL schemes in the iodef record other than mailto: or https:.

3.2.3 Authentication of individual identity

If an Applicant subject to this Section is an Individual, 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. If the Applicant requests an Extended Validation Certificate, then the CA shall follow the EV Guidelines.

3.2.4 Non-verified subscriber information

No stipulation.

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

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

No stipulation.

3.3.2 Identification and authentication for re-key after revocation

No stipulation.

3.4 Identification and authentication for revocation request

No stipulation.

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 4.2.1, provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. 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, or may reuse previous validations themselves, provided that the CA obtained the data or document from a source specified under Section 3.2 or completed the validation itself no more than 825 days prior to issuing the Certificate.

In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.

After the change to any validation method specified in the Baseline Requirements or EV Guidelines, a CA may continue to reuse validation data or documents collected prior to the change, or the validation itself, for the period stated in this BR 4.2.1 unless otherwise specifically provided in a ballot.

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 SHALL NOT issue certificates containing Internal Names (see section 7.1.4.2.1).

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 to subscriber by the CA of issuance of certificate

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;
4. The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

The CA SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
2. The CA obtains evidence that the Certificate was misused;
3. 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;
4. 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);
5. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;

6. The CA is made aware of a material change in the information contained in the Certificate;
7. 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;
8. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate;
9. 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;
10. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or

The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, 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.

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

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 Certificate Problem Reports.

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 and in section 1.5.2 of their CPS.

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within which CA must process the revocation request

Within 24 hours after receiving a Certificate Problem Report, the CA SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report. After reviewing the facts and circumstances, the CA SHALL work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the CA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation MUST NOT exceed the time frame set forth in Section 4.9.1.1. The date selected by the CA SHOULD consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. 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 they didn't receive the goods they ordered); and
1. 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 (if applicable)

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 (if applicable)

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

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

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 (i) at least every twelve months; and (ii) within 24 hours after revoking a Subordinate CA Certificate.

If the OCSP responder receives a request for the status of a certificate serial number that is "unused", then the responder SHOULD NOT respond with a "good" status. If the OCSP responder is for a CA that is not Technically Constrained in line with Section 7.1.5, the responder MUST NOT respond with a "good" status for such requests.

The CA SHOULD monitor the OCSP responder for requests for "unused" serial numbers as part of its security response procedures.

The OCSP responder MAY provide definitive responses about "reserved" certificate serial numbers, as if there was a corresponding Certificate that matches the Precertificate [RFC6962].

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

1. "assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject; or
2. "reserved" if a Precertificate [RFC6962] with that serial number has been issued by (a) the Issuing CA; or (b) a Precertificate Signing Certificate [RFC6962] associated with the Issuing CA; or
3. "unused" if neither of the previous conditions are met.

4.9.11 Other forms of revocation advertisements available

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 re 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

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL 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 controls

The CA maintains controls to provide reasonable assurance that CA facilities and equipment are protected from environmental hazards.

5.1.1 Site location and construction

No stipulation.

5.1.2 Physical access

No stipulation.

5.1.3 Power and air conditioning

No stipulation.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

No stipulation.

5.1.7 Waste disposal

No stipulation.

5.1.8 Off-site backup

No stipulation.

5.2 Procedural controls

5.2.1 Trusted roles

Each CA or Delegated Third Party SHALL document the responsibilities and tasks assigned to Trusted Roles and implement “separation of duties” for such Trusted Roles based on the security-related concerns of the functions to be performed

Each CA or Delegated Third Party SHALL follow a documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them

Each CA or Delegated Third Party SHALL grant administration access to Certificate Systems only to persons acting in Trusted Roles and require their accountability for the Certificate System’s security

5.2.2 Number of persons required per task

The Private Key SHALL be backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

5.2.3 Identification and authentication for each role

Each CA or Delegated Third Party SHALL require that each individual in a Trusted Role use a unique credential created by or assigned to that person in order to authenticate to Certificate Systems.

5.2.4 Roles requiring separation of duties

Each CA or Delegated Third Party SHALL document the responsibilities and tasks assigned to Trusted Roles and implement “separation of duties” for such Trusted Roles based on the security-related concerns of the functions to be performed.

5.3 Personnel controls

The CA must maintain controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA’s operations.

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

No stipulation.

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

No stipulation.

5.3.6 Sanctions for unauthorized actions

The CA must maintain controls to provide reasonable assurance that compliance with the CA's security policies and procedures is ensured.

Each CA or Delegated Third Party SHALL ensure that an individual in a Trusted Role acts only within the scope of such role when performing administrative tasks assigned to that role.

5.3.7 Independent contractor requirements

The CA SHALL verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3.3 and the document retention and event logging requirements of Section 5.4.1.

5.3.8 Documentation supplied to personnel

No stipulation.

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; Frequency of Processing Log
    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
1. Description of the entry.

5.4.2 Frequency of processing log and archiving audit logs
No stipulation.

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
No stipulation.

5.4.5 Audit log backup procedures
No stipulation.

5.4.6 Audit log accumulation system (internal vs. external)
No stipulation.

5.4.7 Notification to event-causing subject
No stipulation.

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.

5.5 Records archival
5.5.1 Types of records archived
No stipulation.

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
No stipulation.

5.5.4 Archive backup procedures
No stipulation.

5.5.5 Requirements for time-stamping of records
No stipulation.

5.5.6 Archive collection system (internal or external)
No stipulation.

5.5.7 Procedures to obtain and verify archive information
No stipulation.

5.6 Key changeover
No stipulation.

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;
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 Computing resources, software, and/or data are corrupted
No stipulation.

5.7.3 Entity private key compromise procedures
No stipulation.

5.7.4 Business continuity capabilities after a disaster
No stipulation.

5.8 CA or RA termination
No stipulation.

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

For other CA Key Pairs 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 CA Key Pair generation process or record a video of the entire 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 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 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 Certification Practice Statement and (if applicable) its Key Generation Script.

6.1.1.2 RA Key Pair Generation

No stipulation.

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

No stipulation.

6.1.4 CA public key delivery to relying parties

No stipulation.

6.1.5 Key sizes

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

6.1.5.1 Root CA Certificates

- Digest algorithm: SHA-256, SHA-384 or SHA-512
- Minimum RSA modulus size (bits): 2048
- ECC curve: NIST P-256, P-384, or P-521
- Minimum DSA modulus and divisor size (bits)*: L= 2048 N= 224 or L= 2048 N= 256

* L and N (the bit lengths of modulus p and divisor q, respectively) are described in FIPS 186-4.

6.1.5.2 Subordinate CA Certificates

- Digest algorithm: SHA-256, SHA-384 or SHA-512
- Minimum RSA modulus size (bits): 2048
- ECC curve: NIST P-256, P-384, or P-521
- Minimum DSA modulus and divisor size (bits)*: L= 2048 N= 224 or L= 2048 N= 256

* L and N (the bit lengths of modulus p and divisor q, respectively) are described in FIPS 186-4.

6.1.5.3 Subscriber Certificates

- Digest algorithm: SHA-256, SHA-384 or SHA-512|
- Minimum RSA modulus size (bits): 2048
- ECC curve: NIST P-256, P-384, or P-521
- Minimum DSA modulus and divisor size (bits)*: L= 2048 N= 224 or L= 2048 N= 256

* L and N (the bit lengths of modulus p and divisor q, respectively) are described in FIPS 186-4.

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 5.6.2.3.36, respectively, NIST SP 800-56A]

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Private Keys corresponding to Root Certificates 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 (administrative role certificates, internal CA operational device certificates); and
4. Certificates for OCSP Response verification.

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 Private Key outside the validated system or device specified above MUST consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Key. The CA SHALL encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic module standards and controls

No stipulation.

6.2.2 Private key (n out of m) multi-person control

No stipulation.

6.2.3 Private key escrow

No stipulation.

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 Method of activating private key

No stipulation.

6.2.9 Method of deactivating private key

No stipulation.

6.2.10 Method of destroying private key

No stipulation.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other aspects of key pair management

6.3.1 Public key archival

No stipulation.

6.3.2 Certificate operational periods and key pair usage periods

Subscriber Certificates issued after 1 March 2018 MUST have a Validity Period no greater than 825 days. Subscriber Certificates issued after 1 July 2016 but prior to 1 March 2018 MUST have a Validity Period no greater than 39 months.

6.4 Activation data

6.4.1 Activation data generation and installation

No stipulation.

6.4.2 Activation data protection

No stipulation.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

The CA must maintain controls to provide reasonable assurance that compromise of information and information processing facilities is prevented.

The CA must maintain controls to provide reasonable assurance that CA system access is limited to authorized individuals.

The CA must maintain controls to provide reasonable assurance that the risk of CA systems failure is minimized.

The CA maintains controls to provide reasonable assurance that operating system and database access is limited to authorized individuals with predetermined task privileges.

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

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

No stipulation.

6.8 Time-stamping

No stipulation.

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.

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 extensions

This section specifies the additional requirements for Certificate content and extensions for Certificates.

7.1.2.1 Root CA Certificate

- basicConstraints This extension MUST appear as a critical extension. The cA field MUST be set true. The pathLenConstraint field SHOULD NOT be present.
- 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.
- certificatePolicies This extension SHOULD NOT be present.
- extendedKeyUsage This extension MUST NOT be present.

7.1.2.2 Subordinate CA Certificate

- 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 Policy, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the CA.

- cRLDistributionPoints This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's CRL service.
- 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].

- basicConstraints This extension MUST be present and MUST be marked critical. The cA field MUST be set true. The pathLenConstraint field MAY be present.
- 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.

- 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.

- 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.

7.1.2.3 Subscriber Certificate

- 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.

- 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.
- 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].

- basicConstraints (optional) If present, the cA field MUST NOT be true.
- keyUsage (optional) If present, bit positions for keyCertSign and cRLSign MUST NOT be set.

A. 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:
    a. such value falls within an OID arc for which the Applicant demonstrates ownership, or
    b. 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 Requirements.

7.1.3 Algorithm object identifiers

CAs MUST NOT issue any Subscriber certificates or Subordinate CA certificates using the SHA-1 hash algorithm. CAs MAY issue Root CA Certificates or Subordinate CA Certificates that are Cross Certificates using the SHA-1 hash algorithm.

CAs MAY continue to use their existing SHA-1 Root Certificates.

Subscriber certificates SHOULD NOT chain up to a SHA-1 Subordinate CA Certificate.

7.1.4 Name forms

7.1.4.1 Issuing CA Certificate Subject

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 for Standard Server Authentication certificates

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 Section 3.2.2.4 or Section 3.2.2.5.

Subject attributes MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.4.2.1 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.

CAs SHALL NOT issue certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name.

Entries in the dNSName MUST be in the "preferred name syntax", as specified in RFC 5280, and thus MUST NOT contain underscore characters ("_").

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: subject:givenName (2.5.4.42) and subject:surname (2.5.4.4) Optional. Contents: If present, the subject:givenName field and subject:surname field MUST contain an natural person Subject's name as verified under Section 3.2.3. A Certificate containing a subject:givenName field or subject:surname field MUST contain the (2.23.140.1.2.3) Certificate Policy OID.

d. Certificate Field: Number and street: subject:streetAddress (OID: 2.5.4.9) Optional if the subject:organizationName field, subject: givenName field, or subject:surname field are present. Prohibited if the subject:organizationName field, subject:givenName, and subject:surname field are absent. Contents: If present, the subject:streetAddress field MUST contain the Subject's street address information as verified under Section 3.2.2.1.

e. Certificate Field: subject:localityName (OID: 2.5.4.7) Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and the subject:stateOrProvinceName field is absent. Optional if the subject:stateOrProvinceName field and the subject:organizationName field, subject:givenName field, or subject:surname field are present. Prohibited if the subject:organizationName field, subject:givenName, and subject:surname field are 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.

f. Certificate Field: subject:stateOrProvinceName (OID: 2.5.4.8) Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and subject:localityName field is absent. Optional if the subject:localityName field and the subject:organizationName field, the subject:givenName field, or the subject:surname field are present. Prohibited if the subject:organizationName field, the subject:givenName field, or subject:surname field are 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.

g. Certificate Field: subject:postalCode (OID: 2.5.4.17) Optional if the subject:organizationName, subject:givenName field, or subject:surname fields are present. Prohibited if the subject:organizationName field,

subject:givenName field, or subject:surname field are 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.

h. Certificate Field: subject:countryName (OID: 2.5.4.6) Required if the subject:organizationName field, subject:givenName, or subject:surname field are present. Optional if the subject:organizationName field, subject:givenName field, and subject:surname field are 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.

i. Certificate Field: subject:organizationalUnitName (OID: 2.5.4.11) 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:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 3.2.2.1.

j. Other Subject Attributes Other attributes MAY be present within the subject field. If present, other attributes MUST contain information that has been verified by the CA.

7.1.4.3 Subject Information - Root Certificates and 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.

7.1.4.3.1 Subject Distinguished Name Fields

a. Certificate Field: subject:commonName (OID 2.5.4.3) Required/Optional: Required Contents: This field MUST be present and the contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.

b. Certificate Field: subject:organizationName (OID 2.5.4.10) Required/Optional: Required Contents: 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".

c. Certificate Field: subject:countryName (OID: 2.5.4.6) Required/Optional: Required Contents: This field MUST contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.

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 7.1.4.2.5.

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

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) subject-identity-validated(2)} (2.23.140.1.2.2), if the Certificate complies with these Requirements and includes Subject Identity Information that is verified in accordance with Section 3.2.2.1.

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 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 documented 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 to a Subordinate CA that is an affiliate of the Issuing CA:

1. MAY include the CA/Browser Forum reserved identifiers or an identifier documented 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.

1. 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 a certificatePolicies extension.

The extension MUST contain one or more policy identifiers that indicate adherence to and compliance with these Requirements. CAs MUST either use a CA/Browser Forum identifier reserved for this purpose or MUST use a policy identifier documented by the CA in its Certificate Policy and/or Certification Practice Statement to indicate the Certificate's compliance with these Requirements.

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

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

7.2.1 Version number(s)

No stipulation.

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP profile

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

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.

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 ETSI TS 119 403, or accredited to conduct such audits under an equivalent national scheme, or accredited by a national accreditation body in line with ISO 27006 to carry out ISO 27001 audits; 5. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust; 6. Bound by law, government regulation, or professional code of ethics; and 7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors &

Omissions insurance with policy limits of at least one million US dollars in coverage

8.3 Assessor's relationship to assessed entity

No stipulation.

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;

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

No stipulation.

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.

CAs SHOULD make its audit report publicly available no later than three months after the end of the audit period. If there is a delay greater than three months and if so requested by an Application Software Supplier, the CA MUST provide an explanatory letter signed by its auditor.

Issuers SHOULD make its audit report publicly available no later than three months after the end of the audit period. If there is a delay greater than three months and if so requested by an Application Software Supplier, the Issuer MUST provide an explanatory letter signed by its 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

No stipulation.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

No stipulation.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

9.2.1 Insurance coverage

Each CA SHALL maintain the following insurance related to their respective performance and obligations under this Certificate Policy:

- Commercial General Liability insurance (occurrence form) with policy limits of at least two million US dollars in coverage; and

- Professional Liability/Errors and Omissions insurance, with policy limits of at least five million US dollars in coverage, and including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

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

A CA MAY self-insure for liabilities that arise from such party's performance and obligations under this Certificate Policy provided that it has at least five hundred million US dollars in liquid assets based on audited financial statements in the past twelve months, and a quick ratio (ratio of liquid assets to current liabilities) of not less than 1.0.

9.2.2 Other assets
No stipulation.

9.2.3 Insurance or warranty coverage for end-entities
No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information
No stipulation.

9.3.2 Information not within the scope of confidential information
No stipulation.

9.3.3 Responsibility to protect confidential information
No stipulation.

9.4 Privacy of personal information

9.4.1 Privacy plan
No stipulation.

9.4.2 Information treated as private
No stipulation.

9.4.3 Information not deemed private
No stipulation.

9.4.4 Responsibility to protect private information
No stipulation.

9.4.5 Notice and consent to use private information
No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process
No stipulation.

9.4.7 Other information disclosure circumstances
No stipulation.

9.5 Intellectual property rights
No stipulation.

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 or Terms of Use Agreement for the Certificate;
2. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
3. All Relying Parties who reasonably rely on a Valid Certificate. 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 Affiliated, the Applicant Representative acknowledged and accepted the Terms of Use; 7. Status: That the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and 8. Revocation: That the CA will revoke the Certificate for any of the reasons specified in these Requirements.

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

No stipulation.

9.6.3 Subscriber representations and warranties

The CA SHALL require, as part of the Subscriber or Terms of Use Agreement, 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 agreement to the Terms of Use agreement.

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

The Subscriber or Terms of Use Agreement MUST contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties: 1. Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA; 2. Protection of Private Key: An obligation and warranty by the Applicant to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token); 3. Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy; 4. Use of Certificate: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber or Terms of Use Agreement; 5. Reporting and Revocation: An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request the CA to revoke the Certificate, in the event that: (a) any information in the Certificate is, or becomes, incorrect or inaccurate, or (b)there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate; 6. Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise. 7. Responsiveness: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period. 8. Acknowledgment and Acceptance: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Agreement or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

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

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).

9.10 Term and termination

9.10.1 Term

No stipulation.

9.10.2 Termination

No stipulation.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for amendment

No stipulation.

9.12.2 Notification mechanism and period
No stipulation.

9.12.3 Circumstances under which OID must be changed
No stipulation.

9.13 Dispute resolution provisions
No stipulation.

9.14 Governing law
No stipulation.

9.15 Compliance with applicable law
No stipulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement
No stipulation.

9.16.2 Assignment
No stipulation.

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 (attorneys' fees and waiver of rights)
No stipulation.

9.16.5 Force Majeure
No stipulation.

9.17 Other provisions

1. 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/ (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.

No stipulation.

APPENDIX A – RFC 6844 Errata 5065

The following errata report has been held for document update for RFC6844, "DNS Certification Authority Authorization (CAA) Resource Record".

You may review the report below and at: http://www.rfc-editor.org/errata/eid5065

Status: Held for Document Update Type: Technical

Reported by: Phillip Hallam-Baker philliph@comodo.com Date Reported: 2017-07-10 Held by: EKR (IESG)

Section: 4

Original Text

Let CAA(X) be the record set returned in response to performing a CAA record query on the label X, P(X) be the DNS label immediately above X in the DNS hierarchy, and A(X) be the target of a CNAME or DNAME alias record specified at the label X.

o If CAA(X) is not empty, R(X) = CAA (X), otherwise

o If A(X) is not null, and R(A(X)) is not empty, then R(X) = R(A(X)), otherwise

o If X is not a top-level domain, then R(X) = R(P(X)), otherwise

o R(X) is empty.

Corrected Text

Let CAA(X) be the record set returned in response to performing a CAA record query on the label X, P(X) be the DNS label immediately above X in the DNS hierarchy, and A(X) be the target of a CNAME or DNAME alias record chain specified at the label X.

o If CAA(X) is not empty, R(X) = CAA (X), otherwise

o If A(X) is not null, and CAA(A(X)) is not empty, then R(X) = CAA(A(X)), otherwise

o If X is not a top-level domain, then R(X) = R(P(X)), otherwise

o R(X) is empty.

Thus, when a search at node X returns a CNAME record, the CA will follow the CNAME record chain to its target. If the target label contains a CAA record, it is returned.

Otherwise, the CA continues the search at the parent of node X.

Note that the search does not include the parent of a target of a CNAME record (except when the CNAME points back to its own path).

To prevent resource exhaustion attacks, CAs SHOULD limit the length of CNAME chains that are accepted. However CAs MUST process CNAME chains that contain 8 or fewer CNAME records.

APPENDIX B – CAA Contact Tag

These methods allow domain owners to publish contact information in DNS for the purpose of validating domain control.

B.1. CAA Methods

B.1.1. CAA contactemail Property

SYNTAX: contactemail

The CAA contactemail property takes an email address as its parameter. The entire parameter value MUST be a valid email address as defined in RFC 6532 section 3.2, with no additional padding or structure, or it cannot be used.

The following is an example where the holder of the domain specified the contact property using an email address.

$ORIGIN example.com. CAA 0 contactemail "domainowner@example.com"

The contactemail property MAY be critical, if the domain owner does not want CAs who do not understand it to issue certificates for the domain.

B.1.2. CAA contactphone Property

SYNTAX: contactphone

The CAA contactphone property takes a phone number as its parameter. The entire parameter value MUST be a valid Global Number as defined in RFC 3966 section 5.1.4, or it cannot be used. Global Numbers MUST have a preceding + and a country code and MAY contain visual separators.

The following is an example where the holder of the domain specified the contact property using a phone number.

$ORIGIN example.com. CAA 0 contactphone "+1 (555) 123-4567"

The contactphone property MAY be critical if the domain owner does not want CAs who do not understand it to issue certificates for the domain.

B.2. DNS TXT Methods

B.2.1. DNS TXT Record Email Contact

The DNS TXT record MUST be placed on the "_validation-contactemail" subdomain of the domain being validated. The entire RDATA value of this TXT record MUST be a valid email address as defined in RFC 6532 section 3.2, with no additional padding or structure, or it cannot be used.

B.2.2. DNS TXT Record Phone Contact

The DNS TXT record MUST be placed on the "_validation-contactphone" subdomain of the domain being validated. The entire RDATA value of this TXT record MUST be a valid Global Number as defined in RFC 3966 section 5.1.4, or it cannot be used.