1.3. PKI PARTICIPANTS

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

1.3.1. Certification Authorities

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

1.3.2. Registration Authorities

With the exception of sections 3.2.2.4 and 3.2.2.5, t~~T~~he 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. [Ballot 204]

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~~ Domain Name falls within the Domain Namespace of ABC Co.'s Registered Domain Name.

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

1.3.3. Subscribers

As defined in Section 1.6.1.

1.3.4. Relying Parties

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

1.3.5. Other Participants

Other groups that have participated in the development of these Requirements include the AICPA/CICA WebTrust for Certification Authorities task force and ETSI ESI. Participation by such groups does not imply

their endorsement, recommendation, or approval of the final product.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate Certificate Uses

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

1.4.2. Prohibited Certificate Uses

1.5. POLICY ADMINISTRATION

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

1.5.1. Organization Administering the Document

No stipulation.

1.5.2. Contact Person

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

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

1.5.3. Person Determining CPS suitability for the policy

No stipulation.

1.5.4. CPS approval procedures

No stipulation.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

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

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

sending the actual certificate request.

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

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

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

Audit 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~~Domain Name. The CA may use the FQDN returned from a DNS CNAME lookup as the ~~FQDN~~ Domain Name for the purposes of domain validation. If the ~~FQDN~~ Domain Name ~~contains~~ is a W~~w~~ildcard Domain Name~~character~~, then the CA MUST remove "*." ~~all wildcard labels~~ from the left most portion of requested ~~FQDN~~Domain Name. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

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

Base Domain Name: The portion of an applied-for ~~FQDN~~ Domain Name 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~~ Domain Names 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, and whose activities are not within the scope of the appropriate CA audits, but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein. [Ballot 204]

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

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

Domain Label: An individual component of a Domain Name.

Domain Name: A set of one or more Domain Labels, each separated by a single full stop character (".").~~The label assigned to a node in the Domain Name System.~~

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

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

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

Effective Date: 1 July 2012.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Parent Company: A company that Controls a Subsidiary Company.

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

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

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

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

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.3.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Requirements: The Baseline Requirements found in this document.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has "False" for Globally Reachable in either of the IANA Special-Purpose IP Address Registries:~~has marked as reserved:~~

https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml
~~http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml~~ or
https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml
~~http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml~~

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

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

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

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

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

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

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

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

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

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

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

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

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

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

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

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

Wildcard Certificate: A Certificate containing ~~an asterisk (*)~~ a Wildcard Domain Name in ~~the left-most position of~~ any of the Subject ~~Fully-Qualified Domain~~ Alternative 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

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VOIP	Voice Over Internet Protocol

2.2. PUBLICATION OF INFORMATION

The CA SHALL publicly disclose its Certificate Policy and/or Certification Practice Statement through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA SHALL publicly disclose its CA business practices to the extent required by the CA's selected audit scheme (see Section 8.1). The disclosures MUST include all the material required by RFC 2527 or RFC 3647, and MUST be structured in accordance with either RFC 2527 or RFC 3647.

Effective as of 8 September 2017, 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 the CA's policy or practice on processing CAA Records for ~~Fully Qualified~~ requested Domain Names; that policy shall be consistent with these Requirements. It shall clearly specify the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue. The CA SHALL log all actions taken, if any, consistent with its processing practice.

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

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

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

3.2.2.2. DBA/Tradename

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

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A Reliable Data Source;
3. Communication with a government agency responsible for the management of such DBAs or tradenames;
4. An Attestation Letter accompanied by documentary support; or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

3.2.2.3. Verification of Country

If the subject:countryName field is present, then the CA SHALL verify the country associated with the Subject using one of the following: (a) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address; (b) the ccTLD of the requested Domain Name; (c) information provided by the Domain Name Registrar; or (d) a method identified in Section 3.2.2.1. The CA SHOULD implement a process to screen proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.

3.2.2.4. Validation of Domain Authorization or Control

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

The CA SHALL confirm that, as of the date the Certificate issues, ~~either~~ the CA ~~or a Delegated Third Party~~ has validated each ~~Fully-Qualified~~ Domain Name ~~(FQDN)~~ listed in the Certificate using at least one of the methods listed below, or is within the Domain Namespace of a Fully-Qualified Domain Name (FQDN) that has been validated using at least one of the methods listed below (not including the method defined in section 3.2.2.4.8). [Ballot 204]

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

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

3.2.2.4.1 [Reserved]

3.2.2.4.2 [Reserved]

3.2.2.4.3 [Reserved]

3.2.2.4.4 [Reserved]

3.2.2.4.5 Domain Authorization Document

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

3.2.2.4.6 Agreed-Upon Change to Website

Confirming the Applicant's control over the requested ~~FQDN~~ Domain Name by confirming one of the following under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of Domain Validation, on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port:

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

If a Random Value is used, the CA ~~or Delegated Third Party~~ [Ballot 204] SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the certificate request, the timeframe permitted for reuse of validated information relevant to the certificate (such as in Section 3.3.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).

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

3.2.2.4.7 [Reserved]

3.2.2.4.8 [Reserved]

3.2.2.4.9 [Reserved]

3.2.2.4.10. TLS Using a Random Number

Confirming the Applicant's control over the requested ~~FQDN~~ Domain Name 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 Other Methods

The CA SHALL confirm that, as of the date the Certificate issues, ~~either~~ the CA ~~or a Delegated Third Party~~ [Ballot 204] has validated each ~~Fully Qualified~~ Domain Name ~~(FQDN)~~ listed in the Certificate by using any method of confirmation, provided that the CA maintains documented evidence that the method of confirmation establishes that the Applicant is the Domain Name Registrant or has control over the ~~Fully Qualified~~ Domain Name ~~(FQDN)~~.

3.2.2.5. Authentication for an IP Address

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

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

2. Obtaining documentation of IP address assignment from the Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC);
3. Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name under Section 3.2.2.4; or
4. Using any other method of confirmation, provided that the CA maintains documented evidence that the method of confirmation establishes that the Applicant has control over the IP Address to at least the same level of assurance as the methods previously described.

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

3.2.2.6. Additional Validation for Wildcard Certificates ~~Domain Validation~~

Before issuing a Wildcard C~~c~~ertificate ~~with a wildcard character (*) in a CN or subjectAltName of type DNS-ID~~, the CA MUST establish and follow a documented procedure[^pubsuffix] ~~-~~that determines if the FQDN portion of any W~~w~~ildcard Domain Name in the certificate is ~~character occurs in the first label position to the left of a~~ "registry-controlled" ~~label~~ or is a "public suffix" (e.g. "*.com", "*.co.uk", see RFC 6454 Section 8.2 for further explanation).

If the FQDN portion of any W~~w~~ildcard Domain Name in the certificate ~~would fall within the label immediately to the left of a~~ is registry-controlled~~:~~ or is a "public suffix", CAs MUST refuse issuance unless the applicant proves its rightful control of the entire Domain Namespace. (e.g. CAs MUST NOT issue "*.co.uk" or "*.local", but MAY issue "*.example.com" to Example Co.).
~~Prior to September 1, 2013, each CA MUST revoke any valid certificate that does not comply with this section of the Requirements.~~

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

3.2.2.7. Data Source Accuracy

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

1. The age of the information provided,

2. The frequency of updates to the information source,

3. The data provider and purpose of the data collection,

4. The public accessibility of the data availability, and

5. The relative difficulty in falsifying or altering the data.

Databases maintained by the CA, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under this Section 3.2.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit a Certificate Application

In accordance with Section 5.5.2, the CA SHALL maintain an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. The CA SHALL use this information to identify subsequent suspicious certificate requests.

4.1.2. Enrollment Process and Responsibilities

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

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

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

Prior to the issuance of a Certificate, the CA SHALL obtain from the Applicant a certificate request in a form prescribed by the CA and that complies with these Requirements. One certificate request MAY suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in Section 3.3.1, provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. The certificate request MAY be made, submitted and/or signed electronically.

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

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification and Authentication Functions

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

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

Section 6.3.2 limits the validity period of Subscriber Certificates. The CA MAY use the documents and data provided in Section 3.2 to verify certificate information, provided that the CA obtained the data or document from a source specified under Section 3.2 no more than 825 days prior to issuing the Certificate.

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

4.9. CERTIFICATE REVOCATION AND SUSPENSION

4.9.1. Circumstances for Revocation

4.9.1.1. Reasons for Revoking a Subscriber Certificate

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

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

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

3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;

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

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

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

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

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

9. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the

CA's Certificate Policy or Certification Practice Statement;

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

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

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

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

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

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

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

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

1. The Subordinate CA requests revocation in writing;

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

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

4.9.7. CRL Issuance Frequency

For the status of Subscriber Certificates:

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

For the status of Subordinate CA Certificates:

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

4.9.8. Maximum Latency for CRLs

No stipulation.

4.9.9. On-line Revocation/Status Checking Availability

OCSP responses MUST conform to RFC6960 and/or RFC5019. OCSP responses MUST either:

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

In the latter case, the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10. On-line Revocation Checking Requirements

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

For the status of Subscriber Certificates:

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

For the status of Subordinate CA Certificates:

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

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

Effective 1 August 2013, OCSP responders for CAs which are not Technically Constrained in line with Section 7.1.5 MUST NOT respond with a "good" status for such certificates.

4.9.11. Other Forms of Revocation Advertisements Available

If the Subscriber Certificate is for a high-traffic ~~FQDN~~Domain Name, 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

a. Extensions that do not apply in the context of the public Internet (such as an extendedKeyUsage value for a service that is only valid in the context of a privately managed network), unless:
   i. such value falls within an OID arc for which the Applicant demonstrates ownership, or
   ii. the Applicant can otherwise demonstrate the right to assert the data in a public context; or

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

7.1.2.5. Application of RFC 5280

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

7.1.3. Algorithm Object Identifiers

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

Effective 16 January 2015, CAs SHOULD NOT issue Subscriber Certificates utilizing the SHA-1 algorithm with an Expiry Date greater than 1 January 2017 because Application Software Providers are in the process of deprecating and/or removing the SHA-1 algorithm from their software, and they have communicated that CAs and Subscribers using such certificates do so at their own risk.

7.1.4. Name Forms

7.1.4.1. Issuer Information

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

7.1.4.2. Subject Information – Subscriber 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.

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 one of the following types: ~~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.~~

1. dNSName: the entry MUST contain either a Fully-Qualified Domain Name or Wildcard Domain Name that the CA has validated in accordance with section 3.2.2.4. FQDNs and the FQDN portion of Wildcard DNs must comply with RFC 5280 section 4.2.1.6 with the following exception: underscore characters ("_") are allowed in Domain Labels such that replacing all underscore characters with hyphen characters ("-") would result in a

valid Domain Label. CAs MUST NOT include Domain Labels which have hyphens as the third and fourth characters unless the first character is "x" or "X", the second character is "n" or "N", and the fifth and later characters are a valid Punycode string. CAs MUST additionally validate that Wildcard DNs are consistent with section 3.2.2.6. The entry MUST NOT contain an Internal Name.

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

2. iPAddress: the entry MUST contain an IP address that the CA has validated in accordance with Section 3.2.2.5. The entry MUST NOT contain a Reserved IP Address.

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). When including a Domain Name in a common name, CAs MUST only use LDH labels as defined in RFC 5890 and MUST NOT use U-labels. When including an IPv6 address in a common name, CAs MUST use a format conforming to Section 4 or Section 5 of RFC 5952. When including an IPv4 address in a common name, CAs MUST encode the name as an IPv4Address as defined in RFC 3986.

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.