Ballot 190 (PB 7-13-2017)

CA/Browser Forum

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

CA/Browser Forum.
Version 1.4.10
July 26, 2017
cabforum.org

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: Any name from the set of Fully-Qualified Domain Names derived from a Requested Domain Name using the rules described in section 3.2.2.4

Deleted: The

Deleted: Name used to obtain authorization for certificate issuance for a given Domain Name. The CA may use the FQDN returned from a DNS CNAME lookup as the Domain Name for the purposes of domain validation. If the Domain Name is a Wildcard Domain Name, then the CA MUST remove "*." from the left most portion of requested 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 a requested 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 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.

Deleted: n

Deleted: applied-for

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.

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 or in a DNS SOA record.

Deleted: of the Base Domain Name

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 ("."). Fully-Qualified Domain Names and Wildcard Domain Names are Domain Names.

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 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 generated by the CA and 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.

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:
https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml
https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

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.

Deleted: 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.¶
¶

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 (2.23.140.2.1), 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 a Wildcard Domain Name in any of the Subject Alternative Names 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

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.

Prior to issuing the Certificate, the CA SHALL confirm that, as of the date the Certificate issues, the CA has validated each Domain Name listed in the Certificate using at least one of the methods listed below.

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

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

Authorization Domain Names are the set of names created from a Domain Name using the following rules:

1. The set initially includes only the Base Domain Name for the Domain Name
2. If the Domain Name is a Wildcard Domain Name, include the Authorizations Domain Names for the FQDN portion of the Wildcard Domain Name.
3. If the Domain Name is a Fully-Qualified Domain Name, include each Domain Name created by pruning a single Domain Label from the Domain Name from left to right until the resulting FQDN is the Base Domain Name.
4. If a DNS lookup for CNAME records for the Domain Name returns a FQDN, include the Authorizations Domain Names for the returned FQDN.

Note: 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 Validating the Applicant as a Domain Contact

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

1. The CA authenticates the Applicant's identity under BR Section 3.2.2.1 and the authority of the Applicant Representative under BR Section 3.2.5, OR

2. The CA authenticates the Applicant's identity under EV Guidelines Section 11.2 and the agency of the Certificate Approver under EV Guidelines Section 11.8; OR

3. The CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

Deleted: The

Deleted: , 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)

Deleted: certificates

Deleted: 3

Deleted: 3

Deleted: certificate

Formatted: Highlight

Deleted: [Reserved]

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

Confirming the Applicant's control over the Domain Name 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 of the Base Domain Name.

Each email, fax, SMS, or postal mail MAY confirm control of multiple Base 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 Domain Name 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 list remain unchanged.

The confirming response MUST be received no more than 30 days after the creation of the Random Value. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

Formatted: Highlight

Deleted: **[Reserved]**

3.2.2.4.3 Phone Contact with Domain Contact

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

Each phone call SHALL be made to a single number and MAY confirm control of multiple Domain Name, 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.

Formatted: Highlight

Deleted: [Reserved]

3.2.2.4.4 Email to Constructed Address

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

Each email MAY confirm control of multiple Domain Names, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each Domain Name 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 list SHALL remain unchanged.

The confirming response MUST be received no more than 30 days after the creation of the Random Value. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

Formatted: Highlight

Deleted: [Reserved]

3.2.2.4.5 Domain Authorization Document

Confirming the Applicant's control over the requested 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 of the Base Domain Name. 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.

Formatted: Highlight

3.2.2.4.6 Agreed-Upon Change to Website

Confirming the Applicant's control over the requested 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 an Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port:

Deleted: the

Formatted: Highlight

1. The presence of either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA, contained in the content of a file or on a web page in the form of a meta tag. The entire Random Value or Request Token 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 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: Examples of Request Tokens include, but are not limited to: (i) a hash of the public key; (ii) a hash of the Subject Public Key Info [X.509]; and (iii) a hash of a PKCS#10 CSR. A Request Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow Certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests. This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR. E.g. `echo $(date -u +%Y%m%d%H%M) $(sha256sum <r2.csr) | sed "s/[ -]//g"` The script outputs: 201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f The CA SHOULD define in its CPS (or in a document referenced from the CPS) the format of Request Tokens it accepts.

3.2.2.4.7 DNS Change

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

If a Random Value is used, the CA MUST confirm the presence of the Random Value no more than 30 days after the creation of the random value. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

3.2.2.4.8 IP Address

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

3.2.2.4.9 Test Certificate

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

3.2.2.4.10. TLS Using a Random Value

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

3.2.2.4.11 Prior Validation Methods

Confirming the Applicant's control over the requested Domain Name by confirming that the Applicant either is the Domain Name Registrant of the Base Domain Name or has control over an Authorization Domain Name using data and documents, as allowed in section 4.2.1, obtained by the CA prior to March 1, 2017 and using one of methods 1, 2, 3, 4, 5, or 6 from section 3.2.2.4 of version 1.3.7 of these Requirements.

Deleted: Required Website Content

Deleted: Required Website Content

Deleted: certificate

Deleted: certificate

Deleted: certificate

Deleted: 3

Deleted: 3

Deleted: certificate

Formatted: Font: (Default) Courier New

Deleted: should

Formatted: Highlight

Deleted: [Reserved]

Commented [PZB1]: 3.2.2.4.8 intentionally does not include "Base Domain Name" or "Authorization Domain Name"

Deleted: [Reserved]

Formatted: Highlight

Deleted: [Reserved]

Deleted: Number

Deleted: the

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Deleted: Other Methods¶
The CA SHALL confirm that, as of the date the Certificate issues, the CA has validated each Domain Name 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 Domain Name.

9.10. TERM AND TERMINATION

9.10.1. Term

9.10.2. Termination

9.10.3. Effect of termination and survival

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

9.12. AMENDMENTS

9.12.1. Procedure for amendment

9.12.2. Notification mechanism and period

9.12.3. Circumstances under which OID must be changed

9.13. DISPUTE RESOLUTION PROVISIONS

9.14. GOVERNING LAW

9.15. COMPLIANCE WITH APPLICABLE LAW

9.16. MISCELLANEOUS PROVISIONS

9.16.1. Entire Agreement

9.16.2. Assignment

9.16.3. Severability

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

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

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

9.16.4. Enforcement (attorneys' fees and waiver of rights)

9.16.5. Force Majeure

9.17. OTHER PROVISIONS

APPENDIX A: AUTHORIZATION DOMAIN NAME EXAMPLES

Formatted: Heading 1, Indent: Left: 0.25"

Formatted: Normal

This Appendix is non-normative.

Examples: The set of Authorization Domain Names for '*.images.example.com' include 'images.example.com' and 'example.com' but do not include '*.images.example.com'. The set of Authorization Domain Names 'beta.ship.example.com', include 'beta.ship.example.com', 'ship.example.com', 'and 'example.com'.

Formatted: Normal