

Document History

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

* Effective Date and Additionally Relevant Compliance Date(s)

Implementers' Note: Version 1.1 of these SSL Baseline Requirements was published on September 14, 2012. Version 1.1 of WebTrust's SSL Baseline Audit Criteria and ETSI Technical Standard Electronic Signatures and Infrastructures (ESI) 102 042 version 2.3.1 incorporate version 1.1 of these Baseline Requirements and are currently in effect. See <http://www.webtrust.org/homepage-documents/item27839.aspx> and also http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.03.01_60/ts_102042v020301p.pdf. The CA/Browser Forum continues to improve the Baseline Requirements, and we encourage all CAs to conform to each revision on the date specified without awaiting a corresponding update to an applicable audit criterion. In the event of a conflict between an existing audit criterion and a guideline revision, we will communicate with the audit community and attempt to resolve any uncertainty, and we will respond to implementation questions directed to questions@cabforum.org. Our coordination with compliance auditors will continue as we develop guideline revision cycles that harmonize with the revision cycles for audit criteria, the compliance auditing periods and cycles of CAs, and the CA/Browser Forum's guideline implementation dates.

Relevant Compliance Dates

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Internal ~~Server~~ 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 Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using 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

the Applicant controls the Fully-Qualified Domain Name or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate.

Wildcard FQDNs are permitted.

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

9.2.2 Subject Common Name Field

Certificate Field: subject:commonName (OID 2.5.4.3)

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

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

9.2.3 Subject Domain Component Field

Certificate Field: subject:domainComponent (OID 0.9.2342.19200300.100.1.25)

Required/Optional: Optional.

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

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

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

9.2.4 Subject Distinguished Name Fields

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

Optional.

Contents: If present, the subject:organizationName field MUST contain either the Subject's name or DBA as verified under Section 11.2. The CA may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if 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.

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

Optional if the subject:organizationName field is present.

Prohibited if the subject:organizationName field is absent.

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

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

11.1.3 Wildcard Domain Validation

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

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

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

†Determination of what is “registry-controlled” versus the registerable portion of a Country Code Top-Level Domain Namespace is not standardized at the time of writing and is not a property of the DNS itself. Current best practice is to consult a “public suffix list” such as <http://publicsuffix.org/>. If the process for making this determination is standardized by an RFC, then such a procedure SHOULD be preferred.

11.1.4 New gTLD Domains

CAs SHOULD NOT issue Certificates containing a new gTLD under consideration by ICANN. Prior to issuing a Certificate containing an Internal ~~Server~~Name with a gTLD that ICANN has announced as under consideration to make operational, the CA MUST provide a warning to the applicant that the gTLD may soon become resolvable and that, at that time, the CA will revoke the Certificate unless the applicant promptly registers the domain name. When a gTLD is delegated by inclusion in the IANA Root Zone Database, the Internal Name becomes a Domain Name, and at such time, a Certificate with such gTLD, which may have complied with these Requirements at the time it was issued, will be in a violation of these Requirements, unless the CA has verified the Subscriber’s rights in the Domain Name. The provisions below are intended to prevent such violation from happening.

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

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