CHANGES PROPOSED BY BALLOT [92] – 16 November 2012

CURRENT BASELINE REQUIREMENTS	PROPOSED NEW LANGUAGE
[No current definition of Public IP Address]	**INSERT** in Section 4. Definitions the following: Public IP Address: An IP Address that is not a Reserved IP Address.
9.2.1 Subject Alternative Name Extension **Certificate Field:** extensions:subjectAltName **Required/Optional:** Required **Contents**: This extension MUST contain at least one entry. Each entry MUST be either a dNSName containing the Fully-Qualified Domain Name or an iPAddress containing the IP address of a server. The CA MUST confirm that the Applicant controls the Fully-Qualified Domain Name or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate. Wildcard FQDNs are permitted. As of the Effective Date of these Requirements, prior to the issuance of a Certificate with a	**REPLACE** Section 9.2.1 (Subject Alternative Name Extension) with the following: **9.2.1 Subject Alternative Name Extension** **Certificate Field:** extensions:subjectAltName **Required/Optional:** Required **Contents:** This extension MUST contain at least one entry that is either a Fully-Qualified Domain Name or Public IP Address. Each subjectAltName entry MUST either be a Domain Name or an IP Address. The CA MUST confirm the Applicant's control of each dNSName or Public IP Address entry in accordance with Section 11.1. SubjectAltName entries MAY include domain Names containing wildcard characters. If the subjectAltName is: 1) a Public IP Address, 2) a Registered Domain Name that has a Domain Name Registrant different than (and not an Affiliate of) the Domain Name Registrant of any other Registered Domain Name in the subjectAltName extension in the Certificate, or 3) a Reserved IP Address or Internal Server Name. then the CA MUST verify the identity of an entity that controls the private key in accordance with Section 11.2 and include the Subject Identity Information in the issued Certificate in accordance with 9.2.4. The CA MAY include explanatory information in the Subject Organizational Unit field or a non-subject certificate field to clarify the Subject Identity Information included in the Certificate. Prior to issuing a Certificate containing an Internal

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.	Server Name or Reserved IP Address, 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. As of the Effective Date, the CA SHALL NOT issue a certificate with an Expiry Date later than 1 November 2015 if the subjectAlternativeName contains 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).	**REPLACE** Section 9.2.2 (Subject Common Name Field) with the following: **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 Public IP address or single Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension (see Section 9.2.1). Reserved IP Addresses and Internal Server Names are prohibited.
10.2.3 Information Requirements 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	**REPLACE** Section 10.2.3 (Information Requirements) with the following: **10.2.3 Information Requirements** 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. 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.	or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. Applicant information MUST include, but not be limited to, at least one Subject Alternative Name as defined in Section 9.2.1.
[No current provisions]	**INSERT** in Section 11.1 (Authorization by Domain Name Registrant) the following two new sections: 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 SHALL refuse issuance unless the applicant proves its rightful control of the entire Domain Namespace. (e.g. CAs SHALL NOT issue "*.co.uk", but MAY issue "*.example.co.uk" to Example Ltd.) †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.