Implications of RFC6125 and Subject Alternative Names

The following sections will be amended in the Baseline Requirements document.

4. Definitions

Public IP Address: An IP Address that is not a Reserved IP Address.

Root Domain Name: The label immediately to the left of a registry-controlled or public suffix.

U-label: As defined in RFC 5890 (http://tools.ietf.org/html/rfc5890#section-2.3.2.1)

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 be a Domain Name or 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.

A Certificate MUST contain Subject Identity Information verified in accordance with Section 9.2.4 if any subjectAltName entry is:

1) a Public IP Address,
2) a Domain Name containing a Root Domain Name which is different from the Root Domain Name of any other Domain Name included within the subjectAltName extension, or
3) a Reserved IP Address or Internal Server Name.

If all subjectAltName entries contain the same Root Domain Name, the CA MAY omit the Subject Identity Information. For example, the entries of:- www.**domain.com**, **domain.com**, example.**domain.com**, *.level.**domain.com** all contain the same Root Domain Name and a corresponding certificate MAY omit the Subject Identity Information. However, adding **domain.co.uk** will cause the certificate to include multiple Root Domains and require inclusion of Subject Identity Information.

Prior to issuing a Certificate containing an Internal 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 Public IP address or single Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension (see Section 0). Reserved IP Addresses and Internal Server Names are prohibited.

9.2.7 Other Subject Attributes

[Text from other errata]

All label components in a Fully-Qualified Domain Name as part of a Subject Alternative Name of type dNSName or Subject commonName attribute that are not part of the registry-assigned name (e.g. the "foo", "bar", and "baz" labels of "foo.bar.baz.example.com") must meet the following guidelines:

1. Hostname labels SHALL be valid according to either RFC3490 rules for Internationalized Domain Names. (IDNA 2003) [http://tools.ietf.org/html/rfc3490] or RFC5890 rules for Internationalized Domain Names (IDNA 2008) [http://tools.ietf.org/html/rfc5890].

2. Hostname U-label components SHALL follow the "Moderately Restrictive" behavior described by Unicode Technical Standard #39, "UNICODE SECURITY MECHANISMS" [http://www.unicode.org/reports/tr39/#Restriction_Level_Detection]

3. Hostname U-label components SHALL NOT include confusable bidirectional text. [http://unicode.org/reports/tr36/#Bidirectional_Text_Spoofing] and [http://www.ietf.org/rfc/rfc3987.txt]

    a. Hostname label components SHALL NOT include left-to-right override characters. U+200E, U+202E

    b. Hostname label components SHALL NOT include both left-to-right and right-to-left characters

    c. Hostname label components using a right-to-left character must start and end with right-to-left characters, with the exception that labels using right-to-left characters may end with combining marks or numbers

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 Subject Alternative Extension Name as defined in Section 9.2.1.

11.1 Authorization by Domain Name Registrant

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 can prove its rightful control of the entire segment of the DNS space. (e.g. CAs SHALL NOT issue "*.co.uk", but MAY issue "*.appspot.com" to Google, Inc.)

> †Determination of what suffixes are "registry-controlled" 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 a future Internet Draft, such a procedure SHOULD be preferred.

11.1.4 New gTLD Domains

ICANN will begin the process of issuing new generic Top Level Domains (gTLDs) beginning in 2012, therefore certain Certificates for non-public names will need to be revoked on an accelerated schedule. CAs SHALL review the proposed new gTLDs and compare them against their records for issued certificates. Where the locally-qualified subject or subject alternative name of a previously issued Certificate would be a valid FQDN under a new gTLD, the CA SHALL re-verify that the Subscriber is the Domain Name Registrant or the Applicant has control over the FQDN in accordance with Section 11 of this document. If the CA cannot verify the customer's right to use, or control of, the Fully-Qualified Domain Name(s) in the Certificate, the CA SHALL notify the Customer that:

> 1. The subscriber must take action to prevent the Certificate from being presented in response to any requests originating from the public Internet following the ability to publicly resolve in the DNS a new gTLD.

2. The Certificate will be revoked no later than 6 months following the ability to publicly resolve in the DNS a new gTLD if the Subscriber cannot prove their right to use or control of the FQDN

The CA SHALL revoke the certificate no later than 6 months following the ability to publicly resolve in the DNS a new gTLD if the Subscriber fails to prove their right to use or control of the FQDN.

Should any such certificate be found to be visible from the public Internet after the new gTLD is operational, the issuing CA SHALL immediately revoke all such certificates for the subscriber.