

This proposal modifies section 7.1.4.3.1. to permit inclusion of rfc822Names and the WFA otherName type. Here's my draft ballot:

Modify Section 7.1.4.2.1. as follows:

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 entries: 1) either a dNSName containing the Fully-Qualified Domain Name, 2) or an iPAddress containing the IP address of a server, 3) a rfc822Name containing an RFC 5322 email address, or 4) an otherName with the id-wfa-hotspot-friendlyName type where id-wfa-hotspot-friendlyName OBJECT IDENTIFIER ::= { 1.3.6.1.4.1.40808.1.1.1 }. For each dNSName and iPAddress included, 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. For each rfc822Name included, the CA MUST confirm the Applicant controls either the included email address or the domain portion of the email address. For permitted otherNames types, the CA MUST follow the requirements established by the entity specifying the otherName type. 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 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. Effective May 1, 2015, each CA SHALL revoke all unexpired Certificates with an Internal Name using onion as the right-most label in an entry in the subjectAltName Extension or commonName field unless such Certificate was issued in accordance with Appendix F of the EV Guidelines.