Amendment to Section 11.1.1 of CA/Browser Forum Baseline Requirements to clarify acceptable methods of validating domain control:

1) Add the following definitions:

Base Domain: The portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "~~domain~~example.co.uk" or "~~domain~~example.com").

Random Value: A value specified by a CA to the Applicant that exhibits 128 bits of entropy.

Request Token: A value derived in a method specified by the CA from the public key to be certified. The uniqueness of the Request Token and the irreversibility of the derivation to be at least as strong as those of the cryptographic signature algorithm to be used to sign the certificate.

2) Section 11.1.1 of the CA/Browser Forum's Baseline Requirements is amended as follows:

…

11.1.1 Authorization by Domain Name Registrant

For each Fully-Qualified Domain Name listed in a Certificate, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by:

1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar through a Reliable Method of Communication, for example using information provided through WHOIS; or

2. Confirming authorization of the Certificate's issuance directly with the Domain Name Registrant using a Reliable Method of Communication that is (i) obtained from the Domain Name Registrar or (ii) listed as the "registrant", "technical", or "administrative" contact for the WHOIS record of the Base Domain; or

4. Confirming authorization for the Certificate's issuance through an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN; or

5. Relying upon a Domain Authorization Document that meets the requirements listed below; or

6. Having the Applicant demonstrate control over the FQDN or Base Domain by adding a file whose name or contents include ~~containing~~ a Random Value or a Request Token to the "/.well-known/certificate" directory at either the FQDN or the Base Domain in accordance with RFC 5785; or

7. Having the Applicant demonstrate control over the FQDN or Base Domain by the Applicant making a change to information in a DNS record for the FQDN or Base Domain where the change is to insert a Random Value or Request Token; or

8. Having the Applicant demonstrate control over the requested FQDN by the CA confirming, in accordance with section 11.1.1, the Applicant's controls the FQDN (or Base Domain of the FQDN) returned from a DNS lookup for CNAME records for the requested FQDN; or

9. Having the Applicant demonstrate control over the requested FQDN by the CA confirming, in accordance with section 11.1.2, that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the requested FQDN; or

10. Having the Applicant demonstrate control over the FQDN by providing a TLS service on a host found in DNS for the FQDN and having the CA (i) initiate a TLS connection with the host and (ii) verify a Random Value or Request Token that is ~~a~~ in a format recognized as a valid TLS response.

Note: For purposes of determining the appropriate domain name level or Domain Namespace, the registerable Domain Name is the Base Domain ~~second-level domain~~ for generic top-level domains (gTLD) such as .com, .net, or .org, or, if the Fully Qualified Domain Name contains a 2 letter Country Code Top-Level Domain (ccTLD), then the domain level is whatever is allowed for registration according to the rules of that ccTLD. If the CA relies upon a Domain Authorization Document to confirm the Applicant's control over a FQDN, then the Domain Authorization Document MUST substantiate that the communication came from either the Domain Name Registrant (including any private, anonymous, or proxy registration service) or the Domain Name Registrar listed in the WHOIS. The CA MUST verify that the Domain Authorization Document was either (i) dated on or after the certificate request date or (ii) used by the CA to verify a previously issued certificate and that the Domain Name's WHOIS record has not been modified since the previous certificate's issuance.

Note: FQDNs 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.

Note: For the purpose of verifying a wildcard FQDN, the CA MUST verify either the Base Domain of the wildcard FQDN or the entire Domain Name Label to the right of the wildcard character.

Note: Where confirmation is sought by email and an automated process for recording the successful response is used, such as the provision of a hyper-link in an email, a Random Value MUST be part of the email and verified by the CA to be present in the response.