**Proposed Revisions to Domain Validation Requirements**

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 to Section 1.6:

[Replace with cross-reference to public suffix

Authorization Domain Name: The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of Domain Validation. Authorization Domain Name Domain Name returned to the CA from a DNS lookup for the CNAME record for the Registered Domain is determined by one of the following two (2) methods:

1. remove all wildcard labels from the requested FQDN and

prune zero or more labels from left to right until encountering a Registered Domain Name; or

(ii).

. and (iii) from the FQDN requested for inclusion in a Certificate or (ii) for wildcard FQDNs, created by pruning at least one or more components from the FQDN, and (iii) contains at least the second-level domainBase Domain for generic top-level domains (gTLD) such as .com, .net, or .org, or, if the FQDN contains a 2 letter Country Code Top-Level Domain (ccTLD), then contains at least whatever domain information is allowed for registration according to the rules of that ccTLD.

Random Value: A value specified by a CA to the Applicant that exhibits at least 112 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.

Test Certificate: A Certificate which includes data that renders the Certificate unusable for use by an application software vendor or publicly trusted TLS server such as the inclusion of a critical extension that is not recognized by any known application software vendor or a certificate issued under a root certificate not subject to these Requirements.

1. Section 11.1.1 of the CA/Browser Forum’s Baseline Requirements is amended as follows:

…

* + 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 (or the Applicant’s Parent Company, Subsidiary Company, or Affiliate, collectively referred to as “Applicant” for the purposes of this section) 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 Certificate issuance for the FQDN directly with the Domain Name Registrant using a Reliable Method of Communication by obtaining that authorization from (i) the Domain Name Registrar or (ii) the contact listed as the “registrant”, “technical”, or “administrative” contact in the WHOIS record for the Registered Domain Name; or

3. Confirming authorization of Certificate issuance for the FQDN 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 an Authorization Domain Name; or

4. Relying upon a Domain Authorization Document that (i) substantiates 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 and (ii) is verified by the CA as either (a) dated on or after the certificate request date or (b) used by the CA to verify a previously issued certificate and that the Registered Domain Name’s WHOIS record has not been modified since the previous certificate’s issuance; or

5. Having the Applicant demonstrate control over the FQDN by adding a file whose name or contents include a Random Value or a Request Token to “/.well-known/certificate” directory, either at port port 80, SMTP, 443, SFTP, for/ at an Authorization Domain Name in accordance with RFC 5785; or

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

7. Having the Applicant demonstrate control over the requested FQDN by the CA confirming the Applicant controls an Authorization Domain Name returned from a DNS lookup for CNAME records for the requested FQDN provided that the CA performs one of subsections 1 through 6 above (or also this subsection 7, iteratively if necessary); or

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

9. Having the Applicant demonstrate practical control over the FQDN by the Applicant requesting and then installing a Test Certificate issued by the CA on the FQDN which is accessed and then validated via https by the CA either at port port 80, SMTP, 443, SFTP, ….

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, the CA MUST verify that a value that is unpredictable and previously unknown to the applicant included in the email is also present in the response. The CA MUST NOT rely on a Random Value, Request Token or Test Certificate generated more than 14 days prior to completion of the verification under this section.

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.