**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. Amend the definition of Domain Authorization Document as follows:

Domain Authorization Document: A Verified Legal Opinion, Verified Accountant Letter, or Documentation provided by, or a CA’s documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

1. Add the definition of a Verified Legal Onion and Verified Accountant Letter from the EV Guidelines to the Baseline Requirements
2. 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 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;

2. Confirming authorization of the Certificate’s issuance directly with the Domain Name Registrant through a Reliable Method of Communication provided by the Domain Name Registrar;

3. Confirming authorization of the Certificate’s issuance directly with the Domain Name Registrant using the contact information listed in the WHOIS record’s “registrant”, “technical”, or “administrative” field;

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;

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

6. Having the Applicant demonstrate practical control over the FQDN by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the FQDN;

7. Having the Applicant demonstrate practical control over the FQDN by the Applicant making an agreed-upon change to information in a DNS record for the FQDN; or

8) 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.

Note: For purposes of determining the appropriate domain name level or Domain Namespace, the registerable Domain Name is the 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.