Ballot 180 (showing changes from Guidelines as of 10-25-2016)

BR 3.2.2.4 Validation of Domain Authorization or Control

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain.

The CA SHALL confirm that, as of the date the Certificate issues, either the CA or a Delegated Third Party has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate ~~using at least one of the methods listed below~~ **by using any method of confirmation, provided that the CA maintains documented evidence that the method of confirmation establishes that the Applicant is the Domain Name Registrant or has control over the Fully Qualified Domain Name (FQDN).**

Completed confirmations of Applicant authority may be valid for the issuance of multiple certificates over time. In all cases, the confirmation must have been initiated within the time period specified in the relevant requirement (such as Section 3.3.1 of this document) prior to certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

~~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.~~

~~**3.2.2.4.1 Validating the Applicant as a Domain Contact.**~~

~~Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact directly with the Domain Name Registrar. This method may only be used if:~~

1. ~~The CA authenticates the Applicant's identity under BR Section 3.2.2.1 and the authority of the Applicant Representative under BR Section 3.2.5, OR~~
2. ~~The CA authenticates the Applicant's identity under EV Guidelines Section 11.2 and the agency of the Certificate Approver under EV Guidelines Section 11.8; OR~~
3. ~~The CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.~~

~~**3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact**~~

~~Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact.~~

~~Each email, fax, SMS, or postal mail MAY confirm control of multiple Authorization Domain Names.~~

~~The CA or Delegated Third Party MAY send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email, fax, SMS, or postal mail.~~

~~The Random Value SHALL be unique in each email, fax, SMS, or postal mail.~~

~~The CA or Delegated Third Party MAY resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.~~

~~The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.~~

~~**3.2.2.4.3 Phone Contact with Domain Contact**~~

~~Confirming the Applicant's control over the requested FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The CA or~~

~~Delegated Third Party MUST place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.~~

~~Each phone call SHALL be made to a single number and MAY confirm control of multiple FQDNs, provided that the phone number is identified by the Domain Registrar as a valid contact method for every Base Domain Name being verified using the phone call.~~

~~3.2.2.4.4 Constructed Email to Domain Contact~~

~~Confirming the Applicant's control over the requested FQDN by (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.~~

~~Each email MAY confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed.~~

~~The Random Value SHALL be unique in each email.~~

~~The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient SHALL remain unchanged.~~

~~The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.~~

~~3.2.2.4.5 Domain Authorization Document~~

~~Confirming the Applicant's control over the requested FQDN by relying upon the attestation to the authority of the Applicant to request a Certificate contained in a Domain Authorization Document. The Domain Authorization Document MUST substantiate that the communication came from the Domain Contact. The CA MUST verify that the Domain Authorization Document was either (i) dated on or after the date of the domain validation request or (ii) that the WHOIS data has not materially changed since a previously provided Domain Authorization Document for the Domain Name Space.~~

~~3.2.2.4.6 Agreed-Upon Change to Website~~

~~Confirming the Applicant's control over the requested FQDN by confirming one of the following under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of Domain Validation, on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port:~~

1. ~~The presence of Required Website Content contained in the content of a file or on a web page in the form of a meta tag. The entire Required Website Content MUST NOT appear in the request used to retrieve the file or web page, or~~
2. ~~The presence of the Request Token or Request Value contained in the content of a file or on a webpage in the form of a meta tag where the Request Token or Random Value MUST NOT appear in the request.~~

~~If a Random Value is used, the CA or Delegated Third Party SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the certificate request, the timeframe permitted for reuse of validated information relevant to the certificate (such as in Section 3.3.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).~~

~~**Note:** Examples of Request Tokens include, but are not limited to: (i) a hash of the public key; (ii) a hash of the Subject Public Key Info [X.509]; and (iii) a hash of a PKCS#10 CSR. A Request Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests. This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR. E.g. echo date -u +%Y%m%d%H%M~~

~~sha256sum <r2.csr | sed "s/[ ]//g" The script outputs: 201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f The CA should define in its CPS (or in a document referenced from the CPS) the format of Request Tokens it accepts.~~

~~3.2.2.4.7 DNS Change~~

~~Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value or Request Token in a DNS TXT or CAA record for an Authorization Domain Name or an Authorization Domain Name that is prefixed with a label that begins with an underscore character.~~

~~If a Random Value is used, the CA or Delegated Third Party SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the certificate request, the timeframe permitted for reuse of validated information relevant to the certificate (such as in Section 3.3.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).~~

~~3.2.2.4.8 IP Address~~

~~Confirming the Applicant's control over the requested FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with section 3.2.2.5.~~

~~3.2.2.4.9 Test Certificate~~

~~Confirming the Applicant's control over the requested FQDN by confirming the presence of a non-expired Test Certificate issued by the CA on the Authorization Domain Name and which is accessible by the CA via TLS over an Authorized Port for the purpose of issuing a Certificate with the same Public Key as in the Test Certificate.~~

~~3.2.2.4.10. TLS Using a Random Number~~

~~Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value within a Certificate on the Authorization Domain Name which is accessible by the CA via TLS over an Authorized Port.~~

EVGL 11.7

11.7.1. Verification Requirements

(1) For each Fully-Qualified Domain Name listed in a Certificate, other than a Domain Name with .onion in the rightmost label of the Domain Name, 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 using a procedure specified in Section 3.2.2.4 of the Baseline Requirements ~~except that a CA MAY NOT verify a domain using the procedure described subsection 3.2.2.4(7)~~. For a Certificate issued to a Domain Name with .onion in the right-most label of the Domain Name, the CA SHALL confirm ~~that~~, as of the date the Certificate was issued, the Applicant's control over the .onion Domain Name in accordance with Appendix F.

(2) **Mixed Character Set Domain Names:** EV Certificates MAY include Domain Names containing mixed character sets only in compliance with the rules set forth by the domain registrar. The CA MUST visually compare any Domain Names with mixed character sets with known high risk domains. If a similarity is found, then the EV Certificate Request MUST be flagged as High Risk. The CA must perform reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that the Applicant and the target in question are the same organization.