DRAFT REVISIONS – BR 3.2.2.4 DOMAIN VALIDATION (Sept. 1, 2015)

Summary of changes

The primary purpose of this change is to replace Domain Validation item 7 "Using any other method of confirmation which has at least the same level of assurance as those methods previously described" with a specific list of the approved domain validation methods (including new methods proposed by Members). This ballot also tightens up and clarifies the existing Domain Validation methods 1 through 6. This revised BR 3.2.2.4 describes the methods that CAs may use to confirm domain ownership or control. Other validation methods can be added in the future.

The Validation Working Group believes the domain validation rules should follow the current BR 3.2.2.4 structure as much as possible so the changes are easy to understand, be worded as simply and clearly as possible so as to be easily implemented by CAs worldwide, and should avoid unnecessary complications or additional requirements that don't address with a realistic security threat. If a Forum Member wants to add any new requirements to these validation methods should be added, the Validation Working Group would prefer that the new requirements be proposed and discussed by separate ballot.

Proposed Effective date: 6 months from ballot approval

	CURRENT BRs	PROPOSED REVISION	COMMENTS
A	**3.2.2.4. Authorization by Domain Name Registrant**	**3.2.2.4. Validation of Domain Ownership or Control**	New title clarifies these are approved methods for domain validation methods
B	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:	This section defines the permitted processes and procedures for validating domain ownership or control. The CA SHALL confirm that the Fully-Qualified Domain Name (FQDN) has been validated by at least one of the methods below for each FQDN listed in a Certificate. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.	Clarifies the purposes of this BR section, and continues the long-standing ability to confirm domain ownership by accepting registration to Applicant's parent, subsidiary, or affiliate (all defined terms).
C	1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar;	1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar. This method may only be used if the CA has authenticated the	No change to first sentence. This is the traditional method of confirming domain ownership over the past 15+ years. The second sentence is new,

		Applicant's identity and the authority of the Applicant Representative under BR 3.2.2.1 or and 3.2.5 or under EV Guidelines Section 11.2 and 11.5 or the CA is also the Domain Name Registrar and directly confirms that the Applicant controls the registration for the Base Domain Name; or	and is meant to ensure that if a CA is validating a domain ownership through a WhoIs lookup that relies on the Registrant name, the CA should first validate the Applicant organization's identity and the authority of the Applicant Representative (so that matching the WhoIs Registrant name to the validated Organization will be appropriate). This will likely only be used for OV and EV certificates, as DV authentication usually occurs through other methods, such as email confirmation under Methods 2 or 3. We have also explicitly added a new validation method applicable to CAs who are also the Registrar for the domain being validated. It used to be generally covered by Method 1 and/or old Method 7, but is separately stated now.
D	2. Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar;	2. Confirming the Applicant's domain ownership or control by communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar using a Random Value and receiving a confirming response. A Random Value is not required for confirmation by telephone; or	No change, except the addition of "Confirming the Applicant's domain ownership or control by ***" at the beginning of the sentence. This uses contact information for the Registrant shown in WhoIs (mailing address, etc.) The Registrant may be the Applicant, or may have authorized the domain for the Applicant to use. We also require the CA to include a Random Value and receive a confirming response back from the Applicant (except for telephone confirmation).

E	3. Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field;	3. Confirming the Applicant's domain ownership or control by communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field using a Random Value and receiving a confirming response. A Random Value is not required for confirmation by telephone; or	No change, except the addition of "Confirming the Applicant's domain ownership or control by ***" at the beginning of the sentence. We also require the CA to include a Random Value and receive a confirming response back from the Applicant (except for telephone confirmation).
F	4. Communicating with the Domain's administrator using 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;	4. Confirming the Applicant's domain ownership or control by sending an email to 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, including a Random Value and receiving a confirming response; or	No substantive change, except the addition of "Confirming the Applicant's domain ownership or control by ***" at the beginning of the sentence. This incorporates the new defined term "Authorization Domain" and so allows the CA to prune components from the left side of the FQDN when sending the confirmation emails. We also require the CA to include a shared secret and receive an appropriate response back from the Applicant. Because this is a human-human interaction, a shared secret is more appropriate that requiring a Random Value with specified bits of entropy.
G	5. Relying upon a Domain Authorization Document;	5. Confirming the Applicant's domain ownership or control by relying upon a Domain Authorization Document. 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	Almost no change from current method, except the addition of "Confirming the Applicant's domain ownership or control by ***" at the beginning of the sentence. All the words after the first sentence are already in BR 3.2.2.4 as a Note at the end of the BR, but because the Note

		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 materially modified since the previous certificate's issuance; or	only deals with Method #5 it has been moved to this section. We added the word "materially" to the last sentence ("and that the Domain Name's WHOIS record has not been materially modified since the previous certificate's issuance.") to indicate that minor changes (e.g., "Street" for "St.") would not prevent use of this revalidation method.
H	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; or	6. Having the Applicant demonstrate control over the requested FQDN by installing a Random Value (contained in the name of the file, the content of a file, on a web page in the form of a meta tag, or any other format as determined by the CA) under "/.well-known/validation" directory on an Authorized Domain Name that can be validated over an Authorized Port; or	This tightens where the practical demonstration can be placed on an Applicant's website by adding the well-known directory requirement and limiting ports that can be used, and also requires that a Random Value be used (new defined term). We also changed the challenge from being just the FQDN to the challenge being an Authorization Domain Name (which allows the CA more locations which are presumably under control of the Applicant) **Open question** – we are having a hard time coming up with a list of Authorized Ports. If we can't agree on which ports are authorized, we should delete references to Authorized Ports.
I	7. Using any other 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	[Omitted]	Old method 7 "any other method" will no longer be used.

	FQDN to at least the same level of assurance as those methods previously described.		
J		7. Having the Applicant demonstrate control over the requested FQDN by the Applicant making a change to information in a DNS record for an Authorization Domain Name where the change is to insert a Random Value or Request Token; or	New Method. **Open question:** At the F2F someone suggested prepending a known string to the front of the random value for DNS text records. The Validation Working Group did not think such a requirement was necessary for this method, but is open to further discussion by Forum members.
K		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 Authorization Domain Name in accordance with section 3.2.2.5; or	New method. Refers to the current methods for validating an IP address at BR 3.2.2.5
L		9. Having the Applicant demonstrate 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 over an Authorized Port.	New method, relies on a Test Certificate (new definition) that can't be used by the Applicant. Similar to new method 7. **Open question** – we are having a hard time coming up with a list of Authorized Ports. If we can't agree on which ports are authorized, we should delete references to Authorized Ports.
M	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	[Omitted]	This has been incorporated into the defined term Authorization Domain Name and Base Domain, and so is no longer needed.

	whatever is allowed for registration according to the rules of that ccTLD.		
N	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.	[Omitted]	This language was moved to new Method 4, and so is no longer necessary here.
	BR 1.6.1 - DEFINITIONS	**BR 1.6.1 - DEFINITIONS**	
O	**Applicant:** The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.	[No change] **Applicant:** The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.	No change
P		**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	This new definition is used in Methods #4 and #7.

		of domain validation. If the FQDN starts with a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.	
Q		**Authorized Port:** One of the following ports: 80 (http), 443 (http), 115 (sftp), 25 (smtp), 22 (ssh).	This definition is used in new Methods 6 and 9. **Open Question**: It's not clear if this is a correct list, or if any list should be specified as customers seem to want to use lots of different ports. This needs further discussion and research. If we can't come up with a limited list of Authorized Ports, we should eliminate the term.
R		**Base Domain Name**: 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. "example.co.uk" or "example.com"). For gTLDs, the domain www.[gTLD] will be considered to be a Base Domain.	This is a new definition, and partly replaces the old Note at line N. **Open Question:** The last sentence was in response to a comment on the list, but another comment said it isn't needed, as things like www.com is an SLDN. For discussion.
S	**Domain Authorization Document**: 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	[No change] **Domain Authorization Document**: 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	No change

	of an Applicant to request a Certificate for a specific Domain Namespace.	of an Applicant to request a Certificate for a specific Domain Namespace.	
T	**Domain Name:** The label assigned to a node in the Domain Name System.	[No change] **Domain Authorization Document**: **Domain Name:** The label assigned to a node in the Domain Name System.	No change
U	**Domain Namespace:** The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.	[No change] **Domain Namespace:** The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.	No change
V	**Domain Name Registrant:** Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.	[No change] **Domain Name Registrant:** Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.	No change
W	**Domain Name Registrar:** A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).	[No change] **Domain Name Registrar:** A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).	No change
X	**Fully-Qualified Domain Name:** A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.	[No change] **Fully-Qualified Domain Name:** A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.	No change

Y		**Random Value**: (1) For domain validation methods that are totally automated or involve making a change specified by the CA to the Applicant's DNS record, a value specified by a CA to the Applicant that exhibits at least 112 bits of entropy; (2) for all other domain validation methods, a value specified by the CA that is unknown to the Applicant.	This definition is used in Methods 2-4 and 6-7.
Z	**Reliable Method of Communication:** A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.		
AA		**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.	This definition is used in new Method 7
BB		**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.	This definition is used in new Method 9.