BR 3.2.2.4 DOMAIN VALIDATION (April 20, 2016)

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.

Effective date: All CAs, and Delegated Third Parties, shall use only the methods in this ballot effective 6 months from ballot approval.

Amendments:

	CURRENT BRs	REVISED TEXT
A	**3.2.2.4. Authorization by Domain Name Registrant**	**3.2.2.4. Validation of Domain Authorization or Control**

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 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. 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.
C	1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar;	**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: (a) 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 (b) 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 (c) The CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name and directly confirms that the Applicant is the Domain Contact.

D	2. Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar;	**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.
E	3. Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field;	This has been included in item 2 above
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;	**3.2.2.4.**4. **Constructed Email to Domain Contact** Confirm 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.

G	5. Relying upon a Domain Authorization Document;	**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; or
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	**3.2.2.4.6. Agreed-Upon Change to Website** Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value or Request Token (contained in the content of a file or on a web page in the form of a meta tag) 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 can be validated over an Authorized Port. 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) .
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 FQDN to at least the same level of assurance as those methods previously described.	[Deleted]

J		**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).
K		**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.
L		**3.2.2.4.9**. **Test Certificate** Confirming the Applicant's control over the requested FQDN by confirming the presence on the Authorization Domain Name of a non-expired Test Certificate issue by the CA 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 which is accessible by the CA via TLS over an Authorized Port.

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 whatever is allowed for registration according to the rules of that ccTLD.	[Deleted]
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.	[Deleted]
	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.	**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.

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 of domain validation. If the FQDN contains 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).
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.
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 of an Applicant to request a Certificate for a specific Domain Namespace.	**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 of an Applicant to request a Certificate for a specific Domain Namespace.
		Domain Contact: The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.
T	**Domain Name:** The label assigned to a node in the Domain Name System.	**Domain Name:** The label assigned to a node in the Domain Name System.
U	**Domain Namespace:** The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.	**Domain Namespace:** The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

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.	**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.
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).	**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).
X	**Fully-Qualified Domain Name:** A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.	**Fully-Qualified Domain Name:** A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
Y		**Random Value**: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

Z		**Request Token**: A value derived in a method specified by the CA which binds this demonstration of control to the certificate request. The Request Token SHALL incorporate the key used in the certificate request. A Request Token MAY include a timestamp to indicate when it was created. A Request Token MAY include other information to ensure its uniqueness. A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation. A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future. A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation. The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.
Ω		**Test Certificate**: Test Certificate: A Certificate with a maximum validity period of 30 days and which i) includes a critical extension with the specified Test Certificate CABF OID, or ii) which chains to a root certificate not subject to these Requirements.

Add a footnote to Section 3.2.2.4:

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]

iii) a hash of a PKCS#10 CSR

Any of the above Request Tokens 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.

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.