DRAFT REVISIONS – BR 3.2.2.4 DOMAIN VALIDATION (Feb. 15, 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.

Proposed Effective date: Pre-ballot methods are forbidden 6 months from ballot approval. Revised methods are allowed immediately upon ballot approval.

	CURRENT BRs	PROPOSED REVISION
A	**3.2.2.4. Authorization by Domain Name Registrant**	**3.2.2.4. Validation of Domain Ownership 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 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.

C	1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar;	1. Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Name Registrant directly with the Domain Name Registrar or Registry. This method may only be used if: (a) The CA authenticates: (1) 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 Applicant's identity under EV Guidelines Section 11.2 and the agency of the Certificate Approver under EV Guidelines Section 11.8; or (b) The CA is also the Domain Name Registrar or Registry, or Affiliate of the Registrar or Registry, and directly confirms that the Applicant is the Domain Name Registrant; or

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 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 by either the Domain Name Registry or Domain Name Registrar as the contact information for the Domain Name registrant, Domain Name technical contact, or Domain Name administrative contact. Such identification MAY be made by consulting WHOIS information provided by the Domain Name Registry or Domain Name Registrar. Each email, fax, SMS, or postal mail MAY confirm control of multiple FQDNs. Each email, fax, SMS, or postal mail SHALL be sent to one or more recipients provided that every recipient SHALL be identified by the Domain Registrar as representing the Registrant for every Domain Name within whose Domain Namespace every FQDN falls. The Random Value SHALL be unique in each email, fax, SMS, or postal mail, however the email, fax, SMS, or postal mail MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation; or 3. Confirming the Applicant's control over the requested FQDN by calling the Domain Name Registrant's phone number. The call must be placed to a phone number identified by either the Domain Name Registry or Domain Name Registrar as the contact information for the Domain Name registrant, Domain Name technical contact, or Domain Name administrative contact. Such identification MAY be made by consulting WHOIS information provided by the Domain Name Registry or Domain Name Registrar. 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 Registry or Registrar as a valid contact method for every Domain Name within whose Domain Namespace every FQDN falls.

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;	4. Confirming the Applicant's control over the requested FQDN by sending an email to an address created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, including a Random Value and receiving a confirming response utilizing the Random Value. Each email MAY confirm control of multiple FQDNs. Each email SHALL be sent to one or more recipients provided that every recipient SHALL be identified as an administrator for each Domain Name within whose Domain Namespace every FQDN falls. The Random Value SHALL be unique in each email, however 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; or
G	5. Relying upon a Domain Authorization Document;	5. 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 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 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	6. Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value or Request Token (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/pki-validation" directory on the Authorization Domain Name that can be validated over an Authorized Port. Either: a) a Random Value SHALL be used in this demonstration of control which SHALL be unique to the Certificate Request and SHALL remain valid for no longer than 30 days, or b) where the Applicant submits certificate requests directly to the CA, a Random Value SHALL be used in this demonstration of control which SHALL be unique to the Applicant and which SHALL remain valid for no longer than the maximum time specified in section 3.3.1, or c) where the Applicant submits certificate requests other than directly to the CA, e.g. when the Applicant is communicating with the CA through an intermediary party not audited to be in compliance with these guidelines such as a reseller or a web-host, a Request Token SHALL be used in this demonstration of control ; or
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.	[Omitted]
J		7. 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. Either: a) a Random Value SHALL be used in this demonstration of control which SHALL be unique to the Certificate Request and SHALL remain valid for no longer than 30 days, or b) where the Applicant submits certificate requests directly to the CA, a Random Value SHALL be used in this demonstration of control which SHALL be unique to the Applicant and which SHALL remain valid for no longer than the maximum time specified in section 3.3.1, or c) where the Applicant submits certificate requests other than directly to the CA, e.g. when the Applicant is communicating with the CA through

		an intermediary party not audited to be in compliance with these guidelines such as a reseller or a web-host, a Request Token SHALL be used in this demonstration of control [time limited? Whether a Request Token should be required to carry a time stamp?]. ; or
K		8. 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; or
L		9. Confirming the Applicant's control over the requested FQDN by confirming the presence on the FQDN of a Test Certificate (using the same public key) issued by the CA for the purposes of this method and which is accessible by the CA via TLS over an Authorized Port. [Whether a test certificate should have a specific time limit?]
	Placeholder for new methods which we think well be added, such as those defined in the IETF ACME RFC.	- Using TLS to deliver/provide a Random Value - Using a Random Value in a Test Certificate (where the Test Certificate was not issued by the CA) - Using DNS where the TXT record for a FQDN is located at: <a standard string>.FQDN
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.	[Omitted]
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	[Omitted]

	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.	
	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.
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 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).
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.	[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 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 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.	[No change] **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.	[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.
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).
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.
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 derivation of the Request Token SHALL incorporate the key used in the certificate request. 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.

		E.g.: A Request Token could be: i) a SHA-256 hash of the public key; ii) a SHA-256 hash of a CSR, provided that the CSR itself is signed with SHA-2 (or better); iii) a SHA-384 hash over a concatenation of the Subject Public Key Info and the FQDN being validated; or iv) a SHA-256 hash over a concatenation of the Subject Public Key Info and a sorted list of all of the FQDNs being validated for this certificate request. ~~Where a Request Token also includes a date stamp the CA must receive proof of possession of the private key from the applicant within 48 hours.~~
Ω		**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. [Tighter definition needed – critical extension always? Based on pre-certificate definition?] The Applicant must prove possession of the private key corresponding to the public key in the Test Certificate.

	CURRENT BRs	PROPOSED REVISION
A	**3.2.2.4. Authorization by Domain Name Registrant**	**3.2.2.4. Validation of Domain Ownership 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 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.

C	1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar;	1. Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Name Registrant directly with the Domain Name Registrar or Registry. This method may only be used if: (a) The CA authenticates: (1) 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 Applicant's identity under EV Guidelines Section 11.2 and the agency of the Certificate Approver under EV Guidelines Section 11.8; or (b) The CA is also the Domain Name Registrar or Registry, or Affiliate of the Registrar or Registry, and directly confirms that the Applicant is the Domain Name Registrant; or

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 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 by either the Domain Name Registry or Domain Name Registrar as the contact information for the Domain Name registrant, Domain Name technical contact, or Domain Name administrative contact. Such identification MAY be made by consulting WHOIS information provided by the Domain Name Registry or Domain Name Registrar. Each email, fax, SMS, or postal mail MAY confirm control of multiple FQDNs. Each email, fax, SMS, or postal mail SHALL be sent to one or more recipients provided that every recipient SHALL be identified by the Domain Registrar as representing the Registrant for every Domain Name within whose Domain Namespace every FQDN falls. The Random Value SHALL be unique in each email, fax, SMS, or postal mail, however the email, fax, SMS, or postal mail MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation; or 3. Confirming the Applicant's control over the requested FQDN by calling the Domain Name Registrant's phone number. The call must be placed to a phone number identified by either the Domain Name Registry or Domain Name Registrar as the contact information for the Domain Name registrant, Domain Name technical contact, or Domain Name administrative contact. Such identification MAY be made by consulting WHOIS information provided by the Domain Name Registry or Domain Name Registrar. 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 Registry or Registrar as a valid contact method for every Domain Name within whose Domain Namespace every FQDN falls.

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;	4. Confirming the Applicant's control over the requested FQDN by sending an email to an address created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, including a Random Value and receiving a confirming response utilizing the Random Value. Each email MAY confirm control of multiple FQDNs. Each email SHALL be sent to one or more recipients provided that every recipient SHALL be identified as an administrator for each Domain Name within whose Domain Namespace every FQDN falls. The Random Value SHALL be unique in each email, however 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; or
G	5. Relying upon a Domain Authorization Document;	5. 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 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 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	6. Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value or Request Token (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/pki-validation" directory on the Authorization Domain Name that can be validated over an Authorized Port. Either: a) a Random Value SHALL be used in this demonstration of control which SHALL be unique to the Certificate Request and SHALL remain valid for no longer than 30 days, or b) where the Applicant submits certificate requests directly to the CA, a Random Value SHALL be used in this demonstration of control which SHALL be unique to the Applicant and which SHALL remain valid for no longer than the maximum time specified in section 3.3.1, or c) where the Applicant submits certificate requests other than directly to the CA, e.g. when the Applicant is communicating with the CA through an intermediary party not audited to be in compliance with these guidelines such as a reseller or a web-host, a Request Token SHALL be used in this demonstration of control ; or
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.	[Omitted]
J		7. 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. Either: a) a Random Value SHALL be used in this demonstration of control which SHALL be unique to the Certificate Request and SHALL remain valid for no longer than 30 days, or b) where the Applicant submits certificate requests directly to the CA, a Random Value SHALL be used in this demonstration of control which SHALL be unique to the Applicant and which SHALL remain valid for no longer than the maximum time specified in section 3.3.1, or c) where the Applicant submits certificate requests other than directly to the CA, e.g. when the Applicant is communicating with the CA through

		an intermediary party not audited to be in compliance with these guidelines such as a reseller or a web-host, a Request Token SHALL be used in this demonstration of control [time limited? Whether a Request Token should be required to carry a time stamp?]. ; or
K		8. 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; or
L		9. Confirming the Applicant's control over the requested FQDN by confirming the presence on the FQDN of a Test Certificate (using the same public key) issued by the CA for the purposes of this method and which is accessible by the CA via TLS over an Authorized Port. [Whether a test certificate should have a specific time limit?]
	Placeholder for new methods which we think well be added, such as those defined in the IETF ACME RFC.	- Using TLS to deliver/provide a Random Value - Using a Random Value in a Test Certificate (where the Test Certificate was not issued by the CA) - Using DNS where the TXT record for a FQDN is located at: <a standard string>.FQDN
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.	[Omitted]
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	[Omitted]

	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.	
	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.
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 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).
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.	[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 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 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.	[No change] **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.	[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.
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).
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.
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 derivation of the Request Token SHALL incorporate the key used in the certificate request. 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.

		E.g.: A Request Token could be: i) a SHA-256 hash of the public key; ii) a SHA-256 hash of a CSR, provided that the CSR itself is signed with SHA-2 (or better); iii) a SHA-384 hash over a concatenation of the Subject Public Key Info and the FQDN being validated; or iv) a SHA-256 hash over a concatenation of the Subject Public Key Info and a sorted list of all of the FQDNs being validated for this certificate request. ~~Where a Request Token also includes a date stamp the CA must receive proof of possession of the private key from the applicant within 48 hours.~~
Ω		**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. [Tighter definition needed – critical extension always? Based on pre-certificate definition?] The Applicant must prove possession of the private key corresponding to the public key in the Test Certificate.

	CURRENT BRs	PROPOSED REVISION
A	**3.2.2.4. Authorization by Domain Name Registrant**	**3.2.2.4. Validation of Domain Ownership 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 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.

C	1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar;	1. Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Name Registrant directly with the Domain Name Registrar or Registry. This method may only be used if: (a) The CA authenticates: (1) 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 Applicant's identity under EV Guidelines Section 11.2 and the agency of the Certificate Approver under EV Guidelines Section 11.8; or (b) The CA is also the Domain Name Registrar or Registry, or Affiliate of the Registrar or Registry, and directly confirms that the Applicant is the Domain Name Registrant; or

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 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 by either the Domain Name Registry or Domain Name Registrar as the contact information for the Domain Name registrant, Domain Name technical contact, or Domain Name administrative contact. Such identification MAY be made by consulting WHOIS information provided by the Domain Name Registry or Domain Name Registrar. Each email, fax, SMS, or postal mail MAY confirm control of multiple FQDNs. Each email, fax, SMS, or postal mail SHALL be sent to one or more recipients provided that every recipient SHALL be identified by the Domain Registrar as representing the Registrant for every Domain Name within whose Domain Namespace every FQDN falls. The Random Value SHALL be unique in each email, fax, SMS, or postal mail, however the email, fax, SMS, or postal mail MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation; or 3. Confirming the Applicant's control over the requested FQDN by calling the Domain Name Registrant's phone number. The call must be placed to a phone number identified by either the Domain Name Registry or Domain Name Registrar as the contact information for the Domain Name registrant, Domain Name technical contact, or Domain Name administrative contact. Such identification MAY be made by consulting WHOIS information provided by the Domain Name Registry or Domain Name Registrar. 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 Registry or Registrar as a valid contact method for every Domain Name within whose Domain Namespace every FQDN falls.

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;	4. Confirming the Applicant's control over the requested FQDN by sending an email to an address created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, including a Random Value and receiving a confirming response utilizing the Random Value. Each email MAY confirm control of multiple FQDNs. Each email SHALL be sent to one or more recipients provided that every recipient SHALL be identified as an administrator for each Domain Name within whose Domain Namespace every FQDN falls. The Random Value SHALL be unique in each email, however 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; or
G	5. Relying upon a Domain Authorization Document;	5. 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 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 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	6. Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value or Request Token (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/pki-validation" directory on the Authorization Domain Name that can be validated over an Authorized Port. Either: a) a Random Value SHALL be used in this demonstration of control which SHALL be unique to the Certificate Request and SHALL remain valid for no longer than 30 days, or b) where the Applicant submits certificate requests directly to the CA, a Random Value SHALL be used in this demonstration of control which SHALL be unique to the Applicant and which SHALL remain valid for no longer than the maximum time specified in section 3.3.1, or c) where the Applicant submits certificate requests other than directly to the CA, e.g. when the Applicant is communicating with the CA through an intermediary party not audited to be in compliance with these guidelines such as a reseller or a web-host, a Request Token SHALL be used in this demonstration of control ; or
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.	[Omitted]
J		7. 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. Either: a) a Random Value SHALL be used in this demonstration of control which SHALL be unique to the Certificate Request and SHALL remain valid for no longer than 30 days, or b) where the Applicant submits certificate requests directly to the CA, a Random Value SHALL be used in this demonstration of control which SHALL be unique to the Applicant and which SHALL remain valid for no longer than the maximum time specified in section 3.3.1, or c) where the Applicant submits certificate requests other than directly to the CA, e.g. when the Applicant is communicating with the CA through

		an intermediary party not audited to be in compliance with these guidelines such as a reseller or a web-host, a Request Token SHALL be used in this demonstration of control [time limited? Whether a Request Token should be required to carry a time stamp?]. ; or
K		8. 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; or
L		9. Confirming the Applicant's control over the requested FQDN by confirming the presence on the FQDN of a Test Certificate (using the same public key) issued by the CA for the purposes of this method and which is accessible by the CA via TLS over an Authorized Port. [Whether a test certificate should have a specific time limit?]
	Placeholder for new methods which we think well be added, such as those defined in the IETF ACME RFC.	- Using TLS to deliver/provide a Random Value - Using a Random Value in a Test Certificate (where the Test Certificate was not issued by the CA) - Using DNS where the TXT record for a FQDN is located at: <a standard string>.FQDN
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.	[Omitted]
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	[Omitted]

	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.	
	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.
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 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).
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.	[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 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 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.	[No change] **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.	[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.
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).
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.
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 derivation of the Request Token SHALL incorporate the key used in the certificate request. 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.

		E.g.: A Request Token could be: i) a SHA-256 hash of the public key; ii) a SHA-256 hash of a CSR, provided that the CSR itself is signed with SHA-2 (or better); iii) a SHA-384 hash over a concatenation of the Subject Public Key Info and the FQDN being validated; or iv) a SHA-256 hash over a concatenation of the Subject Public Key Info and a sorted list of all of the FQDNs being validated for this certificate request. ~~Where a Request Token also includes a date stamp the CA must receive proof of possession of the private key from the applicant within 48 hours.~~
Ω		**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. [Tighter definition needed – critical extension always? Based on pre-certificate definition?] The Applicant must prove possession of the private key corresponding to the public key in the Test Certificate.