**Ballot 190 – Revised Validation Requirements (with comments)**

**Purpose of Ballot:** The purpose of this ballot is to 1) re-introduce the validation methods removed in ballots 180-181 because of IPR concerns, 2) clarify some aspects of the revised validation methods, and 3) clarify the general rule in BR 4.2.1 on the reuse of information and validations when changes are made to validation methods.

The following motion has been proposed by Kirk Hall of Entrust Datacard and endorsed by the following CA/B Forum member representatives: Doug Beattie of GlobalSign and Mads of Henricksveen of Buypass to introduce new Final Maintenance Guidelines for the "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates" (Baseline Requirements).

**--Motion Begins—**

1) In BR Sec. 1.6.1, add new definitions and revise existing definitions as shown:

**Authorized Ports:** One of the following ports: 80 (http), 443 (http), ~~115 (sftp),~~ 25 (smtp), 22 (ssh).

**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 (2.23.140.2.1), or (ii) ~~which chains to a root certificate not subject to these Requirements~~ is issued under a CA where there are no Certificate paths/chains to a root Certificate subject to these Requirements.

**Wildcard Domain Name:** A Domain Name consisting of a single asterisk character followed by a single full stop character ("*.") followed by a Fully-Qualified Domain Name.

2) BR 3.2.2.4 is amended to read as follows:

**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.

Completed ~~confirmations~~ validations of Applicant authority may be ~~valid~~ used for the issuance of multiple ~~certificate~~Certificates over time. In all cases, the ~~confirmation~~ validation must have been initiated within the time period specified in the relevant requirement (such as Section ~~3.3.1~~4.2.1 of this document) prior to ~~certificate~~Certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

CAs SHALL maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.

**Commented [KH1]:** New requirement not in Ballot 169 – added per Jeremy's request.

**Commented [KH2]:** This new definitions was suggested by Peter, to replace the prior definition from Doug and Gerv.

**Commented [KH3]:** I replaced "certificate" with "Certificate" in various places to be consistent.

**Commented [KH4]:** I changed "confirmations" to "validations" and "valid" to "used" here, as that seems to make more sense. Also corrected the reference to old 3.3.1 to new 4.2.1

**Commented [KH5]:** Per Gerv's request

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 ~~[Reserved]~~ 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.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for FQDNs for higher level domain levels that end in the validated FQDN. This method is suitable for validating Wildcard Domain Names.

**3.2.2.4.2 ~~[Reserved]~~ 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.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for FQDNs for higher level domain levels that end in the validated FQDN. This method is suitable for validating Wildcard Domain Names.

**3.2.2.4.3 ~~[Reserved]~~Phone Contact with Domain Contact**

**Commented [KH6]:** The seven validation methods added in below were taken from Ballot 169, except as otherwise noted.

**Commented [KH7]:** A variation of this sentence is added to each method to clarify that validation of an FQDN allows certs for higher level domains that end in the validated FQDN. Also, per Gerv's suggestion we indicate whether or not the validation method is suitable for Wildcard Certificates (Not for Method 8).

Confirming the Applicant's control over the 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.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for FQDNs for higher level domain levels that end in the validated FQDN. This method is suitable for validating Wildcard Domain Names.

**Commented [KH8]:** The word "requested" in front of FQDN was deleted – it is not used in Methods 1 or 2, and adds nothing useful.

**3.2.2.4.4 ~~[Reserved]~~Constructed Email to Domain Contact**

Confirm the Applicant's control over the 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.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for FQDNs for higher level domain levels that end in the validated FQDN. This method is suitable for validating Wildcard Domain Names.

**Commented [KH9]:** The word "requested" in front of FQDN was deleted – it is not used in Methods 1 or 2, and adds nothing useful.

**Commented [KH10]:** BR 3.2.2.4 was changed to eliminate the stub at the very end of this sentence, which previously said "***in which case the CA" - that made no sense.

**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.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for FQDNs for higher level domain levels that end in the validated FQDN. This method is suitable for validating Wildcard Domain Names.

**Commented [KH11]:** The word "requested" in front of FQDN was deleted – it is not used in Methods 1 or 2, and adds nothing useful.

**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~~Certificate request and SHALL not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the ~~certificate~~Certificate request, the timeframe permitted for reuse of validated information relevant to the ~~certificate~~Certificate (such as in Section ~~3.3.1~~4.2.1 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~~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.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for FQDNs for higher level domain levels that end in the validated FQDN. This method is suitable for validating Wildcard Domain Names.

**3.2.2.4.7 ~~[Reserved]~~ DNS Change**

Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token in a DNS CNAME, 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).

**Commented [KH12]:** The word "requested" in front of FQDN was deleted – it is not used in Methods 1 or 2, and adds nothing useful.

**Commented [KH13]:** This also corrects the reference to old BR 3.3.1 to current BR 4.2.1.

**Commented [KH14]:** This is Method 6 as approved in Ballot 169. Did someone have another correction to make?

**Commented [KH15]:** The word "requested" in front of FQDN was deleted – it is not used in Methods 1 or 2, and adds nothing useful.

**Commented [KH16]:** The word CNAME was added per Jeremy's request – was not in Ballot 169

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for FQDNs for higher level domain levels that end in the validated FQDN. This method is suitable for validating Wildcard Domain Names.

**3.2.2.4.8 ~~[Reserved]~~ IP Address**

Confirming the Applicant's control over the 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.

Note: Once the FQDN has been validated using this method, the CA MAY NOT also issue Certificates for FQDNs for higher level domain levels that end in the validated FQDN unless the CA performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

**3.2.2.4.9 ~~[Reserved]~~ Test Certificate**

Confirming the Applicant's control over the 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.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for FQDNs for higher level domain levels that end in the validated FQDN. This method is suitable for validating Wildcard Domain Names.

**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.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for FQDNs for higher level domain levels that end in the validated FQDN. This method is suitable for validating Wildcard Domain Names.

~~**3.2.2.4.11 Other Methods**~~

~~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 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).~~

3) BR Section 4.2.1 is amended as follows:

**4.2.1. Performing Identification and Authentication Functions**

The ~~certificate~~Certificate request MAY include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for the CA to obtain

**Commented [KH17]:** The word "requested" in front of FQDN was deleted – it is not used in Methods 1 or 2, and adds nothing useful.

**Commented [KH18]:** The word "requested" in front of FQDN was deleted – it is not used in Methods 1 or 2, and adds nothing useful.

**Commented [KH19]:** The word "requested" in front of FQDN was deleted – it is not used in Methods 1 or 2, and adds nothing useful.

**Commented [KH20]:** We are finally removing "any other method"

from the Applicant in order to comply with these Requirements and the CA's Certificate Policy and/or Certification Practice Statement. In cases where the ~~certificate~~Certificate request does not contain all the necessary information about the Applicant, the CA SHALL obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. The CA SHALL establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant. Applicant information MUST include, but not be limited to, at least one Fully-Qualified Domain Name or IP address to be included in the Certificate's SubjectAltName extension.

Section 6.3.2 limits the validity period of Subscriber Certificates. The CA MAY use the documents and data provided in Section 3.2 to verify ~~certificate~~Certificate information, or may reuse previous validations themselves, provided that:

(1) Prior to March 1, 2018, the CA obtained the data or document from a source specified under Section 3.2 or completed the validation itself no more than 39 months prior to issuing the Certificate; and

(2) On or after March 1, 2018, the CA obtained the data or document from a source specified under Section 3.2 or completed the validation itself no more than 825 days prior to issuing the Certificate.

In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.

After the change to any validation method specified in the Baseline Requirements or EV Guidelines, a CA may continue to reuse validation data or documents collected prior to the change, or the validation itself, for the period stated in this BR 4.2.1 unless otherwise specifically provided in a ballot.

The CA SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements.

If a Delegated Third Party fulfills any of the CA's obligations under this section , the CA SHALL verify that the process used by the Delegated Third Party to identify and further verify High Risk Certificate Requests provides at least the same level of assurance as the CA's own processes.

4) The proposer and endorsers of this Ballot may withdraw this Ballot at any time prior to completion of the final vote for approval, in which case the Ballot will not proceed further.

**--Motion Ends--**

The procedure for approval of this Final Maintenance Guideline ballot is as follows (exact start and end times may be adjusted to comply with applicable Bylaws and IPR Agreement):

| BALLOT 190<br>Status: Final Maintenance Guideline | Start time<br>(23:00 UTC) | End time<br>(23:00 UTC) |
|---|---|---|

**Commented [KH21]:** Some have argued there is a difference between reusing validation data or documents, and reusing the validation itself (e.g., an organization validation relies on multiple documents and data collected). We have never believed that is true, so this is intended to clarify that point.

**Commented [KH22]:** This clarifies that if a prior validation is based on any data or document that is beyond the permitted reuse period, the prior validation may not be reused any longer.

**Commented [KH23]:** This was added to eliminate any uncertainty about the effect of changes to validation methods on any existing validation data. In order for changes to validations methods to result in a revalidation requirement (overriding BR 4.2.1), that must be specifically stated in the validation method change ballot. I removed the paragraph that had previously been suggested for BR 3.2.2.4 that referred solely to Ballot 190 (and said it did not require revalidations) – better to go with a general rule, and then in the future if we modify a method and want prior validations redone, we can state that specifically in the future ballot for the specific sections that are affected.

| | | |
|---|---|---|
| Discussion (7 to 14 days) | June 25, 2017 | July 2, 2017 |
| Vote for approval (7 days) | July 2, 2017 | July 9, 2017 |
| If vote approves ballot: Review Period (Chair to send Review Notice) (30 days).<br>If Exclusion Notice(s) filed, ballot approval is rescinded and PAG to be created.<br>If no Exclusion Notices filed, ballot becomes effective at end of Review Period. | Upon filing of Review Notice by Chair | 30 days after filing of Review Notice by Chair |

From Bylaw 2.3: If the Draft Guideline Ballot is proposing a Final Maintenance Guideline, such ballot will include a redline or comparison showing the set of changes from the Final Guideline section(s) intended to become a Final Maintenance Guideline, and need not include a copy of the full set of guidelines. Such redline or comparison shall be made against the Final Guideline section(s) as they exist at the time a ballot is proposed, and need not take into consideration other ballots that may be proposed subsequently, except as provided in Bylaw Section 2.3(j).

Votes must be cast by posting an on-list reply to this thread on the Public list. A vote in favor of the motion must indicate a clear 'yes' in the response. A vote against must indicate a clear 'no' in the response. A vote to abstain must indicate a clear 'abstain' in the response. Unclear responses will not be counted. The latest vote received from any representative of a voting member before the close of the voting period will be counted. Voting members are listed here: https://cabforum.org/members/

In order for the motion to be adopted, two thirds or more of the votes cast by members in the CA category and greater than 50% of the votes cast by members in the browser category must be in favor. Quorum is shown on CA/Browser Forum wiki. Under Bylaw 2.2(g), at least the required quorum number must participate in the ballot for the ballot to be valid, either by voting in favor, voting against, or abstaining.