Revised Validation Requirements

Purpose of Ballot: The purpose of this ballot is to 1) re-introduce the methods removed in ballot 180-182 because of IPR concerns, 2) clarify some issues with the .well-known method, 3) specify how the reuse of information works with respect to the newly adopted methods, and 4) clarify how the reuse of information works with respect to the amendment to BR 4.2.1.

The following motion has been proposed by Jeremy Rowley of DigiCert and endorsed by the following CA/B Forum member representatives: Entrust Datacard and YYYY 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--

Ballot Section 1

1) Replace Section 3.2.2.4.1:

3.2.2.4.1 Validating the Applicant as a Domain Contact

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

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

2) Replace Section 3.2.2.4.2:

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) Replace Section 3.2.2.4.3:

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.

4) Replace Section 3.2.2.4.4:

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.

5) Edit Section 3.2.2.4.6:

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 Request Token or Random Value contained in the content of a file or on a web page in the form of a meta tag ~~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. The Request Token or Random Value MUST NOT appear in the request for the file or web-page. ÷

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

~~2. The presence of the Request Token or Request Value contained in the content of a file or on a webpage in the form of a meta tag where the Request Token or Random Value MUST NOT appear in the request.~~

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

Note: Examples of Request Tokens include, but are not limited to: (i) a hash of the public key; (ii) a hash of the Subject Public Key Info [X.509]; and (iii) a hash of a PKCS#10 CSR. A Request Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests. This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR. E.g. echo `date -u +%Y%m%d%H%M` `sha256sum <r2.csr` | sed "s/[-]//g". The script outputs:201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f

The CA should define in its CPS (or in a document referenced from the CPS) the format of Request Tokens it accepts.

6) Add Section 3.2.2.4.7:

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 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).

7) Add Section 3.2.2.4.8:

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.

8) Add Section 3.2.2.4.9:

3.2.2.4.9 Test Certificate

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

9) Delete Section 3.2.2.4.11

10) Delete the definition of "Required Website Content"

11) Replace the reference to Section 3.3.1 with a reference to Section 4.2.1 in the third paragraph under Section 3.2.2.4.

12) Revised the definition of "Authorized Ports" as follows:

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

13) Revise the definition of Test Certificate as follows:

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) is issued under a CA where there are no certificate paths/chains to a root certificate subject to these Requirements

Ballot Section 2

This provisions of Ballot Section 1 will apply only to the validation of domain names occurring after this Ballot 190's effective date. Validation of domain names that occurs before this Ballot's effective date and the resulting validation data may continue to be used for the periods specified in BR 4.2.1 and EVGL 11.14.3 so long as the validations were conducted in compliance with the BR Section 3.2.2.4 validation methods in effect at the time of each validation.

--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 Status: Final Maintenance Guideline	Start time (23:00 UTC)	End time (23:00 UTC)
Discussion (7 to 14 days)		
Vote for approval (7 days)		
If vote approves ballot: Review Period (Chair to send Review Notice) (30 days). If Exclusion Notice(s) filed, ballot approval is rescinded and PAG to be created.	Upon filing of Review Notice by Chair	30 days after filing of Review Notice by Chair

If no Exclusion Notices filed, ballot becomes effective at end of Review Period.		

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.