**--Motion Begins--**

1) Add the following new definitions:

**Sub-Domain**: In relation to a particular FQDN, a Sub-Domain is the FQDN plus at least one additional prepended label. In the case of Wildcard Domains (a type of Sub-Domain), the leftmost prepended label will be a “\*”. All Sub-Domains are subject to the same Maximum Domain Validation Reuse Period as the FQDN to which they relate.

**Maximum Domain Validation Reuse Period**: 825 days starting from when an Initial Confirmation Process is complete.

**Initial Confirmation Process**: The process described in part a of each subsection under Section 3.2.2.4.

2) Revised the definition of “Authorized Ports” as follows:

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

3) 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

4) Replace Section 3.2.2.4 with:

This section specifies the permitted process that a CA may use to validate an Applicant's ownership or control of the domain, the time-limits for re-using a validation for subsequent certificates, whether the process can be used for Certificates with Wildcard Domains, and whether the validation can be reused to issue Certificates for Sub-Domains of validated FQDNs. The CA MUST confirm that, as of the date the Certificate issues, the CA validated each Fully‐Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below within the permitted time-frame. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate. The CA MUST record the subsection and version of the Baseline Requirements used to validate an Applicant’s control over each FQDN included in an issued certificate.

A CA MAY reuse validation of an FQDN under methods 1-6 as listed in Section 4.3.3.2 of Version 1.3.5 of the Baseline Requirements or Section 4.3.3.2 of Version 1.3.9 of the Baseline Requirements to issue new certificates if: 1) the CA obtained the validation data prior to April 1, 2017, 2) a Delegated Third Party did perform the validation required by the Baseline Requirements, and 3) 825 days have not passed since the VCA obtained the validation data.

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.

5) Replace Section 3.2.2.4.1:

**3.2.2.4.1 Validating the Applicant as a Domain Contact**

**a) Initial Confirmation Process:**

Prior to issuing a certificate that includes a FQDN validated under this method, the CA MUST confirm the Applicant's control over the FQDN by confirming that directly with the Domain Name Registrar that the Applicant is the Domain Contact. 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.

**b) Reuse Period:**

The CA MAY rely on its previous confirmation of the Applicant’s FQDN under this method to issue additional certificates for the FQDN if (1) the Maximum Domain Validation Reuse Period has not elapsed and (2) the CA confirms, within the Maximum Domain Validation Reuse Period, that the WHOIS information for the Base Domain has not changed since the CA performed the verification process.

**c) Sub-Domains**

The CA MAY rely on its confirmation of control over the FQDN under this method to issue certificates for Sub-Domains of the FQDN if reuse of the confirmation of control over the FQDN to issue Sub-Domains is expressly approved by the Applicant.

6) Replace Section 3.2.2.4.2:

**3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact**

**a) Initial Confirmation Process:**

Prior to issuing a certificate that includes a FQDN validated under this section, the CA MUST confirm the Applicant's control over the FQDN by:

1. Creating a Random Value,
2. Sending a Random Value via email, fax, SMS, or postal mail to a Domain Contact, and
3. Within 30 days of creating the Random Value, receiving a confirming response that utilizes the Random Value.

The CA MAY specify a shorter period for receiving a confirming response that utilizes the Random Values in its CPS, in which case the CA MUST receive a confirming response utilizing the Random Value within the time frame specified by the CPS.

The CA MAY use a single email, fax, SMS, or postal mail to confirm the Applicant’s control over multiple FQDNs and multiple Authorization Domain Names if all FQNs and Authorization Domain Names in the email have the same Domain Contact. The CA MAY send the email, fax, SMS, or postal mail identified under this method to more than one recipient if every recipient is listed as a Domain Contact for all FQDNs and Authorization Domain Names validated using the communication.

The CA MAY resend an email, fax, SMS, or postal mail that reuses the previously sent Random Value if the communication's entire contents (including the Random Value) and recipient(s) are not changed. In all other cases, CA MUST use a unique Random Value in each email, fax, SMS, or postal mail.

**b) Reuse Period:**

The CA MAY rely on its previous confirmation of the Applicant’s FQDN under this method to issue additional certificates for the FQDN if (1) the Maximum Domain Validation Reuse Period has not elapsed and (2) the CA confirms, within the Maximum Domain Validation Reuse Period, that the WHOIS information for the Base Domain has not changed since the CA performed the verification process.

**c) Sub-Domains**

The CA MAY rely on its confirmation of control over the FQDN under this method to issue certificates for Sub-Domains of the FQDN if reuse of confirmation of control over the FQDN to issue Sub-Domains is expressly approved by the Applicant.

7) Replace Section 3.2.2.4.3:

**3.2.2.4.3 Phone Contact with Domain Contact**

**a) Initial Confirmation Process:**

Prior to issuing a certificate that includes an FQDN validated under this method, the CA MUST confirm the Applicant's control over the requested FQDN by

1. Obtaining a Domain Contact’s phone number from WHOIS or the Domain Name Registrar,
2. Calling the obtained phone number. and
3. Receiving a response during the phone call that confirms the Applicant's request for validation of the FQDN.

The CA MUST make each phone call to a single number. The CA MAY use a single phone call to confirm control of multiple FQDNs if the phone number is identified by WHOIS or the Domain Registrar as the Domain Contact for each FQDN.

**b) Reuse Period:**

The CA MAY rely on its previous confirmation of the Applicant’s FQDN under this method to issue additional certificates for the FQDN if (1) the Maximum Domain Validation Reuse Period has not elapsed and (2) the CA confirms, within the Maximum Domain Validation Reuse Period that the WHOIS information for the Base Domain has not changed since the CA performed the verification process.

**c) Sub-Domains**

The CA MAY rely on its confirmation of control over the FQDN under this method to issue certificates for Sub-Domains of the FQDN if reuse of the confirmation of control over the FQDN to issue Sub-Domains is expressly approved by the Applicant.

8) Replace Section 3.2.2.4.4:

**3.2.2.4.4 Constructed Email to Domain Contact**

**a) Initial Confirmation Process:**

Prior to issuing a certificate that includes a FQDN validated under this method, the CA MUST confirm the Applicant's control over the requested FQDN by

1. Creating a Random Value,
2. Sending an email that includes the created Random Value 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, and
3. Within 30 days of creating the Random Value, receiving a confirming response that utilizes the Random Value.

The CA MAY specify a shorter period for receiving a confirming response that utilizes the Random Values in its CPS, in which case the CA MUST receive a confirming response utilizing the Random Value within the time frame specified by the CPS.

The CA MAY use a single email to confirm the Applicant’s control over multiple FQDNs and multiple Authorization Domain Names if the Authorization Domain Name used to create the email address is an Authorization Domain Name for all FQDNs and Authorization Domain Names included in the email.

The CA MAY resend an email that reuses the previously sent Random Value if the email’s entire contents (including the Random Value) and recipient(s) are not changed. In all other cases, CA MUST use a unique Random Value in each email.

**b) Reuse Period:**

The CA MAY rely on its previous confirmation of the Applicant’s FQDN under this method to issue additional certificates for the FQDN if the Maximum Domain Validation Reuse Period has not elapsed.

**c) Sub-Domains**

The CA MAY rely on its confirmation of control over the FQDN under this method to issue certificates for Sub-Domains of the FQDN if reuse of the confirmation of control over the FQDN to issue Sub-Domains is expressly approved by the Applicant.

9) Replace Section 3.2.2.4.5

**3.2.2.4.5 Domain Authorization Document**

**a) Initial Confirmation Process:**

Prior to issuing a certificate that includes a FQDN validated under this method, the CA MUST confirm the Applicant's control over the requested FQDN by:

1. Obtaining a Domain Authorization Document that attests to the authority of the Applicant to request a Certificate that includes the FQDN,
2. Verifying that the Domain Authorization Document came from the Domain Contact, and
3. Verifying 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 the Domain Contact provided a previous Domain Authorization Document for FQDN.

**b) Reuse Period:**

The CA MAY rely on its previous confirmation of the Applicant’s FQDN under this method to issue additional certificates for the FQDN if the Maximum Domain Validation Reuse Period has not elapsed.

**c) Sub-Domains**

The CA MAY rely on its confirmation of control over the FQDN under this method to issue certificates for Sub-Domains of the FQDN if reuse of the confirmation of control over the FQDN to issue Sub-Domains is expressly approved by the Applicant.

10) Replace Section 3.2.2.4.6:

**3.2.2.4.6 Agreed-Upon Change to Website**

**a) Initial Confirmation Process:**

Prior to issuing a certificate that includes a FQDN validated under this method, the CA MUST confirm 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 under the "/.well‐known/pki‐validation" directory, or another path registered with IANA for the purpose of Domain Validation, on the Authorization Domain Name. The CA MUST access the content of the file or web page via HTTP or HTTPS over an Authorized Port. The Request Token or Random Value MUST NOT appear in the request for the file or web-page.

If the CA uses a Random Value is used, the CA MUST provide a Random Value unique to the certificate request. The CA MAY NOT confirm the Applicant’s control over the requested FQDN if the Random Value was generated more than 30 days prior to completing the confirmation under this confirmation process.

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.

**b) Reuse Period:**

The CA MAY rely on its previous confirmation of the Applicant’s FQDN under this method to issue additional certificates for the FQDN if the Maximum Domain Validation Reuse Period has not elapsed.

**c) Sub-Domains**

The CA MAY rely on its confirmation of control over the FQDN under this method to issue certificates for Sub-Domains of the FQDN if reuse of the confirmation of control over the FQDN to issue Sub-Domains is expressly approved by the Applicant.

10) Add Section 3.2.2.4.7:

**3.2.2.4.7 DNS Change**

**a) Initial Confirmation Process**

Prior to issuing a certificate that includes a FQDN validated under this method, the CA MUST confirm 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 the CA uses a Random Value is used, the CA MUST provide a Random Value unique to the certificate request. The CA MAY NOT confirm the Applicant’s control over the requested FQDN if the Random Value was generated more than 30 days prior to completing this confirmation process.

**b) Reuse Period:**

The CA MAY rely on its previous confirmation of the Applicant’s FQDN under this method to issue additional certificates for the FQDN if the Maximum Domain Validation Reuse Period has not elapsed.

**c) Sub-Domains**

The CA MAY rely on its confirmation of control over the FQDN under this method to issue certificates for Sub-Domains of the FQDN.

11) Add Section 3.2.2.4.8:

**3.2.2.4.8 IP Address**

**a) Confirmation Process:**

Prior to issuing a certificate that includes an FQDN validated under this method, the CA MUST confirm 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.

**b) Reuse Period:**

The CA MUST NOT rely on its previous confirmation of the Applicant’s FQDN under this method to issue additional certificates.

**c) Sub-Domains**

The CA MUST NOT rely on its confirmation of control over the FQDN under this method to issue certificates for Sub-Domains of the FQDN.

12) Add Section 3.2.2.4.9:

**3.2.2.4.9 Test Certificate**

Prior to issuing a certificate that includes a FQDN validated under this method, the CA MUST confirm the Applicant's control over the requested FQDN by:

1. Issuing a Test Certificate to the Applicant for an Authorization Domain Name,
2. Accessing the Authorization Domain Name via TLS over an Authorized Port, and
3. Confirming the issued Test Certificate is used on the Authorization Domain Name.

If the CA uses this method to validate Applicant’s control over a requested FQDN, the CA MUST only issue certificates to the FQDN using the same Public Key as specified in the Test Certificate.

**b) Reuse Period:**

The CA MAY rely on its previous confirmation of the Applicant’s FQDN under this method to issue additional certificates for the FQDN if the Maximum Domain Validation Reuse Period has not elapsed.

**c) Sub-Domains**

The CA MAY rely on its confirmation of control over the FQDN under this method to issue certificates for Sub-Domains of the FQDN if reuse of the confirmation of control over the FQDN to issue Sub-Domains is expressly approved by the Applicant.

13) Replace Section 3.2.2.4.10:

**3.2.2.4.10 TLS Using a Random Number**

Prior to issuing a certificate that includes a FQDN validated under this method, the CA MUST confirm the Applicant's control over the requested FQDN by:

1. Generating a Random Value
2. Accessing an Authorization Domain Name via TLS over an Authorized Port,
3. Confirming the Random Value is included in a Certificate present on the accessed Authorization Domain Name.

**b) Reuse Period:**

The CA MAY rely on its previous confirmation of the Applicant’s FQDN under this method to issue additional certificates for the FQDN if the Maximum Domain Validation Reuse Period has not elapsed.

**c) Sub-Domains**

The CA MAY rely on its confirmation of control over the FQDN under this method to issue certificates for Sub-Domains of the FQDN if reuse of the confirmation of control over the FQDN to issue Sub-Domains is expressly approved by the Applicant.

14) Amend Section 3.2.2.4.11 to:

**3.2.2.4.11 [Reserved]**

15) Delete the definition of “Required Website Content”

16) 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.

**--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.  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.