Ballot 181 – Readopting BR 3.2.2.4 (Part 1)

The following motion has been proposed by Kirk Hall of Entrust and endorsed by Peter Bowen of Amazon and Virginia Fournier of Apple as a Final Guideline:

-- MOTION BEGINS –

In accordance with the Bylaws and Intellectual Property Rights (IPR) Policy of the CA/Browser Forum (the "Forum"), the Forum Baseline Requirements (BR) and Extended Validation Guidelines (EVGL), as previously approved by all ballots up to and including Ballot 176, are hereby readopted by this Ballot, with the following amendments.

1. BR 3.2.2.4 is amended to read in its entirety 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 of Applicant authority may be valid for the issuance of multiple certificates over time. In all cases, the confirmation must have been initiated within the time period specified in the relevant requirement (such as Section 3.3.1 of this document) prior to certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.
>
> 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]**
>
> **3.2.2.4.2 [Reserved]**
>
> **3.2.2.4.3 [Reserved]**
>
> **3.2.2.4.4 [Reserved]**
>
> **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.

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 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.

3.2.2.4.7 [Reserved]

3.2.2.4.8 [Reserved]

3.2.2.4.9 [Reserved]

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.

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).

In the event that this Ballot and Ballot 180 are both approved by the Forum, the provisions of this Ballot shall supersede and replace any conflicting provisions of Ballot 180.

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

BALLOT 181 Status: Final Guideline	Start time (22:00 UTC)	End time (22:00 UTC)
Discussion (7 days)	Oct. 25, 2016	Nov. 1, 2016
Review Period (Chair to send Review Notice) (60 days). If Exclusion Notice(s) filed, PAG to be created and no further action until PAG recommendations received. If no Exclusion Notice(s) filed, proceed to:	Nov. 1, 2016	Dec. 31, 2016
Vote for approval (7 days)	Dec. 31, 2016	Jan. 7, 2017

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 currently ten (10) members – at least ten members must participate in the ballot, either by voting in favor, voting against, or abstaining.