Ballot 197 – Effective Date of Ballot 193 Provisions

Recent Ballot 193 reduced the maximum period for certificates and for reuse of vetting data for DV and OV certificates from 39 months to 825 days. The effective date for reducing the maximum validity period of certificates was specified as March 1, 2018, but no effective date was specified for when the reduction of the maximum period for reuse of vetting data becomes effective.

It was the intention of the authors of Ballot 193 that the effective date for reducing the maximum period for reuse of vetting data under BR 4.2.1 would also be March 1, 2018. This ballot is intended to clarify that intention. The ballot also makes these changes retroactive to the effective date of Ballot 193 so there is no gap period.

Ballot 193 is in the Review Period (which will end on April 22, 2017), and has not yet taken effect. Bylaw 2.3 states that Ballots should include a "redline or comparison showing the set of changes from the Final Guideline section(s) intended to become a Final Maintenance Guideline" and that "[s]uch redline or comparison shall be made against the Final Guideline section(s) as they exist at the time a ballot is proposed".

To avoid confusion, this Ballot will show the proposed changes to BR 4.2.1 will be presented two ways: (1) a comparison of the changes to BR 4.2.1 as it existed before Ballot 193 (which is as BR 4.2.1 exists at this time this ballot is proposed), and also (2) a comparison of the changes to BR 4.2.1 as it will exist after the Review Period for Ballot 193 is completed (assuming no Exclusion Notices are filed).

The following motion has been proposed by Chris Bailey of Entrust Datacard and endorsed by Ben Wilson of DigiCert, and Wayne Thayer of GoDaddy to introduce new Final Maintenance Guidelines for the "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates" (Baseline Requirements) and the "Guidelines for the Issuance and Management of Extended Validation Certificates" (EV Guidelines).

-- MOTION BEGINS --

Ballot Section 1

BR 4.2.1 is amended to read as follows:

[Ballot amendments shown against BR 4.2.1 as it currently exists without the changes adopted in Ballot 193]

BR 4.2.1. Performing Identification and Authentication Functions

The 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 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 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 information, provided that: ~~the CA obtained the data or document from a source specified under Section 3.2 no more than thirty-nine (39) months prior to issuing the Certificate.~~

> **(1) Prior to March 1, 2018, the CA obtained the data or document from a source specified under Section 3.2 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 no more than 825 days prior to issuing the Certificate.**

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.

[Ballot amendments shown against BR 4.2.1 <u>as it existed after Ballot 193 was approved</u>]

BR 4.2.1. Performing Identification and Authentication Functions

The 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 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 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 information, provided that: ~~the CA obtained the data or document from a source specified under Section 3.2 no more than 825 days prior to issuing the Certificate.~~

> **(1) Prior to March 1, 2018, the CA obtained the data or document from a source specified under Section 3.2 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 no more than 825 days prior to issuing the Certificate.

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.

Ballot Section 2

The provisions of Ballot Section 1 will be effective retroactive to the effective date of Ballot 193.

--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 197 Status: Final Maintenance Guideline	Start time (22:00 UTC)	End time (22:00 UTC)
Discussion (7 to 14 days)	April 19, 2017	April 26, 2017
Vote for approval (7 days)	April 26, 2017	May 3, 2017
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.