Ballot 193 - 825-day Certificate Lifetimes

Purpose of Ballot: Recent Ballot 185 demonstrated a consensus among Forum members to reduce the maximum lifetime for DV and OV certificates from 39 months to 825 days (roughly 27 months). This ballot reflects that consensus, and also reduces the maximum period for reuse of vetting data for DV and OV certificates from 39 months to 27 months, and makes other clarifying changes including moving certain provisions from the EV Guidelines to the Baseline Requirements.

The following motion has been proposed by Chris Bailey of Entrust Datacard and endorsed by the following CA/B Forum member representatives (listed in alphabetical order) Robin Alden of Comodo, Ben Wilson of DigiCert, and Doug Beattie of GlobalSign 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 --

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 **(i)** the CA obtained the data or document from a source specified under Section 3.2 no more than **825 days** ~~*thirty-nine (39) months*~~ prior to issuing the Certificate**; and (ii) the method used to obtain the document or data was acceptable under Section 3.2 at the time the document or data was obtained**.

A CA may rely on a previously verified certificate request to issue a replacement certificate, so long as the certificate being referenced was not revoked due to fraud or other illegal conduct, if:
(1) The expiration date of the replacement certificate is the same as the expiration date of the Certificate that is being replaced, and
(2) The Subject Information of the Certificate is the same as the Subject in the Certificate that is being replaced.

If an Applicant has a currently valid Certificate issued by the CA, a CA MAY rely on its prior authentication and verification of the Applicant's right to use the specified Domain Name under Section 3.2.2.4, provided that the CA verifies that the WHOIS record still shows the same registrant as when the CA verified the specified Domain Name for the existing 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.

BR 6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Subscriber Certificates issued after **March 1, 2018** ~~*the Effective Date*~~ MUST have a Validity Period no greater than **825 days** ~~*60 months*~~. **Subscriber Certificates issued after 1 April 2015 but prior to 1 March 2018 MUST NOT have a Validity Period greater than thirty-nine (39) months.**

~~*Except as provided for below, Subscriber Certificates issued after 1 April 2015 MUST have a Validity Period no greater than 39 months.*~~

~~*Until 30 June 2016, CAs MAY continue to issue Subscriber Certificates with a Validity Period greater than 39 months but not greater than 60 months provided that the CA documents that the Certificate is for a system or software that:*~~

~~*(a) was in use prior to the Effective Date;*~~
~~*(b) is currently in use by either the Applicant or a substantial number of Relying Parties;*~~
~~*(c) fails to operate if the Validity Period is shorter than 60 months;*~~
~~*(d) does not contain known security risks to Relying Parties; and*~~
~~*(e) is difficult to patch or replace without substantial economic outlay.*~~

EVGL 9.4. Maximum Validity Period For EV Certificate
The validity period for an EV Certificate SHALL NOT exceed **825 days** ~~*twenty seven months*~~. It is RECOMMENDED that EV Subscriber Certificates have a maximum validity period of twelve months.

EVGL 11.14.2. Re-issuance Requests
As specified in Section 4.2.1 of the Baseline Requirements. ~~*A CA may rely on a previously verified certificate request to issue a replacement certificate, so long as the certificate being referenced was not revoked due to fraud or other illegal conduct, if:*~~
~~*(1) The expiration date of the replacement certificate is the same as the expiration date of the EV Certificate that is being replaced, and*~~
~~*(2) The Subject Information of the Certificate is the same as the Subject in the EV Certificate that is being replaced.*~~

11.14.3. Age of Validated Data
(1) Except for reissuance of an EV Certificate under Section 11.14.2 and except when permitted otherwise in Section 11.14.1, the age of all data used to support issuance of an EV Certificate (before revalidation is required) SHALL NOT exceed the following limits:
(A) Legal existence and identity – thirteen months;
(B) Assumed name – thirteen months;
(C) Address of Place of Business – thirteen months;

(D) Verified Method of Communication – thirteen months;
(E) Operational existence – thirteen months;
(F) Domain Name – thirteen months;
(G) Name, Title, Agency, and Authority – thirteen months, unless a contract between the CA and the Applicant specifies a different term, in which case, the term specified in such contract controls. For example, the contract MAY include the perpetual assignment of EV roles until revoked by the Applicant or CA, or until the contract expires or is terminated.

(2) The thirteen-month period set forth above SHALL begin to run on the date the information was collected by the CA.

(3) The CA MAY reuse a previously submitted EV Certificate Request, Subscriber Agreement, or Terms of Use, including use of a single EV Certificate Request in support of multiple EV Certificates containing the same Subject to the extent permitted under Sections 11.9 and 11.10.

(4) The CA MUST repeat the verification process required in these Guidelines for any information obtained outside the time limits specified above except when permitted otherwise under section 11.14.1.

(5) The CA MUST ensure that any documents or data used to support the issuance of an EV Certificate complies with the requirements set forth in Section 4.2.1 of the Baseline Requirements.

-- 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 193 Status: Final Maintenance Guideline	Start time (23:00 UTC)	End time (23:00 UTC)
Discussion (7 to 14 days)	March 1	March 8
Vote for approval (7 days)	March 8	March 15
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.