***Ballot NNN – SHA-1 deprecation ballot***

***9.4 Validity Period***

**9.4.1 Subscriber Certificates**

Subscriber Certificates issued after the Effective Date MUST have a Validity Period no greater than 60 months.

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

Effective 1 April 2015, 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.

**9.4.2 SHA-1 Validity Period**

Effective 1 January 2016, CAs MUST NOT issue any new Subscriber certificates or Subordinate CA certificates using the SHA-1 hash algorithm. CAs MAY continue to sign certificates to verify OCSP responses using SHA1 until 1 January 2017. This Section 9.4.2 does not apply to Root CA or CA cross certificates.  CAs MAY continue to use their existing SHA-1 Root Certificates. SHA-2 Subscriber certificates SHOULD NOT chain up to a SHA-1 Subordinate CA Certificate.

Effective 10 November 2014, CAs SHOULD NOT issue Subscriber Certificates utilizing the SHA-1 algorithm with an Expiry Date greater than 1 January 2017 because Application Software Providers are in the process of deprecating and/or removing the SHA-1 algorithm from their software, and they have communicated that CAs and Subscribers using such certificates do so at their own risk.

…

**Appendix A - Cryptographic Algorithm and Key Requirements (Normative)**

…

Add this note under Table 2, Subordinate CA certificates:

\* SHA-1 MAY be used with RSA keys in accordance with the criteria defined in Section 9.4.2.

And amend this note at the end of the 3 tables.

\* SHA-1 MAY be used with RSA keys in accordance with the criteria defined in Section 9.4.2  ~~until SHA-256 is supported widely by browsers used by a substantialportion of relying-parties worldwide~~.