Ballot SC38 - Alignment of Record Archival

Background

Ballot SC28 attempted to clarify the relationship between audit logging obligations under the Network and Certification System Security Requirements and Baseline Requirements and reduce the retention period for log data, when appropriate. During the drafting and analysis of ballot SC28, the relationship between sections 5.4 and 5.5 was not fully considered. The difference between audit logs and archived records can differ based on each CAś interpretation, but overlap considerably. Some CAś equate audit logs and archived records in these sections of their CP(s) and CPS(s).

After the updated language included in SC28 Sections 5.4.3 and 5.5.2 could be in conflict. Section 5.5.2 requires all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof be retained for seven years after certificates cease to to be valid. Section 5.4.3 requires all audit logs of Subscriber Certificate lifecycle management event records be maintained for two years after the revocation or expiration of the Subscriber Certificate. These sections intersect at the retention requirements for audit logs and archived records, as they relate to subscriber certificate lifecycle events. The retention periods are in conflict as to the length of retention.

Purpose

The proposed changes seek to bring these two sections of the ¨Baseline Requirements” into agreement and avoid confusion and potential issues of noncompliance as they relate to retention periods.

Risk vs Benefits

The benefits of this ballot allows CAs to adjust log retention procedures to take advantage of the intended reduction in retention requirements of SC28, while avoiding any potential compliance issues. This ballot clarifies the intention and avoids any confusion in interpretation between the two sections.

There are no identified risks that were not already accepted with the passing of ballot SC28.

Proposal

The following ballot is proposed by Neil Dunbar of TrustCor Systems and endorsed by David Kluge of Google and Ben Wilson of Mozilla.

— MOTION BEGINS —

Delete the following Section 5.5.2 Retention period for archive from the “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”, which currently reads as follows:

> The CA SHALL retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid.

Insert, as Section 5.5.2. Retention period for archive of the “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”, the following:

> The CA SHALL retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least two years after any Certificate based on that documentation ceases to be valid.

— MOTION ENDS —

*** WARNING ***: USE AT YOUR OWN RISK. THE REDLINE BELOW IS NOT THE OFFICIAL VERSION OF THE CHANGES (CABF Bylaws, Section 2.4(a)):

A comparison of the changes can be found at:

https://github.com/cabforum/documents/compare/8f63128...neildunbar:180341b

Effective as of the date this Ballot becomes incorporated into a Final Guideline.

This ballot proposes one Final Maintenance Guideline.

The procedure for approval of this ballot is as follows:

Discussion (7+ days)

Start Time: <INSERT>

End Time: <INSERT>

Vote for approval (7 days)

Relevant provisions

From the BRs

5.5.2.AUDIT LOGGING PROCEDURES

> The CA SHALL retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid.