**Audit Period Defined**

Audit engagements are normally conducted in one of two ways, covering either a point in time or period of time. When an auditor conducts a point in time engagement, including a point in time readiness assessment (also known by CAs and Browsers as a PITRA), the testing procedures are concentrated on one particular day (the reporting date). These engagements focus on the condition of the PKI operation in a “snapshot” fashion. The auditor assesses and reports on the suitability of the design and the proper implementation of those controls necessary and/or required by the relevant audit schemes (i.e., ETSI or WebTrust) and the CA/Browser Forum on a particular day. In a point in time engagement, the auditor does not opine on the operating effectiveness of controls. Also, in a point in time engagement, the auditor is not opining on the suitability and implementation of controls for any period before or after the particular reporting date. In a point in time engagement, the audit period is restricted to one day,

In a period of time engagement, the auditor assesses and reports on the suitability of the design and the proper implementation and effective operations of those controls necessary and/or required by the relevant audit schemes (i.e., ETSI or WebTrust) and the CA/Browser Forum over a meaningful period of time. This is known as the reporting or audit period. Professional audit standards requires a minimum audit testing period of two months for reporting on PKI operations. Audit periods normally cannot exceed twelve months for WebTrust engagements.

An “Audit Period” should not be confused with the timing when audit procedures are conducted by the auditor, which is commonly referred to as audit fieldwork. An auditor is not typically onsite performing testing procedures throughout the entire audit period. In addition, an auditor will typically perform some testing of transactions that occurred during the audit period after the period is over. Whether the auditor is testing onsite, remotely, or in phases throughout the audit period, the entire audit period remains the scope of the audit requiring testing coverage throughout that period of time.

At present, it is common for a CA to undergo a point in time readiness assessment or audit for its initial audit. This point in time engagement serves as an anchor for the subsequent engagement that generally will be required by each of the Browsers to begin the application process to be included in their trusted root stores. Subsequent to the point in time engagement, the auditor performs a period of time engagement beginning with the later of

* the date of the point in time engagement if no significant remediation was required to address any deficiencies in disclosures and/or controls, or
* the date that any remediation was completed that addressed significant deficiencies in disclosures and/or controls that existed

for a minimum of two months. It is noteworthy Browsers require continuous audit coverage with no gaps in audit periods tested during each renewal audit period, regardless of the type of audit opinion issued (qualified or unqualified).