Audit Lifecycle

Of a Root Certificate

Problem Statement

The WebTrust and ETSI audit requirements for CA certificates throughout their lifecycle are not well defined, leading to confusion and failure to perform the right audits at the right times to comply with BR and root program requirements.

Root Events

- Preparation (facility, personnel, policies, auditors, etc.)
- Generate root key pair
- Generate root certificate
- First signing event (OCSP, CRL, Intermediate CA certificate)
- Sign intermediate CA certificate
- Issue end-entity certificate (will become a Publicly Trusted Certificate)
- Cross-signed by older publicly-trusted root
- Recognized by a browser
- Issue PTC (for testing)
- Issue PTC to a Subscriber
- Stop issuing PTCs
- Root expiration
- Removal from browser root store
- Key destruction

BR Requirements (partial)

Section 6.1 (for Roots and subordinate CA certificates not operated by the TSP):

- have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

Section 8.1 (when not technically constrained):

- The period during which the CA issues Certificates SHALL be divided into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration.
- If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 8.1, then no pre-issuance readiness assessment is necessary.
- If the CA does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in Section 8.1, then, before issuing Publicly-Trusted Certificates, the CA SHALL successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in Section 8.1. The point-in-time readiness assessment SHALL be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.

Relevant Mozilla Requirements

- Before being included, CAs MUST provide evidence that their CA certificates have continually, from the time of creation, complied with the then-current Mozilla Root Store Policy and Baseline Requirements.
- Full-surveillance period-of-time audits MUST be conducted and updated audit information provided no less frequently than **annually**. Successive audits MUST be contiguous (no gaps).
- Point-in-time audit statements may be used to confirm that all of the problems that an auditor previously identified in a qualified audit statement have been corrected. However, a point-in-time assessment does not replace the period-of-time assessment.
- MUST be audited in accordance with Mozilla’s Root Store Policy. If the CA has a currently valid audit report at the time of creation of the certificate, then the new certificate MUST appear on the CA's next periodic audit reports.

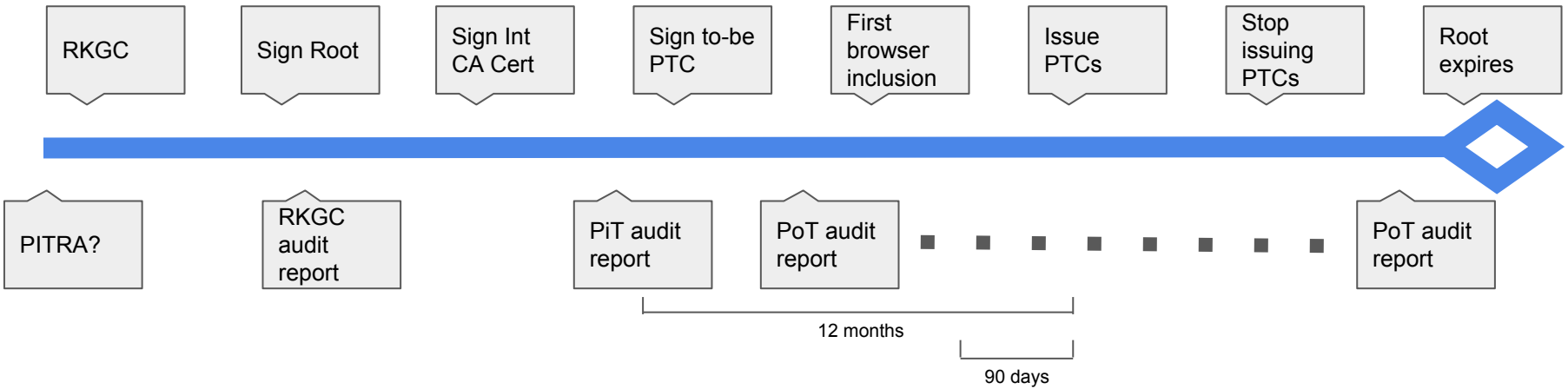
Relevant Microsoft Requirements

- Microsoft requires an audit prior to commencing commercial operations. For commercial CAs that have not been operational as an issuer of certificates for 90 days or more, Microsoft will accept a point-in-time readiness audit conducted by a Qualified Auditor. If the CA uses a point-in-time readiness audit, Microsoft requires a follow-up audit within 90 days after the CA issues its first certificate.
- A commercial CA already in our program applying for a new root to be included is exempt from the point-in-time and period-in-time audit requirement for the new roots. Rather, they should be up to date on audits for their existing roots in the program.
- For CAs that have not commenced commercial operations, Microsoft allows application to their program on a preliminary basis without a Point-in-Time audit. Once preliminary approval is granted, then the CA must adhere to the point-in-time/period-in-time standards aforementioned

Questions

- What is a “publicly-trusted certificate”, and is that important relative to audits?
  - If a cert (end-entity or intermediate CA) is issued prior to root inclusion, is it “publicly trusted”?
  - Does this apply to certificates issued for test websites?
- Does RKGC only cover keygen or also root signing?
  - Does ETSI have a report that covers root ket generation and signing?
- What if key generation and signing don’t happen at the same time? Are raw keys exempt from our policies?
- When must PoT audits begin to provide contiguous audit coverage?
- Do the BRs mean PiT audit when they say PITRA?
- What type of audit is required for periods when no certificates were issued?
- When can audits for legacy roots be discontinued?
- Are PiT audits required for new roots under existing TSP with current audits?
- Are EV audits required for an existing root prior to requesting EV status?

Simplified Timeline



RKGC - Root key generation ceremony
PTC - Publicly-trusted certificate
PiT - Point-in-time
PoT - Period-of-time
PITRA - Readiness assessment - no public audit statement

Scenarios

- Brand new TSP
  - RKGC + Root signing
  - PiT when?
  - First PoT when?
- Existing TSP
  - As long as new/acquired root is added to existing CPS, no PiT required
  - EV audit when?
- Brand new TSP acquires a root
  - PiT / PoT when?
- Brand new TSP acquires entire operation of existing TSP
  - Are any additional audits required?

Potential Policy Updates

- Replace PITRA with PiT Audit in all policies
- Require CAs to provide RKGC audit reports to root store operators
- Define exactly when a PiT audit is required
- Require first PoT audit within 90 days of PiT audit
- Require first PoT audit to cover the period back to first key generation
- Define PTC or remove the concept of “publicly trusted”