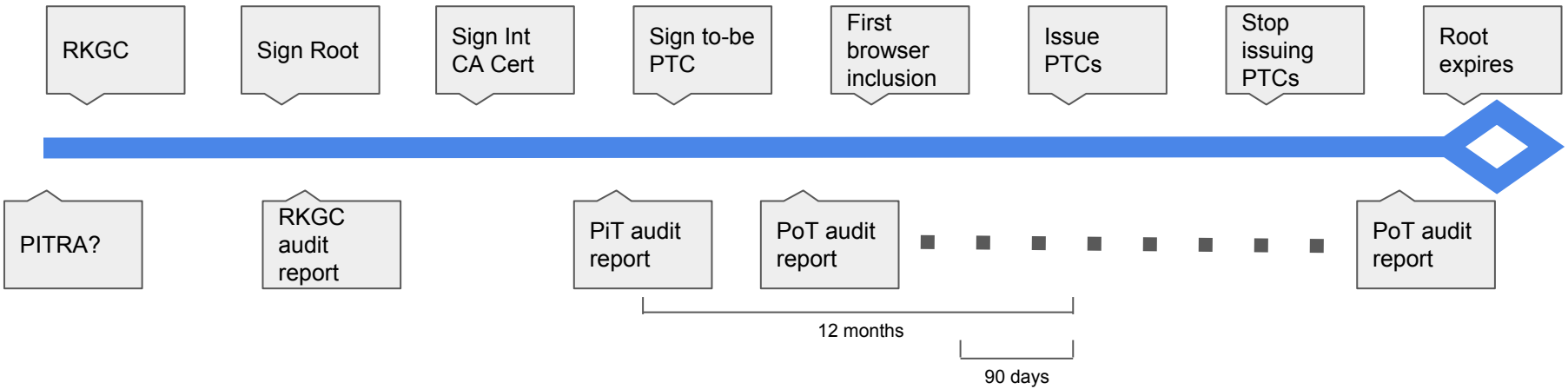
Audit Lifecycle

Proposed Guidelines Changes

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.

Simplified Timeline (Current State)



RKGC - Root key generation ceremony
PTC - Publicly-trusted certificate
PiT - Point-in-time (‘Type 1’ in SOC terms)
PoT - Period-of-time (‘Type 2’)
PITRA - Readiness assessment - no public audit statement

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.
- Intermediate CA Certificates 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.

Summary of Proposed Changes

- Require continuous period-of-time audits from the time the key pair is created until the root(s) expire
  - EV audits can still begin prior to issuing first EV certificate so long as no EV-capable certificates issued
  - PoT audits required even when there is no active issuance
- Resolve “test certificate” confusion by replacing “Publicly-Trusted Certificate”
- Clarify current requirements for audits of new roots created by existing CAs
- Replace “PITRA” terminology with PiT audit

Draft: https://docs.google.com/document/d/1OlayY56iKDeJMAl-ec3QDOKgE9vwt3yemEjlC_7gzv0/edit?usp=sharing

Change #1: Continuous Audits

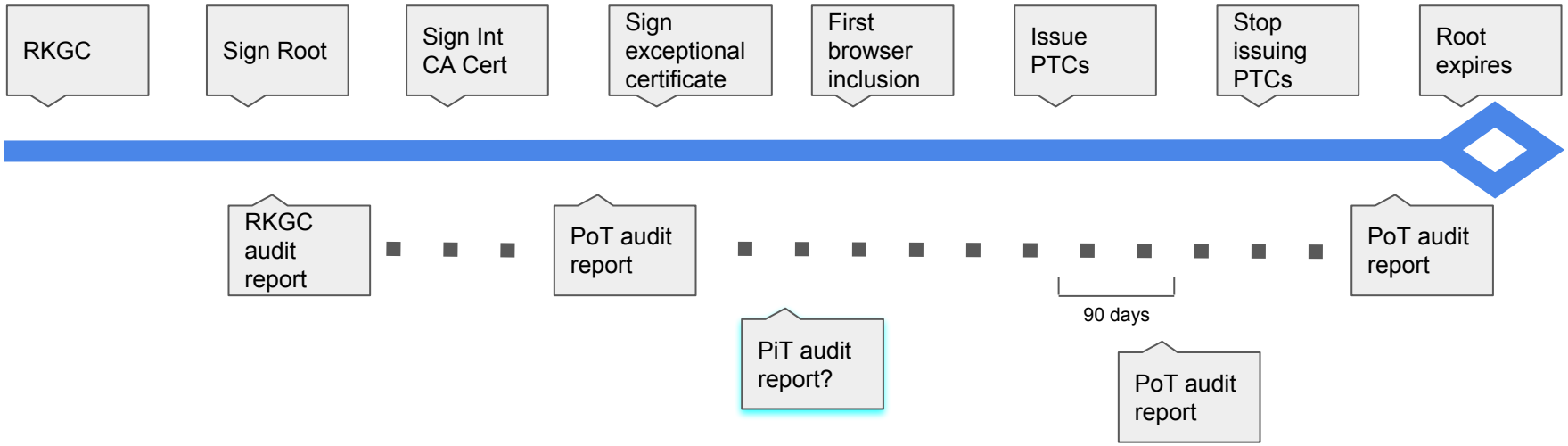
Require continuous BR audit coverage from key generation until revocation or expiration. Require PoT audits even when there is no active issuance. This provision will have a phase-in date to exempt current roots, but after that date CA certificates that have not been continuously audited cannot comply with the BRs.

> Root and Subordinate CA Key Pairs and Certificates~~The period during which the CA issues Certificate~~s generated after <date> SHALL be audited continuously from the date of Key Pair Generation until all certificates utilizing the Key Pair are revoked or expire. Each sequential~~divided into an unbroken sequence of audit periods. An~~ audit period MUST NOT exceed one year in duration. There MUST NOT be gaps in time between successive audit periods.

Continue to allow EV issuance after a PiT EV audit. EV audits only required from point before issuing first EV-capable cert.

> **17.2. Audit Period**
>
> CAs issuing EV Certificates MUST undergo an annual audit that meets the criteria of Section 17.1 and MUST~~.Root and Subordinate CA Certificates after <date>~~ be audited continuously from the date of issuing the first Certificate asserting an EV policy until the Root and Subordinate CA Certificates are revoked or expire.~~Each sequentialdivided into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration.¶~~

Simplified Timeline (Future State)



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

Change #2: Resolve Confusion over “Test” Certs

Remove the term “Publicly Trusted Certificate” from the audit requirements and replace with concept of exception for infrastructure and verification. This resolves confusion about certificates that will be publicly trusted in the future and about “test” certificates.

If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 8.4~~1~~, then Root and Subordinate CA Certificates must either:

1. Be managed under a CP/CPS listed in a currently valid Audit Report, and appear on the CA's audit reports beginning with the period during which the Root Key Generation Ceremony was conducted; or,
2. Before issuing certificates, except as permitted in section 8.1.1, complete an audit performed in accordance with applicable standards under one of the audit schemes listed in Section 8.4 and reporting on a period of at least 60 days~~no pre-issuance readiness assessment is necessary~~.

8.1.1 Issuance Exceptions for Infrastructure and Verification

The CA MAY issue certificates in the following circumstances:

- For the purposes described in section 6.1.7
- For valid, revoked, and expired test web pages as described in section 2.2

Change #3: Clarify requirements for existing CAs

Clarify audit requirements for newly created CA certificates controlled by a CA with an existing audit.

If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 8.~~4~~1, then Root and Subordinate CA Certificates must either:

1. Be managed under a CP/CPS listed in a currently valid Audit Report, and appear on the CA's audit reports beginning with the period during which the Root Key Generation Ceremony was conducted; or,
2. Before issuing certificates, except as permitted in section 8.1.1, complete an audit performed in accordance with applicable standards under one of the audit schemes listed in Section 8.4 and reporting on a period of at least 60 days~~no pre-issuance readiness assessment is necessary~~.

Change #4: Eliminate BR PITRA Language

Eliminate use of “Point-in-time Readiness Assessment” - this term is often confused with Point-in-Time audits, but has a different meaning. A PITRA does not result in a public audit statement. It’s a private engagement that identifies gaps in a CAs preparedness to undergo a PiT or PoT audit.

If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 8.4~~1~~, then Root and Subordinate CA Certificates must either:

1. Be managed under a CP/CPS listed in a currently valid Audit Report, and appear on the CA’s audit reports beginning with the period during which the Root Key Generation Ceremony was conducted; or,
2. Before issuing certificates, except as permitted in section 8.1.1, complete an audit performed in accordance with applicable standards under one of the audit schemes listed in Section 8.4 and reporting on a period of at least 60 days~~no pre-issuance readiness assessment is necessary~~.

Change #5: Eliminate 12-Month window for PiT

Retain the PiT audit prior to issuing Subscriber certificates, but allow it to happen prior to root inclusion submission, which may be far more than 12 months prior

If the CA does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in Section 8.41, then, before issuing certificates, except as permitted in section 8.1.1 ~~to Subscribers other than the CA itself~~Publicly-Trusted Certificates, the CA SHALL successfully complete a point-in-time auditreadiness ~~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.~~ Within 90 days of issuing the first certificate, except as permitted in section 8.1.1, the CA SHALL successfully complete an audit performed in accordance with applicable standards under one of the audit schemes listed in Section 8.4 and reporting on a period during which certificates were issued to Subscribers other than the CA itself.

Change #6: Update EV Audit Schemes

Remove ETSI TS 102 042 audit scheme

17. Audit

17.1. Eligible Audit Schemes

A CA issuing EV Certificates SHALL undergo an audit in accordance with one of the following schemes:
(i) WebTrust Program for CAs audit and WebTrust EV Program audit,
(ii) ~~ETSI TS 102 042 audit for EVCP, or~~¶
~~(iii)~~ ETSI EN 319 411-1 audit for EVCP policy.

Change #7: EV

Clarify audit requirements for new CAs

17.4. Pre-Issuance ~~Readiness~~ Audit

If the CA does not have a currently valid Audit Report indicating compliance with an audit scheme listed in Section 17.1, then:

(1) If the CA has a currently valid WebTrust Seal of Assurance for CAs, then, before issuing EV Certificates, except as permitted in BR section 8.1.1, the CA and its Root CA MUST successfully complete a point-in-time readiness assessment audit against the WebTrust EV Program.

(2) ~~If the CA has a currently valid ETSI 102 042 audit, then, before issuing EV Certificates, the CA and its Root CA MUST successfully complete a point-in-time readiness assessment audit against ETSI TS 102 042 reporting on a period of at least one day.¶~~

¶

~~(3)~~ If the CA has a currently valid ETSI EN 319 411-1 audit for EVCP policy, then, before issuing EV Certificates, except as permitted in BR section 8.1.1, the CA and its Root CA MUST successfully complete a~~n point-in-time readiness assessment~~ audit against ETSI EN 319 411-1 for EVCP or ETSI EN 319 411-2 reporting on a period of at least one day.

(4) If the CA does not have a currently valid WebTrust Seal of Assurance for CAs or an ETSI EN 319 411-2~~102 042 EVCP~~ audit or an ETSI EN 319 411-1 audit for EVCP policy, then, before issuing EV Certificates, except as permitted in BR section 8.1.1~~ to Subscribers other than itself~~, the CA and its Root CA MUST successfully complete either: (i) a point-in-time or period-of-time~~n point-in-time readiness assessment~~ audit against the WebTrust for CA Program, or (ii) a~~n point-in-time readiness assessment~~ audit against the WebTrust EV Program, the ETSI EN 319 411-2~~TS 102 042 EVCP~~, or the ETSI EN 319 411-1 for EVCP policy reporting on a period of at least one day..

The CA MUST complete any required pre-issuance readiness audit~~point-in-time readiness assessment~~ no earlier than twelve (12) months prior to issuing an EV Certificate , except as permitted in BR section 8.1.1. The CA MUST undergo a~~n complete~~ audit reporting on a period of at least 60 days under such scheme within ninety (90) days of issuing the first EV Certificate to a Subscriber other than itself.