

Chrome Root Program

CA/Browser Forum F2F 62

In this update

- 01 Policy Updates
- 02 Incident Reporting
- 03 Other PKI-related Updates

01

Policy Updates



Version 1.5, Landed January 2024

The draft CRP Policy Version 1.5 was shared in advance with CA Owners included in the Chrome Root Store.

- **11** CA Owners provided a total of **62** initial comments, which resulted in changes to the drafted text.

In short:

1. **Thank you.** This resulted in a **better** policy update.
2. We plan to continue “pre-fighting” future policy updates.

Reminder: “Moving Forward, Together”


- First introduced at [F2F 55](#).
- **Long-term** initiatives that promote increased speed, security, stability and simplicity.
 - Non-normative, **not** policy.
- Feedback is **welcome**.
- More information is located [here](#).

Reminder: A Phased Approach (tentative)

- Support for automation
- Term limit for roots
- Establish minimum expectations for linting
- Phase out “multi-purpose” roots
- Phase out clientAuth use cases
- Strengthen domain validation
- Shorter validity period for subCAs
- Shorter validity period for leaf certificates



Reminder: What's Next? (tentative)

- Support for automation
 - Term limit for roots
 - Establish minimum expectations for linting
 - Phase out “multi-purpose” roots
 - Phase out clientAuth use cases
 - Strengthen domain validation
 - Shorter validity period for subCAs
 - Shorter validity period for leaf certificates
-  **addressed in Policy V1.5**

Reminder: What's Next? (tentative)

- ~~Support for automation~~
- ~~Term limit for roots~~
- **Establish minimum expectations for linting**
- **Phase out “multi-purpose” roots**
- **Phase out clientAuth use cases**
- Strengthen domain validation
- Shorter validity period for subCAs
- Shorter validity period for leaf certificates



under exploration

What's Next? (current status)

- ~~Support for automation~~
- ~~Term limit for roots~~
- **Establish minimum expectations for linting**
- **Phase out “multi-purpose” roots**
- **Phase out clientAuth use cases**
- Strengthen domain validation
- Shorter validity period for subCAs
- Shorter validity period for leaf certificates



our goals may be
addressed by
SC-075

What's Next? (current status)

- ~~Support for automation~~
- ~~Term limit for roots~~
- Establish minimum expectations for linting
- Phase out “multi-purpose” roots
- Phase out clientAuth use cases
- Strengthen domain validation
- Shorter validity period for subCAs
- Shorter validity period for leaf certificates



**CA Owner
feedback
collected in April
2023 survey**


What's Next? (current status)

- ~~Support for automation~~
- ~~Term limit for roots~~
- Establish minimum expectations for linting
- Phase out “multi-purpose” roots
- Phase out clientAuth use cases
- Strengthen domain validation
- Shorter validity period for subCAs
- Shorter validity period for leaf certificates



**our goals may be
addressed by way
of the ongoing
'single-purpose'
hierarchy
discussions**

What's Next? (current status)

- ~~Support for automation~~
- ~~Term limit for roots~~
- Establish minimum expectations for linting
- Phase out “multi-purpose” roots
- Phase out clientAuth use cases
- **Strengthen domain validation** 
- Shorter validity period for subCAs
- Shorter validity period for leaf certificates

**our goals are
partly addressed
by SC-067 (MPIC)
- if passed**

Version 1.6?

TBD.

We'll continue following ongoing CA/Browser Forum discussions to determine if a Chrome Root Program Survey may better help us explore planned changes.

02

Incident Reporting



Incident Reporting is an Opportunity

Incident Reporting is an **opportunity** to demonstrate **continuous improvement** and to **make the ecosystem more resilient and secure**.

We rely on the public incident reporting process:

- as a demonstration that continued trust is justified.
- while reviewing CA Inclusion Requests.

We think incident reporting should be **boring** (i.e., routine).

Incident Reporting Tone

We expect:

- reports to be **detailed, candid, timely, and transparent**.
- CA Owners to demonstrate **ownership and accountability** (i.e., not place blame or deflect responsibility).

We think the value derived from an Incident Report is commensurate with the effort and thought put into writing and responding to it.

Incident Reporting Content

Our [policy](#) highlights the factors that are most significant to Chrome:

- a demonstration of **understanding of the root causes** of an incident,
- a **substantive commitment** and timeline to changes that **clearly and persuasively address the root cause**,
- past history by the Chrome Root Program Participant in its incident handling and its **follow through on commitments**, and,
- the severity of the security impact of the incident.

Incident Reporting “Do’s”

- Follow the Incident Reporting [guidelines](#) on CCADB.org;
- Use Markdown to improve formatting and readability;
- Be candid, detailed, and objective;
- Foster a culture of blamelessness;
- Promptly and accurately convey the incident’s scope;
- Provide a thorough and comprehensive root cause analysis;
- Make clear, detailed, timebound, and measurable commitments;
- Promote continuous improvement (e.g., postmortems and lessons learned); and
- Participate (often, and in more than just your organization's reporting process!).

Incident Reporting “*Don’ts*”

- Make generic responses, or responses that could be (mis-)interpreted as being evasive, misleading, or dishonest;
- Make claims that are subjective, unqualified opinions, speculative, or impossible to substantiate;
- Perform superficial root cause analysis; or
- Provide an incomplete or opaque actions commitment list.

Opportunity Ahead

We're working with members of the CCADB Steering Committee to propose an update to the CCADB Incident Reporting Guidelines.

Intended goals:

- Promote transparency, collaboration, and continuous improvement.
- More clearly define response expectations;
- Make incident reports more useful; and
- Highlight examples of good practice.

We'll share these updates for comment with public@ccadb.org in advance of considering their adoption.

Final Thoughts

We consider recent trends observed in Bugzilla **unacceptable**. Examples include:

- Mis-issuance prevented by linting
- Delayed revocations becoming routine rather than exceptional

Persistent and willing non-compliance has no place in this ecosystem.

We're evaluating opportunities to realign community expectations and intend to promote a renewed emphasis on upholding reasonable compliance expectations.

Once ready, we'll share more with CA Owners included in the Chrome Root Store.

03

Other PKI-related Updates



Active Experiment: Leaf Revocation

We've recently begun an experiment in the Chrome Canary, Dev, and Beta release channels that adds a subset of leaf certificate revocations to [CRLSet](#) for CRLs disclosed to the CCADB and trusted in Chrome.

We hope to share more on this work and any potential outcomes in the future.

Active Experiment: Enterprise Policies

We're experimenting with new Enterprise Policies to help make it easier to manage certificate trust in Chrome.

Use cases under exploration include:

- Adding local trust;
- Constraining trust (i.e., apply name constraints); and
- Distribute intermediates (optimize path building).

Once landed, expect to find these policies defined [here](#).

Coming Soon: Chrome Root Store UI Refresh

We're working on an update that refreshes the existing certificate management settings interface and applies it consistently across all desktop platforms and Android.

The new settings interface allows users to:

- add local trust anchors,
- more easily view the contents of the Chrome Root Store,
- view certificates imported from the Operating System,
- view certificates deployed by their enterprise administrators, and
- apply additional constraints (i.e., name constraints).

Under Exploration: Sunlight Logs

We're excited and encouraged by the recent announcement of [Sunlight](#), and are exploring plans for support in Chrome.

Workstreams in-progress:

- Evaluating necessary CT Policy updates to introduce Sunlight log adoption
- Establishing mechanisms for compliance monitoring (i.e, parity with existing RFC6962 log evaluations)

Once ready, we'll share more information at ct-policy@chromium.org.

Contact us at:

[chrome-root-program\[at\]google\[dot\]com](mailto:chrome-root-program@google.com)

Policy page at:

<https://g.co/chrome/root-policy>