

Chrome Root Program

CA/Browser Forum F2F 63

In this update

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

01

Policy Updates



State of the Chrome Root Program Policy

Version 1.5 landed in January 2024.

Actively working towards releasing Version 1.6 for CA Owner pre-flight.

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**.


Actively working towards an update, which will be located [here](#) when it lands.

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

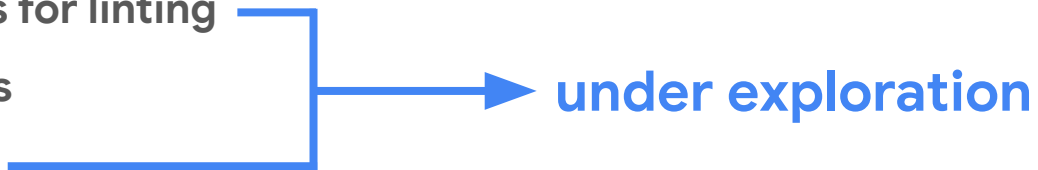


Reminder: What's Next? (tentative)

- ~~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~~  **addressed by SC-075**
- **Phase out “multi-purpose” roots**
- **Phase out clientAuth use cases**
- Strengthen domain validation
- Shorter validity period for subCAs
- Shorter validity period for leaf certificates

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



in-scope for Policy V1.6

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



**partly addressed by:
SC-067 (MPIC), SC-080
(if passed), and Policy V1.6**

Version 1.6?

CA Owners in the Chrome Root Store can expect a policy pre-flight via CCADB message in the coming weeks.

Goal: offer at least 90 days between initiating the pre-flight process and when new requirements become normative.

02

Incident Reporting Updates



Reminder: Incident Reporting

We (Chrome Root Program) do not:

- have the authority to grant exceptions to the CA/Browser Forum TLS Baseline Requirements.
- offer guarantees of specific outcomes in response to the course(s) of action deemed most appropriate by a CA Owner.

Reminder: Incident Reporting

As detailed in our policy, we evaluate all incidents on a case-by-case basis and point to the factors significant to our program, which include (but are not limited to):

- 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** of incident handling and its **follow through on commitments**, and,
- the **severity of the security impact** of the incident.

Reminder: Incident Reporting

Outside egregious cases (e.g., abject security failures), we do not make trust decisions on individual incidents, and always consider the wider context.

What's Next?

We've been collaborating with the members of the CCADB Steering Committee to further improve Web PKI Incident Reporting.

Additional information, along with an opportunity to share feedback on the set of proposed updates, will be communicated via public@ccadb.org in the coming weeks.

03

Other PKI-related Updates



Landed: Leaf Revocation

All Chrome release channels have added leaf certificate revocations with a reasonCode of either keyCompromise or privilegeWithdrawn to [CRLSet](#) for CRLs disclosed to the CCADB and trusted in Chrome.

We intend to further study expanding the set of reasonCodes consumed by CRLSet in the future.

Coming Soon: Support for Static CT Logs

We now have monitoring parity for both RFC 6962 logs and "Static", sometimes referred to as "Tiled" Certificate Transparency ("CT") logs.

We're evaluating the necessary CT Policy updates to introduce Static log adoption.

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>