Chrome Root Program

CA/Browser Forum F2F 64

In this update

01 Policy

02 “Moving Forward, Together”

03 PKI-related happenings

01
Policy

State of the Chrome Root Program Policy

Version 1.6 landed February 15, 2025.

The draft CRP Policy Version 1.6 was shared in advance with CA Owners included in the Chrome Root Store on November 13, 2024.

- **19** CA Owners provided a total of **98** initial comments, which resulted in changes to the drafted text and the need for a second round of review with those CA Owners.
- **8** CA Owners then provided a total of **21** additional comments, which resulted in additional changes.

Thank you to those who participated and helped us improve our policy.

Scope of updates

- Future phase-out of non-TLS server authentication hierarchies.
- Require simplified policies in Markdown for future Applicants.
- Strengthening automation support requirements for future Applicants.
- Improved TLS Baseline Requirements alignment (e.g., SC-077).
- Document reorganization.

In February 2025, we asked CA Owners with certificates included in the Chrome Root Store to acknowledge the policy update.

- **100%** of CA Owners included in the Chrome Root Store acknowledged their understanding and intent to adhere to the updated policy. **Thank you**.

Chromium.org transition

Transitioning from Chromium.org to **GitHub**.

- Markdown formatted version of our policy available here.
- HTML rendering of that Markdown is available here.
- Please update your bookmarks! We'll send a CCADB mass email to CA Owners included in the Chrome Root Store before deprecating the old site.

Unused roots in the Chrome Root Store

- As stated in the Chrome Root Program Policy: "*CA certificates included in the Chrome Root Store must provide value to Chrome end users that exceeds the risk of their continued inclusion.*"
- We do not consider unused roots (i.e., those not actively issuing beyond test certificates and/or those with no measurable reliance during validation) consistent with a CA offering broad value that exceeds the risk of their inclusion.
- We've contacted several CA Owners related to the upcoming removal of unused roots from the Chrome Root Store.
- Proactive disclosure and removal requests related to unused roots are welcome and appreciated!

02
“Moving Forward, Together”

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**.

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~~ → addressed in Policy V1.5
- ~~Establish minimum expectations for linting~~ → addressed by SC-075
- ~~Phase out "multi-purpose" roots~~
- ~~Phase out clientAuth use cases~~ → addressed in Policy V1.6
- ~~Strengthen domain validation~~ → partly addressed by SC-067, SC-080, and Policy V1.6
- Shorter validity period for subCAs
- Shorter validity period for leaf certificates

What's Next? (current priority)

- ~~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** → **could be addressed by SC-081 (if passed)**

Moving Forward, Together - Chapter 2

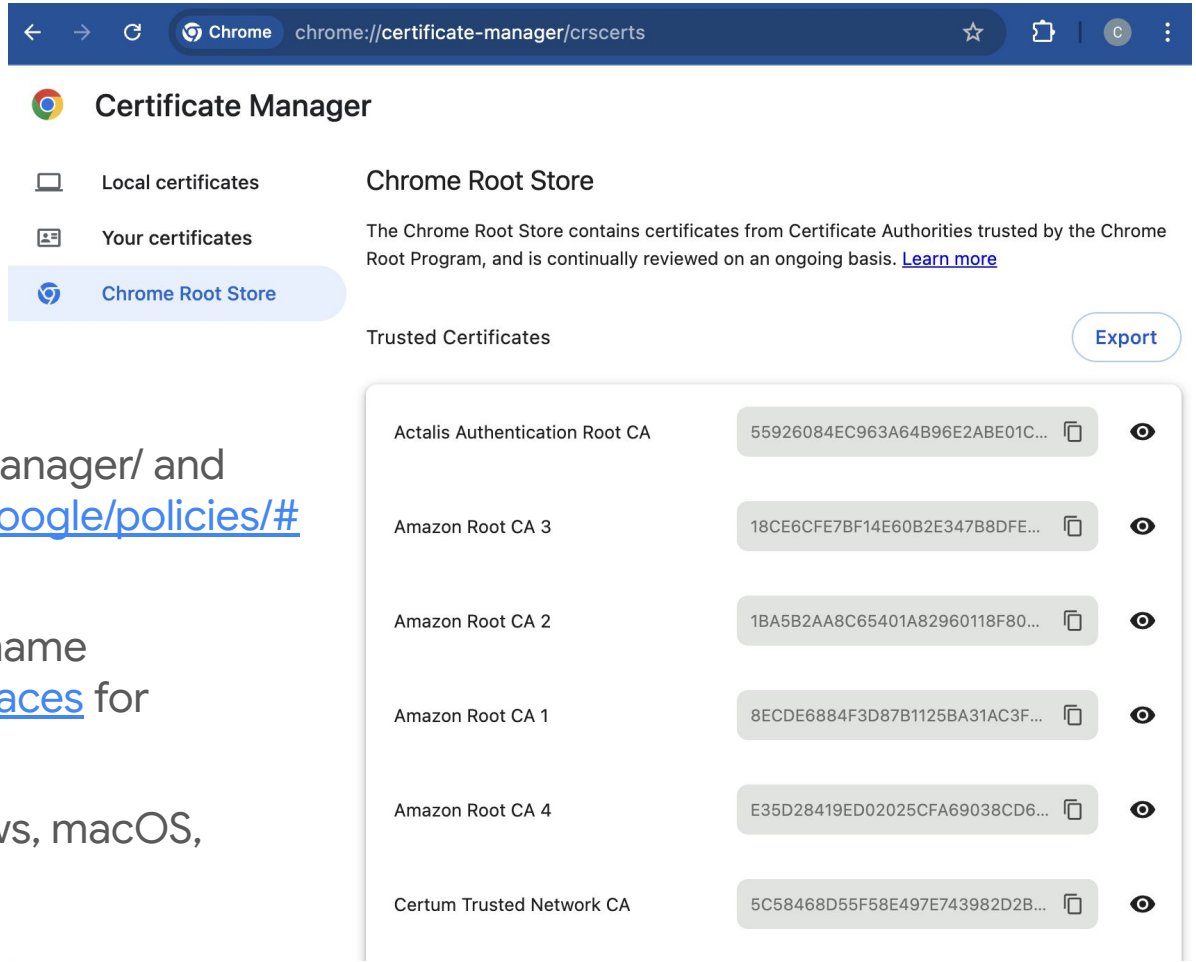
- Further improving CA agility (e.g., ICA validity)
- Further improving transparency (e.g., “DCV transparency”)
- Further strengthening domain control validation
- Further promoting ARI and ARI-like capabilities
- Improving incident detection and disclosure
- Emphasizing externally-verifiable processes and requirements
- Support for post-quantum cryptography in the Web PKI

03
PKI-related happenings

Secure Time

- Previously, Chrome used the system clock to decide whether a certificate was within its validity period. Doing so created opportunities for certificate errors when the system clock was not properly set.
- We recently launched a feature that changes certificate validation to instead rely on a Chrome-managed time source, with fallback to the system clock.
- This feature is especially important considering the use of short-lived certificates.
    - We've also noticed an ~8% decrease in certificate validity errors since launch.

Root Store Management UI and Enterprise Settings



- See chrome://certificate-manager/ and https://chromeenterprise.google/policies/#CertificateManagement
- Offers new features (e.g., name constraints) and new interfaces for managing existing features
- Rolling out now for Windows, macOS, ChromeOS, and Linux

Static CT API

- Announced initial acceptance of tiled logs while maintaining RFC 6962 fallback.
- CT policy effective for Chrome M134 (released March 4th) permits tiled log SCTs with at least one RFC 6962 SCT.
- All certificates passing Chrome's previous CT policy will continue to validate under the updated policy.
- Static-CT-API logs may be submitted for inclusion starting April 1st.
- **Goal**: API-agnostic policy, possibly as soon as October.

Future Chrome updates

- We're naturally arriving at an (approximately) annual Chrome Root Program Policy update cadence.
- We are satisfied with our ability to communicate with CA Owners during regularly-scheduled working group meetings, via email, and via CCADB messages.
- We're equally satisfied with our ability to collect feedback from CA Owners using our current processes.
- Going forward, we may scale-back F2F updates.
- We hope, instead, this time can be dedicated to CA Owners sharing updates related to actions being taken to meaningfully improve the security of the Web PKI.

Contact us at:
chrome-root-program[at]google[dot]com

Policy page (*for now*) at:
https://g.co/chrome/root-policy