Chrome Browser Update

CA/Browser Forum F2F 56
June 6, 2022

Agenda

- Chrome Root Program Updates
- Certificate Transparency Updates
- General Browser Updates

Chrome Root Program (Policy)

- Updated policy posted (https://g.co/chrome/root-policy)
    - In force immediately, but many requirements are future dated

Chrome Root Program (*Reminder from F2F 55*)

- Long-term priorities focused on:
    - encouraging modern infrastructures and agility
        - replace “legacy” roots (i.e., keys established before the BRs or modern audit schemes) with newer ones
    - focusing on simplicity
        - purpose-driven infrastructures with dedicated use cases (e.g., HTTPS only)
    - promoting automation
        - establish minimum expectations for ACME support
    - reducing mis-issuance
        - set minimum expectations for pre/post-issuance linting
    - increasing accountability and ecosystem integrity
        - improve automated monitoring and reporting capabilities
    - preparing for a “post-quantum” world
        - encourage experimentation with and testing of quantum-resistant algorithms

Chrome Root Program (Updated Policy Highlights)

- For Root CAs included in the initial Chrome Root Store:
  - Audit, Incident Reporting, and Communication Requirements consistent with other public root program requirements
  - Annual self-assessment process, beginning in 2023
- For new Root CA applicants:
  - Key material must have been generated within five (5) years from time of application
  - Attestation of domain validation methods in use during TLS certificate issuance
  - Hierarchies must be dedicated to TLS certificate issuance
  - Submission of self-assessment expressing conformance with Chrome Root Program policy and the Baseline Requirements

Chrome Root Program (Future Policy Considerations)

- Future considerations:
  - Establish a limit for how long the Chrome Root Store will distribute CA certificates
  - Phase-out existing multipurpose root CA certificates included in the Chrome Root Store (align existing CAs with requirements for new applicants)
  - Promote automation by requiring new CAs established after a future date support ACME for certificate issuance and revocation
  - Apply consistent audit standards for all subordinate CAs, regardless of the presence of technical constraints

Chrome Root Program (Application Process)

- Planning integration with CCADB
- *Targeting* to open application process in **September**

Chrome Root Program (Feature Launch Roadmap)

Platform	Current State (Today)		Future State (Summer/Fall 2022)	
	Certificate Verifier	Root Store	Certificate Verifier	Root Store
Android	Platform Verifier	Platform Root Store	Platform Verifier	Platform Root Store
Chrome OS	Chrome Cert Verifier		Chrome Cert Verifier	Chrome Root Store
iOS	Platform Verifier		Platform Verifier	Platform Root Store
Linux	Chrome Cert Verifier		Chrome Cert Verifier	Chrome Root Store
macOS	Chrome Cert Verifier*		Chrome Cert Verifier	Chrome Root Store
Windows	Chrome Cert Verifier*	Chrome Root Store*	Chrome Cert Verifier	Chrome Root Store

***Note**: Phased roll-out in-progress

Feature Launched 🟩

Chrome Root Program (Reminders for CA Operators)

- For CA operators listed in the initial store, continue to:
  - Follow your policies, the BRs, and the Chrome Root Program Policy
    - Report incidents to chrome-root-program@google.com.
  - Follow the CCADB Policy and ensure timely updates to policy and practices documents and CA disclosures.

- For HTTPS CA operators NOT listed in the initial store:
  - We'll share a notification once the application process is open.

Certificate Transparency Updates

- Certificate Transparency Policy (https://goo.gl/chrome/ct-policy)
  - Recent updates (enforcement began in Chrome 100):
    - Removal of “One Google Log” requirement for CT-compliance
    - Changed SCT requirements for certificates with validity periods >= 180 days
- Certificate Transparency Log Policy (https://goo.gl/chrome/ct-log-policy)
  - Recent updates (effective March 22, 2022):
    - CT Logs are permitted to enforce id-kp-serverAuth EKU for logging submissions.

Certificate Transparency Updates (continued)

- Launched CT in Chrome on Android (Chrome 101)
- We’re still working on turning down Google’s legacy non-sharded Logs.

General Browser Updates

- Beginning in **Chrome 103** (Jun. 21, 2022)
  - Targeted release for Chrome Root Store Component Updater
- Beginning in **Chrome 104** (Aug. 2, 2022)
  - CCV expected to be enabled by default on macOS (integrated with platform root store)
  - Targeted release for Chrome Certificate Viewer
- Beginning in **Chrome 105** (Aug. 30, 2022)
  - Initial rollout of CRS on macOS and Windows
  - Initial rollout of CCV on Windows (coupled with CRS)

Contact us at:

chrome-root-program@google.com

Policy page at:

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

[Backup] Testing the CCV and CRS on Windows

1. Download the latest version of Chrome Canary
2. Enable feature flag
    - *Right-click* **Chrome Canary** shortcut
    - *Append* `--enable-features=ChromeRootStoreUsed` to the **Target** variable

      ```
      Example: "C:\Users\User1\AppData\Local\Google\Chrome
      SxS\Application\chrome.exe" --enable-features=ChromeRootStoreUsed
      ```
3. Open Canary and begin testing