Chrome Browser Update

CA/Browser Forum F2F 57

October 24, 2022

Agenda

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

Chrome Root Program - General Updates

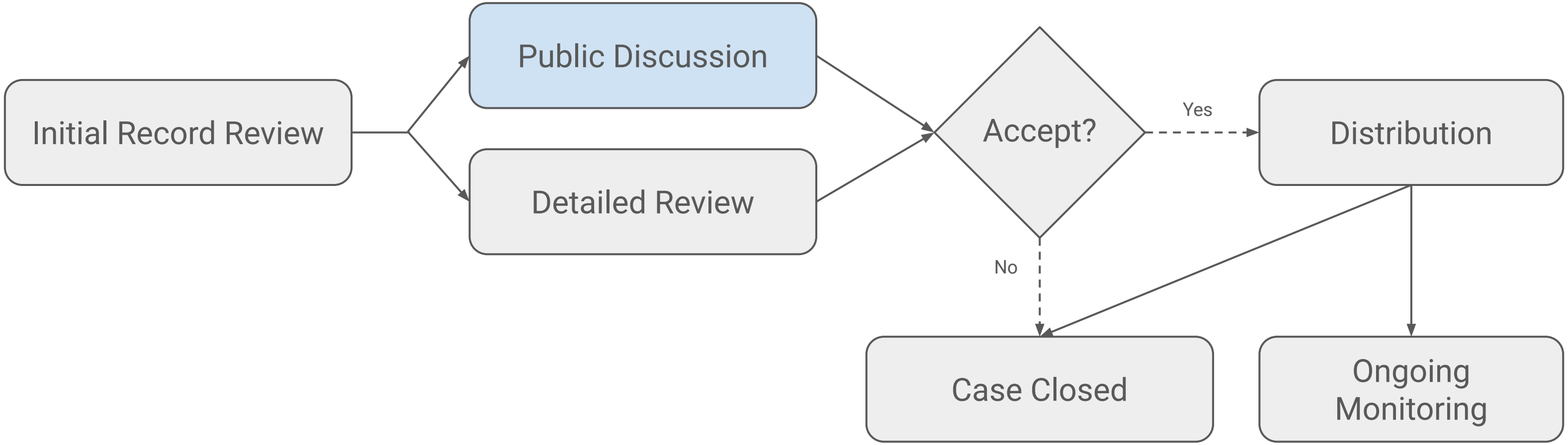
- **“Open for business”**
  - Additional CCADB enhancements coming soon to improve inclusion request process
- **Latest Policy**
  - Version: 1.2
  - Effective: September 1, 2022
  - URL: https://g.co/chrome/root-policy
- **Comparing Version 1.2 against Version 1.1 (June 1, 2022)**
  - Removal of pre-launch discussion
  - Enhancements and clarifications resulting from June CCADB survey
    - Added “Change History” table
    - Clarified audit expectations
    - Aligned terminology with Baseline Requirements and CCADB (e.g., “CA Owners”)
    - Aligned self assessment process with the existing Mozilla process
  - Moved non-normative sections (i.e., “Requesting Inclusion” and “Moving Forward, Together”) to separate pages

Chrome Root Program - Application Submission

- **Application Process**
  1. CA Owner creates and submits a new “Add/Update Root Request” case in CCADB
  2. On-rotation CCADB Steering Committee member processes and closes case
  3. Chrome Root Program notified of completed “Add/Update Root Request” case
     - **Today:** CA Owner emails chrome-root-program@google.com
     - **Coming Soon:** CA Owner submits a “Root Inclusion Request” case in CCADB

Chrome Root Program - Application Review

- **High-Level Milestones**



Chrome Root Program - Detailed Review

- **Scope of review includes:**
  - CA owner justification statement (risk/value statement)
  - CA owner/operator organization background and ownership
  - Incident history (timely?, transparent?, detailed?, focused on continuous improvement?, etc.)
  - PKI hierarchy (external trust relationships?, dedicated to TLS?, etc.)
  - Certificate and profile review (key-pair freshness, automated tests, etc.)
  - Audit statements
  - Self assessment
  - Policies and practices (CP, CPS, subscriber agreement, etc.)
  - Community comments and concerns from the Public Discussion process

Chrome Root Program - Reminder of Priorities

- **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 - Reminder of Priorities

- **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 - Reminder of Priorities

- **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 - Reminder of Priorities

- **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 - What's Next

- **"Moving Forward Together: Chapter 1"**
    - Upcoming CCADB survey focused on understanding adoption (existing and planned) of automated certificate issuance and management solutions for CA owners included in the Chrome Root Store
    - Survey results will be used to improve perspective that may lead to future updates to the Chrome Root Program Policy
    - Underlying goals:
        - promote agility,
        - better prepare the ecosystem for responding to a post-quantum future,
        - reduce the impact of mis-issuance and other security events on site owners, and
        - better uphold the commitments made in the Baseline Requirements.
    - Current focus:
        - Ensuring automated issuance and management solutions are an option for site owners, but not requiring they are the *only* option.

Chrome Root Program - Feature Launch Roadmap

Platform	Current State (Today)		Future State (Spring 2023)	
	Certificate Verifier	Root Store	Certificate Verifier	Root Store
Android	Platform Verifier	Platform Root Store	Chrome Cert Verifier	Chrome 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 Root Store	Chrome Cert Verifier	Chrome Root Store
Windows	Chrome Cert Verifier	Chrome Root Store	Chrome Cert Verifier	Chrome Root Store

Feature Rollout In-Progress 🟨 Feature Launched 🟩

Certificate Transparency Updates

- Certificate Transparency Policy (https://goo.gl/chrome/ct-policy)
  - No policy updates to report

- Certificate Transparency Log Policy (https://goo.gl/chrome/ct-log-policy)
  - No policy updates to report

Certificate Transparency Updates (continued)

- Log State Changes:
  - **September 15, 2022**, the following logs transitioned to *Retired*, with the last ‘Qualified’ SCT having a timestamp no later than 2022-09-15T00:00:00Z:
    - Google 'Icarus' log (https://ct.googleapis.com/icarus/)
    - Google 'Pilot' log (https://ct.googleapis.com/pilot/)
    - Google 'Rocketeer' log (https://ct.googleapis.com/rocketeer/)
    - Google 'Skydiver' log (https://ct.googleapis.com/skydiver/)
  - **October 14, 2022**, the following logs transitioned to *Retired*, with the last ‘Qualified’ SCT having a timestamp no later than 2022-09-29T00:00:00Z:
    - DigiCert Yeti2022-2 Log (https://yeti2022-2.ct.digicert.com/log/)
    - DigiCert Yeti2023 Log (https://yeti2023.ct.digicert.com/log/)

General Browser Updates

- Beginning in **Chrome 104** (*August 2, 2022*)
  - Certificate Viewer lands on Windows and macOS (already in-use on Linux and Chrome OS)
- Beginning in **Chrome 105** (*August 30, 2022*)
  - CCV/CRS rollout begins on Windows and macOS
- Beginning in **Chrome 106** (*September 27, 2022*)
  - Disable OCSP checks by default for EV certificates
- Coming Soon (*TBD*)
  - Encrypted Client Hello (ECH)
  - Chrome Root Store on Chrome OS and Linux
  - Chrome Root Store and Certificate Verifier on Android

Contact us at:
chrome-root-program@google.com

Policy page at:
https://g.co/chrome/root-policy

Background: Additional Information

- Testing Instructions
- Frequently asked questions
- ChromeRootStoreEnabled Enterprise Policy (temporary)