Chrome Browser Update

CA/Browser Forum F2F 55
February 22, 2022
Agenda

- Chrome Root Program Updates
- Chrome Certificate Verifier Updates
- Certificate Transparency Updates
- General Browser Updates
Chrome Root Program (launch planning)

- Looking to launch V1 this Summer
- V1 Scope:
  - **Governance:**
    - policy,
    - application and inclusion process, and
    - incident management process
  - **Root Store and Component Updater enabled by default on:**
    - Chrome OS,
    - Linux,
    - macOS, and
    - Windows

**Note:** platforms will launch at different times (more on this later)
Chrome Root Program (next steps for CA operators)

- Prior to launch, we’ll share next-steps with CA operators listed in the transitional store and organizations that have directly expressed interest.

- For CA operators listed in the transitional store, continue to:
  - Follow your policies and the BRs.
  - Report incidents to chrome-root-authority-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 transitional store:
  - Email us at chrome-root-authority-program@google.com to be notified of program launch and subsequent application processing.
Chrome Root Program (perspective and vision)

- **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 Certificate Verifier (trials and results)

- In conjunction with the Chrome Root Store, we’re transitioning away from platform certificate verifiers to our own
  
  - For over the past year, we’ve been running experiments on macOS and Windows to evaluate the Chrome Certificate Verifier (CCV) against platform verifiers.
  
  - Overall, CCV verifications are comparable in terms of outcome and performance.
  
  - Experiments and corresponding data will continue to be used to detect potential issues and guide remaining launches.
# Combined Feature Set (launch roadmap)

<table>
<thead>
<tr>
<th>Platform</th>
<th>Current State (Today)</th>
<th>Future State (Summer 2022)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Certificate Verifier</td>
<td>Root Store</td>
</tr>
<tr>
<td>Android</td>
<td>Platform Verifier</td>
<td>Platform Root Store</td>
</tr>
<tr>
<td>Chrome OS</td>
<td>Chrome Cert Verifier</td>
<td></td>
</tr>
<tr>
<td>iOS</td>
<td>Platform Verifier</td>
<td>Platform Root Store</td>
</tr>
<tr>
<td>Linux</td>
<td>Chrome Cert Verifier</td>
<td></td>
</tr>
<tr>
<td>macOS</td>
<td>Chrome Cert Verifier*</td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td>Platform Verifier</td>
<td></td>
</tr>
</tbody>
</table>

*Note: Phased roll-out in-progress beginning in Release 98 (first available Feb. 3, 2022)*

Feature Launched
Certificate Transparency

- Recently **announced** updates to the Chrome CT Policy
- Technical implementations landing in **Chrome 100 (3/29/22)**:
  - Relaxing the ‘One Google Log’ requirement for CT-compliance
    - For certificates issued **on-or-after** 4/15/22, certificates are no longer required to be accompanied by an SCT from a Google-operated CT log.
    - Instead, there must be SCTs from at least 2 distinct CT log operators as specified in the **Chrome CT log list**.
  - Changing SCT requirements for certificates with validity periods >= 180 days
    - For certificates issued **on-or-after** 4/15/22 with validity periods of 180 days or longer that are embedding SCTs, there must now be at least 3 SCTs from distinct CT logs (aligns Chrome and Apple policies).
General Browser Updates

- **Beginning in Chrome 98** (Feb. 1, 2022)
  - TLS 1.0 and 1.1 now blocked with a non-bypassable error, rather than an interstitial warning
  - Phased roll-out of Chrome Certificate Verifier on macOS

- **Beginning in Chrome 99** (Mar. 1, 2022)
  - EV root clean-up (added UI treatment for several roots, some removals)

- **Beginning in Chrome 100** (Mar. 29, 2022)
  - Technical enforcement of new CT policy (‘One Google Log’ / # of SCTs)
Contact us at: chrome-root-authority-program@google.com

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