Chrome Browser Update

CA/Browser Forum F2F 58
February 28, 2023
Agenda

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

- Policy
- Application Process
- Reminder of Priorities ("Moving Forward, Together")
- ACME Survey Results
- What’s Next?
Chrome Root Program Updates

- **Latest Policy**
  - **Version:** 1.4 *(COMING SOON)*
  - **Effective:** Immediately upon publication
  - **URL:** https://g.co/chrome/root-policy

*CA owners with certificates included in the Chrome Root Store will be notified of publication via CCADB message.*
Chrome Root Program Updates

- **Comparing Version 1.4 against Version 1.3**
  - alignment with CCADB Policy Version 1.2 and the Baseline Requirements...
    - updated audit and incident reporting requirements
    - require subordinate CA disclosures in CCADB
    - standardize terminology
  - clarify requirements to...
    - better align with program intent (e.g., CA owner policy document freshness)
    - reduce opportunities for confusion (i.e., related to the submission of annual self assessments)
  - remove requirements to reduce...
    - duplicative effort (i.e., incident reporting)
    - operational burden (i.e., CA certificate issuance notification)
Chrome Root Program Updates

- **Apply for Inclusion**
  - process outlined [here](#), described at [F2F 57](#)

- **Reminders:**
  - TLS hierarchies, only
  - Applications and changes are processed through CCADB
  - Self Assessment is required at time of submission
  - Applicants must demonstrate:
    - broad value for Chrome users
    - why the benefits of inclusion outweigh the risks to user safety and privacy
Chrome Root Program Updates

- **Long-term priorities focused on [REMINDER FROM F2F 55]:**
  - 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 Updates

- “Moving Forward, Together”:
  - Beginning in Version 1.1, our policy has referenced our “Moving Forward, Together” (MFT) initiative.
  - MFT:
    - represents our goals and priorities.
    - reinforces our commitment to working alongside CA owners to make the web a safer place.
    - describes our vision for the future that includes modern, reliable, highly agile, purpose-driven PKIs that promote automation, simplicity, and security.
    - is non-normative, but describes what might become normative.
Chrome Root Program Updates

- **ACME Survey Summary:**
  - **Focus:** understanding adoption (existing and planned) of automated certificate issuance and management solutions for CA owners included in the Chrome Root Store, with an emphasis on ACME
  - **How:** CCADB message with embedded [survey](#) form
  - **Response Window:** Dec 13, 2022 to Jan 13, 2023
  - **Participation:** 48 responses
Key Results...

41.7% of respondents offer the use of ACME services for publicly-trusted TLS certificates
Key Results...

70%

observe ACME use increasing
Key Results...

70% observe ACME use increasing

30% observe ACME use remaining the same
Key Results...

70% observe ACME use increasing

30% observe ACME use remaining the same

0% observe ACME use decreasing
Key Results...

>95% of the certificates issued by the “Web PKI” today are issued by a CA owner with some form of existing ACME implementation available for customers (this includes DV, OV, and EV)
Key Results...

1 in 2 certificates issued by the “Web PKI” today rely on ACME.
ACME is not yet ubiquitous...

58.3% of CAs owners included in the Chrome Root Store do not offer ACME services for publicly-trusted TLS certificates.
Key Results...

36%

Expect to offer ACME services in 2023 or 2024
Key Results...

36% Expect to offer ACME services in 2023 or 2024

64% Did not express a timeline for offering ACME services
Understanding why ACME is not offered...

- “ACME isn’t…”
  - compatible with OV/EV (a common misunderstanding)
  - compatible with existing certificate issuance systems and workflows
  - an option for all customers

- “We offer…”
  - other forms of automation (i.e., proprietary methods based on SCEP, EST, CMP, etc.)
Chrome Root Program - What’s Next

• **Strengthening our commitment to ACME:**
  - After carefully reviewing responses and considering CA feedback, we’re planning a future policy update that will require ACME support for *applicant hierarchies*.
    - ACME must be *an option*, not the only option.

• **Why ACME and not [$OTHER_SOLUTION]***
  - Widespread ecosystem support and adoption (CA owners and site owners)
  - ACME is open and benefits from continued innovation and enhancements from a robust set of ecosystem participants
  - Extensive set of well-documented client options spanning multiple languages
  - Designed specifically to meet to TLS certificate issuance needs for the “Web PKI”
Chrome Root Program - What’s Next

- Benefits of unifying the Web PKI ecosystem in support of ACME:
  - promote agility
  - increase resiliency for CA owners and website owners alike
  - help website owners address scale and complexity challenges related to certificate issuance, installation, and management
  - drive innovation through ongoing enhancements and support from an open community
  - ease the transition to quantum-resistant algorithms, and
  - better positions the Web PKI ecosystem to manage risk
Chrome Root Program - What’s Next

● “Moving Forward, Together” Update (COMING SOON)
  ○ We continue to sharpen our focus while promoting modern, reliable, highly agile, purpose-driven PKIs that focus on automation, simplicity, and security.
  ○ An update released alongside policy Version 1.4 will:
    ■ offer expanded commentary on existing initiatives (e.g., ACME)
    ■ highlight new areas of interest and signal commitment for leading change
      ● promote subordinate CA agility
      ● reduced maximum TLS certificate validity
      ● reduced domain validation reuse periods
      ● require multiperspective domain and CAA validation
Chrome Root Program - What’s Next

- **CCADB Survey (COMING SOON)**

  - An upcoming CCADB survey will seek to understand operational impacts related to many of our proposed initiatives to include:
    - root CA “term limit”
    - establishing maximum validity periods for subordinate CA certificates
    - reducing leaf certificate validity and domain validation document reuse
    - sunsetting use of id-kp-clientAuth in server authentication certificates
### Chrome Root Program - Feature Launch Roadmap

<table>
<thead>
<tr>
<th>Platform</th>
<th>Current State (Today)</th>
<th>Future State (Spring 2023, ~Chrome 115)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Certificate Verifier</td>
<td>Root Store</td>
</tr>
<tr>
<td></td>
<td>Certificate Verifier</td>
<td>Root Store</td>
</tr>
<tr>
<td>Android</td>
<td>Chrome Cert Verifier</td>
<td>Chrome Root Store</td>
</tr>
<tr>
<td></td>
<td>Chrome Cert Verifier</td>
<td>Chrome Root Store</td>
</tr>
<tr>
<td>Chrome OS</td>
<td>Chrome Cert Verifier</td>
<td>Platform Root Store</td>
</tr>
<tr>
<td></td>
<td>Chrome Cert Verifier</td>
<td>Chrome Root Store</td>
</tr>
<tr>
<td>iOS</td>
<td>Platform Verifier</td>
<td>Platform Root Store</td>
</tr>
<tr>
<td></td>
<td>Platform Verifier</td>
<td>Platform Root Store</td>
</tr>
<tr>
<td>Linux</td>
<td>Chrome Cert Verifier</td>
<td>Chrome Root Store</td>
</tr>
<tr>
<td></td>
<td>Chrome Cert Verifier</td>
<td>Chrome Root Store</td>
</tr>
<tr>
<td>macOS</td>
<td>Chrome Cert Verifier</td>
<td>Chrome Root Store</td>
</tr>
<tr>
<td></td>
<td>Chrome Cert Verifier</td>
<td>Chrome Root Store</td>
</tr>
<tr>
<td>Windows</td>
<td>Chrome Cert Verifier</td>
<td>Chrome Root Store</td>
</tr>
<tr>
<td></td>
<td>Chrome Cert Verifier</td>
<td>Chrome Root Store</td>
</tr>
</tbody>
</table>
Certificate Transparency Updates

  - No policy updates to report
  - Looking to [better understand](https://goo.gl/chrome/ct-policy) active use-cases of SCTs delivered via OCSP Stapling and/or TLS extension (i.e. not embedded in the certificate)

  - No policy updates to report
Certificate Transparency Updates (continued)

- **Log State Changes:**
  - **February 1, 2023**, the following logs transitioned to *Retired*, with the last ‘Qualified’ SCT having a timestamp no later than 2023-01-15T00:00:00Z:
    - Sectigo 'Mammoth' ([https://mammoth.ct.comodo.com/](https://mammoth.ct.comodo.com/))
Certificate Transparency Updates (continued)

- **Log State Changes:**
  - **February 1, 2023**, the following logs transitioned to *Rejected*:
    - DigiCert CT2 Log (https://ct2.digicert-ct.com/log)
    - Let's Encrypt Oak2022 Log (https://oak.ct.letsencrypt.org/2022)
Certificate Transparency Updates (continued)

- **Log State Changes:**
  - **November 22, 2022**, the following log transitioned to *Qualified*
General Browser Updates

- **Beginning in Chrome 111 (March 7, 2023)**
  - Chrome Root Store Version 10
  - “Trusted People” / Leafs

- **Beginning in Chrome 112 (April 4, 2023)**
  - Mixed content auto-upgrading (Chrome on iOS)

- **Beginning in Chrome 113 (May 2, 2023)**
  - Remove “ChromeRootStoreEnabled” enterprise policy on Mac and Windows

- **Coming Soon (TBD)**
  - Encrypted Client Hello (ECH) [thread]
  - 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