Chrome Browser Update

CA/Browser Forum F2F 59
June 6, 2023

Agenda

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

Chrome Root Program Updates

Chrome Root Program Updates

- Policy
- Reminders
- Feature Launch Roadmap

Chrome Root Program Policy

- **Latest Policy**
  - **Version:** 1.4 *(released and effective March 3, 2023)*
  - **URL:** https://g.co/chrome/root-policy
- **Policy "Preflight" Process - Coming Soon**
  - We value your feedback!
  - Future policy releases will be shared in advance of becoming effective.
  - Changes will continue to be communicated via CCADB message.

Policy Version 1.5 (planned updates)

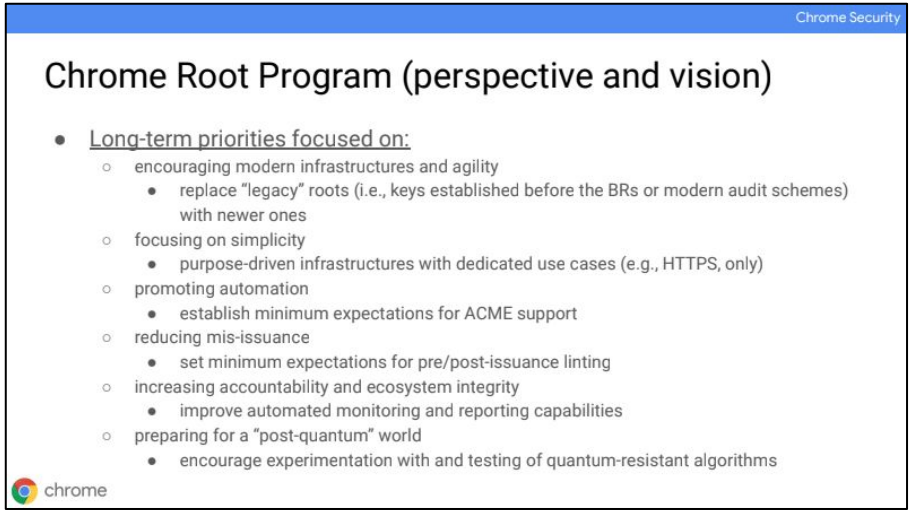
- **Applicant hierarchies must also support ACME.**
- **The update may specify requirements for:**
  - The types of certificates (i.e., certificate policy OIDs) which must be “ACME-capable”,
  - URL disclosures within CCADB,
  - Endpoint capabilities and availability,
  - Support for RFC 8657, and
  - Support for ACME Renewal Information (ARI).

Incident Reporting Reminders

- **No need to email us if the incident is disclosed to Bugzilla.**
- **Incident report formats described on CCADB.org.**
- **Reports must:**
  - be accurate, detailed, timely, candid, and transparent.
  - clearly demonstrate an understanding of the root cause.
  - demonstrate a substantive commitment to change that **clearly** and **persuasively** addresses the root cause.
- **Reports should:**
  - **not** linger without a response for more than seven calendar days.
  - share lessons learned or identify ecosystem opportunities for improvement.

“Moving Forward, Together” Reminder

- **First introduced at F2F 55.**
- **Long-term initiatives that promote increased speed, security, stability and simplicity.**
- **Feedback is welcome.**
  - Shared CCADB surveys to collect targeted CA owner feedback and understand impact.
  - Want to know the challenges and how they can be addressed.
- **More information is located here.**



Moving Forward, Together: Currently exploring

Promoting Automation

Modern Infrastructures

Improved Domain Validation

Increased Simplicity

Under consideration:

- Establish minimum expectations for ACME support.

Moving Forward, Together: Currently exploring

Promoting Automation

Modern Infrastructures

Improved Domain Validation

Increased Simplicity

Under consideration:

- Maximum “term limits” for roots.
- Define maximum validity periods for subordinate CAs.
- Reduce maximum subscriber certificate lifetimes.

Moving Forward, Together: Currently exploring

Promoting Automation

Modern Infrastructures

Improved Domain Validation

Increased Simplicity

Under consideration:

- Require “Multi-Perspective Domain Validation.”
- Reduce opportunity for domain validation reuse abuse.

Moving Forward, Together: Currently exploring

Promoting Automation

Modern Infrastructures

Improved Domain Validation

Increased Simplicity

Under consideration:

- A phase-out plan for existing “multipurpose” roots.

Moving Forward, Together: In the future

Reduced Mis-issuance

Preparing for Post-Quantum

Even More Simplicity

Increased Accountability

For more, see: https://www.chromium.org/Home/chromium-security/root-ca-policy/moving-forward-together/

“Modern Infrastructures” Survey Reminder

- **Focus:** understand impact related to “Moving Forward, Together” proposals related to our “modern infrastructures” initiatives (term limit, reduced certificate lifetime, reduce domain validation reuse period, etc.)
- **How:** CCADB message with embedded survey form.
- **Response Window:** April 24, 2023 to June 9, 2023.
- **Thank You:** CA owners who have already responded.

General Survey Reminders

- Surveys represent a good-faith effort by our team to understand ecosystem impacts related to MFT proposals.
- We appreciate candid feedback from individual organizations that offers their unique perspective.
- We can also consider other methods of data collection.
- We **welcome your feedback** at chrome-root-program [at] google [dot] com.

Motivation

Why promote automation?

- It promotes agility.
  - Automation increases the speed at which the benefits of new security capabilities are realized.
- It increases resilience and reliability.
  - Automation eliminates human error and can help scale the certificate management process across complex environments.
  - Innovations like ACME Renewal Information (ARI) present opportunities to seamlessly protect site-owners and organizations from outages related to unforeseen events.
- It increases efficiency.
  - Automation reduces the time and resources required to manually manage certificates. Team members are instead free to focus on more strategic, value-adding activities.
- Stated plainly, automation reduces risk.

Community Perspective (automation)

- *"Cryptographic agility will be enhanced through automation. Automating the update of keys and certificates will increase efficiency and reduce cost of maintaining appropriate security controls."* - (2023)
- *"Manually managing certificates also puts enterprises at significant risk of certificates being forgotten until expiration and of exposure to gaps in ownership, resulting in sudden outages or failure of critical business systems..."* - (2020)
- *"Digital certificates are needed everywhere in today's distributed and cloud environments, making manual certificate management an overwhelming task, one made prone to error by the sheer volumes alone."* - (2021)
- *"Crypto and Policy agility are reasons that require CAs, Subscribers and Relying Parties to be in a position to adapt quickly to changes."* - (2020)
- *"For us, automation will be an important key word to make future certificate management easier."* - (2020)
- *"Automation means fewer expirations and certificate-related events, which better protects against down sites, financial loss and/or compliance/regulatory penalties."* - (2023)

Why reduced validity?

- It **encourages automation**.

- It **improves security**.
  - reduces the maximum time a certificate can persist for an unauthorized domain.
    - Scenario: A domain owner transfers a domain or lets it expire shortly after obtaining a certificate. They are capable of holding a certificate for the domain for which they are no longer authorized to own for up to 795 days. With a reduced validity period, these certificates will become no longer valid much sooner.
  - reduces the maximum time a private key can be abused*.
    - * this assumes that a new key pair is generated for each renewal, which we observed as commonplace when studying ACME clients.

Why reduced validity?

- **It will reduce CRL size.**
  - Ecosystem participants are moving toward privacy-preserving status checking mechanisms.
  - When considering publicly-trusted serverAuth certificates trusted by Chrome:
    - Certificates with a validity > 90 days represent approximately:
      - 43% of the time-valid certificate population
      - 89% of the time-valid but revoked certificate population
      - 64% of the time-valid but revoked certificate population marked “Key Compromise”
  - Reducing validity means smaller CRLs.
  - Smaller CRLs translates into reduced...
    - latency,
    - timeouts,
    - bandwidth, and
    - operational costs.

Why reduced validity?

- **It will reduce the impact of unexpected CT log retirements.**
  - Reduced certificate validity results in a shorter period where a certificate's use depends upon a particular CT log remaining qualified (i.e., "usable").

Why reduced validity?

- **It can help “repair” revocation.**
  - It’s long been argued that revocation is “broken.”
  - Products tend to fail open to because of...
    - timeouts (*e.g., an OCSP responder/ CRL server is online but does not respond within an acceptable time limit*),
    - availability issues (*e.g., the OCSP responder / CRL server is offline*),
    - invalid responses (*e.g., a “stale” or malformed status response*), and
    - local network attacks (*e.g., an attacker can misroute traffic or block responses*).
  - However, certificate expiration is broadly and reliably enforced across major certificate consumers.
  - When coupled with reduced CRLs and out-of-band revocation tools like “CRLSet”, “CRLite”, or “Valid”, revocation will be more reliable.

Community Perspective (validity)

- *"Short validity period certificates are becoming ever more common to reduce the scope of data compromised if a server vulnerability is uncovered."* - (2019)
- *"Shorter service life of TLS / SSL certificates is due to a stronger focus on security in the industry, and will contribute to faster replacement of outdated technology (eg weak algorithms) and more accurate information in the certificates."* - (2020)
- *"A decrease in certificate lifecycles will reduce ecosystem reliance on revocation, meaning less website down-time and a smaller window of opportunity for threat actors. Additionally, shorter-lived certificates will decrease the impact of unexpected Certificate Transparency Log disqualifications."* - (2023)
- *"Shorter validity periods coupled with automation achieve a higher level of security by reducing the time in which a compromised certificate is usable."* - (2023)
- *"To sum things up, a shorter-term length can lead to improved security around SSL certificates."* - (2020)
- *"The longer between identity validation, the greater the risk."* - (2020)

Feature Launch Roadmap

Platform	Current State (Today)		Future State (Spring 2023, ~Chrome 115)	
	Certificate Verifier	Root Store	Certificate Verifier	Root Store
Android	Chrome Cert Verifier	Chrome Root Store	Chrome Cert Verifier	Chrome Root Store
Chrome OS	Chrome Cert Verifier	Chrome Root Store	Chrome Cert Verifier	Chrome Root Store
iOS	Platform Verifier	Platform Root Store	Platform Verifier	Platform Root Store
Linux	Chrome Cert Verifier	Chrome Root Store	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 Updates

- **Certificate Transparency Policy (https://goo.gl/chrome/ct-policy):**
  - No updates to report.
- **Certificate Transparency Log Policy (https://goo.gl/chrome/ct-log-policy):**
  - No updates to report.
- **Log State Changes:**
  - Nessie 2024 transitioned to **Retired**, with the last 'Qualified' SCT having a timestamp no later than 2023-05-27T00:00:00Z.
  - Non-sharded Google Logs are being transitioned to **Rejected**.

Log List V2 Deprecation

- **Background:**
  - Chrome enforces its CT policy using a curated list of CT logs.
  - The log list is updated through Component Updater.
- **Summary of Upcoming Changes:**
  - The Version 2 log list URL has been deprecated (more information available here.)
- **Action Requested:**
  - **As soon as possible**, CAs should verify they are relying on the Version 3 log list URL to determine the set of logs considered usable in Chrome.

General Browser Updates

PKI-related Changes in Upcoming Releases

- Beginning in **Chrome 114** (May 30, 2023)
  - Chrome Root Store on Linux and Chrome OS
- Beginning in **Chrome 115** (July 18, 2023)
  - Chrome Root Store and Certificate Verifier on Android
- Beginning in **Chrome 116** (August 15, 2023)
  - N/A
- Beginning in **Chrome 117** (September 12, 2023)
  - Lock icon replacement

Contact us at:

chrome-root-program[at]google[dot]com

Policy page at:

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

Appendix

Why? [additional commentary]

- *"We cannot underestimate the impact of not using automation in certificate management."* - (2019)
- *"Equally important is the ability to replace outdated crypto assets without significantly disrupting their system's infrastructure. One of the best ways to achieve this is through automation."* - (2022)
- *"... agrees that shorter lifetimes help enhance the security of the ecosystem and has the tools necessary to help our customers automate the certificate lifecycle process. We support short-lived certificates, with lifetimes as short as a few hours for customers with advanced automation capabilities."* - (2020)
- *"The broadening use of and reliance on TLS server certificates to secure important applications is rendering manual certificate management impractical. Risks such as certificate-related outages are often the result of errors made while manually managing certificates."* - (2020)
- *"Most enterprises are considering PKI automation, with 91% at least discussing it. Only 9% say they are not discussing it and have no plans to do so. Most (70%) expect to implement a solution within 12 months."* - (2021)