

Chrome Root Program

CA/Browser Forum F2F 60

In this update

- 01 Chrome Root Program
- 02 Certificate Transparency
- 03 General Browser News

01

Chrome Root Program Updates



Chrome Root Program

- Modern Infrastructures Survey
- Policy Update
- Feature Launch Roadmap

Modern Infrastructures Survey



Why promote modern infrastructures?

Encryption makes the Internet **more secure**, but only if consistently and reliably deployed.

The adoption of modern infrastructures and practices creates opportunity to enhance consistency and reliability through increased **simplicity** and **agility**.

Reminder: “Moving Forward, Together”

- First introduced at [F2F 55](#)
- **Long-term** initiatives that promote increased speed, security, stability and simplicity
 - Non-normative, **not** policy.
- Feedback is **welcome**
- More information is located [here](#)

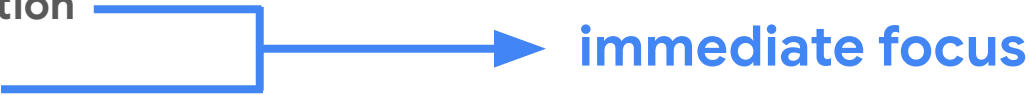
A phased approach (tentative)

- Support for automation
- Term limit for roots
- Establish minimum expectations for linting
- Phase out “multi-purpose” roots
- Phase out clientAuth use cases
- Strengthen domain validation
- Shorter validity period for subCAs
- Shorter validity period for leaf certificates



time

A phased approach (tentative)

- Support for automation
 - Term limit for roots
 - Establish minimum expectations for linting
 - Phase out “multi-purpose” roots
 - Phase out clientAuth use cases
 - Strengthen domain validation
 - Shorter validity period for subCAs
 - Shorter validity period for leaf certificates
-  **immediate focus**

What informs our approach?

- Studying ecosystem data from publicly available tools like crt.sh and [Censys](https://censys.io)
- Interpreting results from Chrome tools, experiments, and usage data
- Evaluating peer-reviewed research
- Collecting feedback through surveys

Survey objective

Understand individual and unique CA Owner perspective of impact related to “Moving Forward, Together” proposals for “modern infrastructures” initiatives (i.e., 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
- **Responses:** 49 of 49 CA Owners included in the Chrome Root Store (**thank you**)

“Please provide any comments you’d like to share...”

47%

of CA Owners provided comments:

47% expressed concern for the proposed root term limit

26% stated “Thank you for providing this questionnaire” or similar

22% expressed a desire for sufficient migration time for proposals that intend to become requirements

Survey results TL;DR

Focus on promoting automation and aspects of modern infrastructures

- Automation = opportunity
- Term limit for roots = risk

Main Findings and Themes



Automation



Why promote automation?

- Focal point of our [F2F 59](#) update
- In summary, we feel automation:
 - promotes **agility**
 - increases **resilience and reliability**
 - increases **efficiency**

Automation Survey Goals

1. What % of CA Owners included in the Chrome Root Store support automation?



76%

...of CA Owners included in the Chrome Root Store stated support for automated solutions

Automation Survey Goals

1. What % of CA Owners included in the Chrome Root Store support automation?
2. What % of “Web PKI” certificates are issued by organizations that support automation?

~99.9%



...of the certificates issued in the Web PKI today are issued by these CA Owners.

[estimated by combining survey responses with publicly available data from [Certificate Transparency](#) logs and tools like [crt.sh](#)]

Automation Survey Goals

1. What % of CA Owners included in the Chrome Root Store support automation?
2. What % of “Web PKI” certificates are issued by organizations that support automation?
3. What % of “Web PKI” certificates are issued using automation?



~82%

...of the certificates issued by the Web PKI today are issued using some form of automation.

[estimated by combining survey responses with publicly available data from [Certificate Transparency](#) logs and tools like [crt.sh](#)]

Conclusions

- Strong and increasing demand for and support of automation
- Broader support for automation will create opportunities for website owners
- There are opportunities to continue improving the ecosystem (availability, features enhancements, user education, etc.)

Term Limits



Why term limits?

- **Benefit from continuous improvement**
 - Baseline Requirements, audit schemes and criteria, and organizational processes continue to improve, and technology continues to advance
- **Encourage agility**
 - Newer root CAs avoids over-reliance and allows the ecosystem to benefit from new standards and security features
- **Reduce risk**
 - The longer a CA exists, the greater the opportunity for abuse (e.g., mishandling of key material, cryptanalysis, unexpected advancements in hardware, etc.)

Term Limit Goals

1. What is the “active certificate signing lifetime” of the certificates included in the Chrome Root Store?”

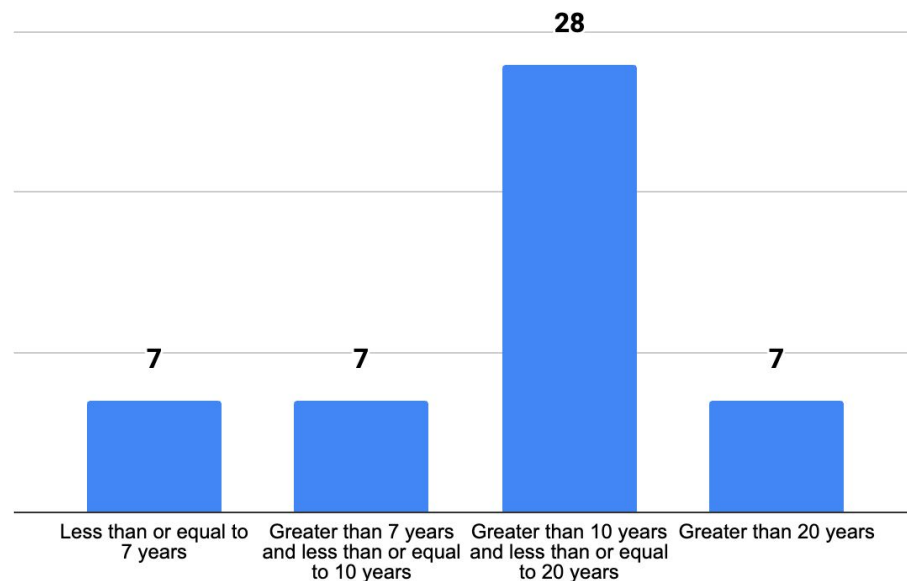
15.05 years



...average “active certificate signing lifetime” reported by CA Owners included in the Chrome Root Store.

Term Limit Goals

1. What is the “active certificate signing lifetime” of the certificates included in the Chrome Root Store?”
2. How would a 7-year term limit impact CA Owners and their customers?



Breakdown of CA Owner responses

Term Limit Goals

1. What is the “active certificate signing lifetime” of the certificates included in the Chrome Root Store?”
2. How would a 7-year term limit impact CA Owners and their customers?



86%

A horizontal progress bar is located below the percentage. It is divided into four segments: blue, red, yellow, and green. The blue segment is the longest, followed by red, yellow, and green.

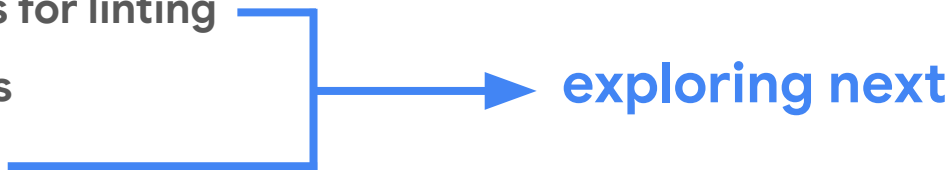
...of CA Owners included in the Chrome Root Store reported an “active certificate signing lifetime” of **greater than 7 years**

Conclusions

- CA Owners expressed concern with our proposed root CA term limit and we plan to adjust
- We'd still prefer a more agile approach
 - Recent ecosystem improvements will help (e.g., Chrome Root Store launch)
 - Opportunity for innovation (e.g., trust anchor negotiation)
 - We may explore this further in the future

What's next? (tentative)

- Support for automation
- Term limit for roots
- **Establish minimum expectations for linting**
- **Phase out “multi-purpose” roots**
- **Phase out clientAuth use cases**
- Strengthen domain validation
- Shorter validity period for subCAs
- Shorter validity period for leaf certificates




exploring next

What to expect

- future survey(s) allowing CA Owners to share, or further clarify known use cases and expected impact
- requirements (that, *if* drafted) attempt to:
 - minimize unintended impact
 - allow stakeholders time to prepare for and respond to changes
- studying trade-offs and evaluating impact will take time
 - for example, our first survey on automation landed in December 2022; however, our policy has not yet included any effective normative requirements related to its use

What about leaf validity?

- Support for automation
- Term limit for roots
- Sunset “multi-purpose” roots
- Sunset clientAuth
- Strengthen domain validation
- Shorter validity period for subCAs
- **Shorter validity period for leaf certificates**  **long-term goal**

Policy



Version 1.5, Coming Soon!

The draft CRP policy Version 1.5 will be shared with CA Owners to provide the opportunity to seek clarification before the update becomes effective.

- **How:** CCADB message with embedded draft Doc and feedback Sheet.
- **Pre-flight Window:** ~October 9, 2023 to October 27, 2023.

What to expect

Updates include, but are not limited to:

- incorporated CA Owner feedback in response to policy Version 1.4 (clean-ups and clarifications throughout the policy)
- added new subsections for Root CA Key Material Freshness, Automation Support, and the Root CA Term-Limit
- aligned incident reporting format and timelines with CCADB.org

What to expect

- added new subsections for Root CA Key Material Freshness, Automation Support, and the Root CA Term-Limit

What to expect

- added new subsections for Root CA Key Material Freshness, Automation Support, and the Root CA Term-Limit

Clarified: applicants to submit documented evidence of adherence to Sections 6.1.1 and 6.2 of the Baseline Requirements

Clarified: applicants to submit documented evidence of protection aligned with Section 6.2 for keys not used to issue a self-signed root CA certificate on the same day it was generated

Root CA Key Material Freshness, Automation Support, and

the Root CA Term-Limit

What to expect

- added new subsections for Root CA Key Material Freshness, Automation Support, and the Root CA Term-Limit

New: effective January 15, 2024 the Chrome Root Program will only accept CCADB “Root Inclusion Requests” from Applicant PKI hierarchies that support an automated solution for certificate issuance and renewal

Applicant PKI hierarchies:

- **SHOULD** support the ACME protocol
- **MAY** support other automated solutions
- are **NOT** prohibited from supporting “non-automated” methods of certificate issuance and renewal

What to expect

- added new subsections for Root CA Key Material Freshness, Automation Support, and the Root CA Term-Limit

New: effective January 15, 2024, any root CA certificate with corresponding key material generated more than **15 years** ago will be removed from the Chrome Root Store on an ongoing basis

New: to phase-in these requirements in a manner that reduces negative impact to the ecosystem, affected root CA certificates included in the Chrome Root Store will be removed according to a schedule (detailed in the policy)

Feature Launch Roadmap



Feature Launch Roadmap

Platform	Certificate Verifier & Root Store Enabled by Default
Android	Chrome 115
Chrome OS	Chrome 114
iOS	N/A
Linux	Chrome 114
macOS	Chrome 108
Windows	Chrome 108

Learn more: [here](#)

02

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:**
 - [Several new](#) CT Logs have been approved for inclusion in Chrome, having completed their application and successfully undergone compliance monitoring.

03

General Browser Updates



PQ Key Exchange (Chrome 116)

- TL;DR:
 - Began rolling out X25519Kyber768 support for establishing symmetric secrets
 - This is **not** PQ x.509 support
 - Goals:
 - Immediate: Prevent “harvest now, decrypt later” attacks (*important, urgent*)
 - Future: Determine how PQC fits into the Web PKI (*important, less urgent*)
 - [Enterprise policy](#) (temporarily available)
- Learn more: [here](#)

Contact us at:

[chrome-root-program\[at\]google\[dot\]com](mailto:chrome-root-program@google.com)

Policy page at:

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