Mozilla Root Program Update for the CA/Browser Forum Berlin - October 2022

Link to Previous Mozilla Face-to-Face Briefing (June 2022) - https://cabforum.org/wp-content/uploads/2022-June-Mozilla-Browser-News.pdf

Ben Wilson and Kathleen Wilson
Mozilla Root Store Program Managers

Recap: Mozilla Root Store Policy, v. 2.8

- **June 1, 2022**: Previously unreported qualifications or non-conformities are also considered incidents and must have corresponding Incident Reports filed in Bugzilla - MRSP 2.4; and public review required if a new CA operator will control an unconstrained intermediate certificate that directly or transitively chains to the CA's included certificate(s) - MRSP 8.4
- **July 1, 2022:** Disclose name-constrained intermediate CA certificates in the CCADB when they are capable of issuing working server or email certificates - MRSP 5.3.2
- **Oct. 1, 2022**: Populate the CCADB with either the full CRL or a JSON array of partitioned CRLs that make up the full CRL - MRSP 4.1; a CT precertificate is considered a binding intent to issue a certificate, must be revocable, and is in-scope for purposes of MRSP compliance - MRSP 5.4 ; and CRL Revocation Reason Codes for TLS End-Entity Certificates, specifying which reasons must be used, and when - MRSP 6.1.1.
- **Dec. 31, 2022**: CAs must maintain an online archive of older versions of their CPs and CPSes - MRSP 3.3
- **July 1, 2023**: CAs must not be signing anything using SHA-1 - MRSP 5.1.3

Upcoming changes

https://github.com/mozilla/pkipolicy/issues

- **Phasing in limits on the useful life for existing and new Root CA Certificates** - Mozilla GitHub Issue # 232
- **Requiring CA operators to submit Compliance Self-Assessments annually** - Mozilla GitHub Issue # 240
- **Clarifying requirements for reporting incidents involving CA internal systems** - Mozilla GitHub Issue # 252
- **Requiring Disclosure of TLS Certificates in Certificate Transparency** - Mozilla GitHub Issue # 255
- **Moving toward Discontinuance of OCSP for the Web PKI** - CABF Server Certificate WG, GitHub Issue # 389

Transition to 15-year Root CAs

Key Material Created	Removal of Websites Trust Bit	Distrust for S/MIME After Date
Before 2006	April 15, 2025	April 15, 2028
2006-2007	April 15, 2026	April 15, 2029
2008-2009	April 15, 2027	April 15, 2030
2010-2011	April 15, 2028	April 15, 2031
2012- April 14, 2014	April 15, 2029	April 15, 2032
April 15, 2014 - present	15 years from creation	18 years from creation

Distrust Date:

- For TLS: Websites trust bit will be removed 15 years after CA key creation
- For Email: Mozilla will set “Distrust for S/MIME After Date” to 18 years from CA key creation

CA key creation will be determined by date in auditor-witnessed key generation report.

CA Inclusion Requests

https://wiki.mozilla.org/CA/Dashboard

Status	**Count**
Received - Initial Status (CA hasn’t provided enough information to begin review process)	11
Information Verification (CA is providing additional information, which is being reviewed)	14
Detailed CP/CPS Review (CA’s CP and CPS are being reviewed and updated)	5
Awaiting Public Discussion (CA is in queue for public discussion)	3
In Public Discussion (CA is in period of public review and comment)	0
TOTAL	**33**

Currently Open CA Incidents

https://wiki.mozilla.org/CA/Incident_Dashboard

Types of Incident	Count
CRL/OCSP issues (formatting and invalid responses)	11
Certificate Profiles and linting	9
Delayed response, deployed reporting, delayed revocation	5
Incorrect locality or similar location information	2
CPS/Documentation issues (correctness, timely publication, etc.)	2
Organization data (faulty source, human transcription error)	1
Weak key detection	1
Audit delay	1
TOTAL	**32**

(Working on a plan to improve incident labeling using the whiteboard in Bugzilla, e.g. .)

CRLite Update

- CRLite is a privacy-enhancing, revocation-checking mechanism that uses a Bloom filter cascade and whole-ecosystem analysis of the Web PKI to push the entire web's TLS revocation information to Firefox clients.
- Rolling out with Firefox 107 – November 15, 2022, release
  - Used by Firefox Nightly 102 through 107 without incident
  - Will cover 327 Million TLS Certificates
  - Reliance on OCSP requests, and stapled and cached OCSP will drop
- If CRLite determines the certificate is revoked, we'll double-check using OCSP.
  - We'll fail open if OCSP response is that the certificate is "good".
  - Telemetry will help identify whether mismatches are due to stale OCSP responses or for other reasons.
  - Eventually we will phase out the OCSP double-checking for privacy

Mozilla’s Top Priorities and Goals:

#1 - Keep the web safe for our end users

A fast and secure TLS handshake with a browser URL bar that is easy for end users to understand.

- Public-facing and transparent processes
  - Use knowledge from the community in policy adoption, root inclusion, and problem resolution
  - Continue to update the BRs, policies, and practices as web attack scenarios continue to advance
- Consistent requirements and enforcement for CAs across the globe
  - Vet CAs and monitor them to ensure they do not expose users to risk
  - Share knowledge to prevent repeating mistakes
- Continue to improve automated monitoring and reporting abilities
  - Faster identification and resolution of problems
  - More timely inclusion of root CA certificates based on program priorities
- Hard-fail for revoked TLS certificates without leaking browsing information
  - CRLite, Requiring full CRL information, Revocation Reason Codes – policy/consistency

Contacting Us:

certificates@mozilla.org