Browser News - Mozilla

CA/B Forum F2F
June 2022

Ben Wilson

Link to Previous Mozilla February 2022 Face-to-Face briefing -
https://cabforum.org/wp-content/uploads/CABForum-February2022-Mozilla-Update.pdf

Mozilla Root Store Policy (MRSP) v. 2.8 (effective June 1, 2022)

Recent post to the Mozilla Security Blog about MRSP v. 2.8 -
https://blog.mozilla.org/security/2022/05/23/upgrading-mrsp-to-v-2-8/

CA Survey Results - https://wiki.mozilla.org/CA/Communications#May_2022_Responses

Four CA Operators did not respond to the survey on a timely basis. All have since responded. The following incidents were filed in Bugzilla, and two have filed incident reports so far:

E-Tuğra - https://bugzilla.mozilla.org/show_bug.cgi?id=1772414

eMudhra - https://bugzilla.mozilla.org/show_bug.cgi?id=1772413

iTrusChina - https://bugzilla.mozilla.org/show_bug.cgi?id=1772412

NAVER Cloud - https://bugzilla.mozilla.org/show_bug.cgi?id=1772411

Survey responses -

General - One comment requested that we modify the wiki page "Process for Updating the Root Store Policy" to take into account new CA requirements and provide reasonable time for compliance following official publication.

We will take the request under consideration. However, discussions of changes to the MRSP began in August 2021, and for problematic compliance dates, many accommodations have been made. See Effective Dates: https://wiki.mozilla.org/CA/Root_Store_Policy_Archive#2.8

Online Availability of Certificate Policies (CPs) and Certification Practices Statements (CPSes) -

CA operators indicated that some clarifications are needed:

- The requirement is intended to be for ***all*** historic versions of the CA's CP and CPS documents. I have opened Issue #249 in GitHub to state this more clearly in the next version of the policy.
- Some CAs cannot obtain all older versions of their CPs and CPSes, so the expectation is that they will upload all the versions that they can find, and maintain public access to all versions going forward.
- Some CAs need longer (e.g. until December 31) to upload all older versions of their documents because of other requirements such as the Web Content Accessibility Guidelines (WCAG) – This exception has been added to https://wiki.mozilla.org/CA/Root_Store_Policy_Archive#2.8

Misissuance of Certificate Transparency (CT) Precertificates -

Section 5.4 of the Mozilla Root Store Policy states that while Mozilla does not currently require CT logging, if a precertificate is logged, then the Mozilla community has certain expectations concerning revocation, regardless of whether a final certificate exists. (Beginning in 2019, these expectations were stated in Mozilla's Recommended Practices wiki page. https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#Precertificates.) Several CAs stated that they did not understand the new policy requirements. They questioned, "if a final certificate hasn't been issued, then how can we revoke it?" These comments illustrate a misunderstanding of the issue because the serial number of a precertificate can still be added to the CRL.

The historical reasons for adopting this new section of policy can be found in these discussion threads:

- https://bugzilla.mozilla.org/show_bug.cgi?id=1577014
- https://groups.google.com/g/mozilla.dev.security.policy/c/LC_y8yPDI9Q/m/NbOmVB77AQAJ
- https://www.mail-archive.com/trans@ietf.org/msg03015.html
- https://cabforum.org/2019/11/14/ballot-sc23-v3-precertificates/
- https://github.com/mozilla/pkipolicy/issues/138
- https://groups.google.com/u/1/a/mozilla.org/g/dev-security-policy/c/Co65loD9i-0/m/Trt4N9QQAgAJ

CRL Revocation Reasons for TLS Certificates -

One CA raised concern about cascading requirements with regard to scope of revocation for keyCompromise, so we have added clarification here: https://wiki.mozilla.org/CA/Revocation_Reasons#Scope_of_Revocation

CA Inclusion Requests

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

Status	Count
Received - Initial Status (CA hasn't provided enough information to begin review process)	7
Information Verification (CA is providing additional information, which is being reviewed)	15
Detailed CP/CPS Review (CA's CP and CPS are being reviewed and updated)	6
Waiting Public Discussion (CA is in queue for public discussion)	2
In Public Discussion (CA is in period of public review and comment)	0
TOTAL	**30**

CA Compliance

In addition to the four new incidents mentioned above, at the time this table was created (last week) there were approximately 30 other incidents open in Bugzilla of the following types. https://wiki.mozilla.org/CA/Incident_Dashboard

Type of Incident	Count
OCSP issues (including invalid responses)	7
Certificate Profiles and linting	6
Incorrect locality or similar location information	4
CPS/Documentation issues (correctness, timely publication, etc.)	4
Delayed response, delayed revocation	3
Validation Procedures	3
Organization data (faulty source, human transcription error)	2
Problems with code	1
Audit delay (CPA Canada / WebTrust Seal issue)	1
TOTAL	**31**

CRLite

Improvements continue with CRLite, which is deployed and collecting data in Firefox Nightly and Firefox Beta. To read more, see:
https://blog.mozilla.org/security/2020/12/01/crlite-part-4-infrastructure-design/

Root Store Priorities

Ongoing

1. Keep the web safe for end users, the TLS handshake fast and secure, and the browser URL bar easy for end users to understand
2. Update policies and practices to help protect individuals in the face of an ever-evolving cybersecurity threat landscape
3. Champion public-facing and transparent processes for root inclusions, policy and audit documents, and resolving problems
4. Maintain consistent requirements and enforcement for CAs across the globe
5. Enhance automated monitoring and reporting capabilities

Tactical

1. Hard-fail for revoked end-entity TLS certificates without leaking browsing information.
    - CRLite
    - Requiring full CRL information
    - Revocation Reason Codes – policy/consistency
2. Create policy and process for retiring CA hierarchies that are older than 15 years.
    a. There are 64 root certificates with the Websites trust bit enabled that have Valid From earlier than the first Effective Date of the BRs -- July 1, 2012.
    b. There are 24 root certificates that are more than 15 years old.
    c. Effective dates for policies are in terms of future certificate issuance/action, so very old CA hierarchies may have outdated content, non-compliant hierarchies, or other cruft that only really gets cleaned up by moving to a new CA hierarchy.
3. Encourage all CAs to implement and improve pre-issuance and post-issuance tests to ensure certificates comply with the BRs and prevent mis-issuance.
    a. https://wiki.mozilla.org/CA/Incident_Dashboard

Long Term

- All CAs can rapidly replace certificates
    - Encourage automation (e.g. Automatic Certificate Management Environment (ACME)) that makes it easier and faster for website operators to update their TLS certificates
- Healthy CT log ecosystem with multiple robust log providers

- Reduce maximum TLS certificate validity periods and verification of domain ownership to 3 months or less

Our Email Address

Email: certificates@mozilla.org