CA/B Forum Virtual F2F, June 2020

Browser News - Mozilla

A Mozilla Representation

Ben Wilson has joined Mozilla as a CA Program Manager and CA/Browser Forum representative. Wayne Thayer also continues to represent Mozilla with the Forum in a volunteer capacity.

B Inclusion Request Status

There are about 45 CAs in one stage or another in the root inclusion process

- https://wiki.mozilla.org/CA/Dashboard
- Kathleen is approximately 5 months behind on reviewing CA updates to root inclusion requests in the Information Verification phase,[1] but is starting to work on this again.
- Ben has begun performing detailed reviews of the policy and audit documents for CAs in the Detailed Review phase,[2] some CAs in this phase have been waiting for a year for their detailed review.
- The delays were due to Mozilla resource constraints that have now been resolved, but it will take a while to catch up.

[1] https://wiki.mozilla.org/CA/Application_Verification#Information_Verification
[2] https://wiki.mozilla.org/CA/Application_Verification#Detailed_Review

C CA Compliance Bugs in Bugzilla

Prompt and thorough communication is always important. Mozilla expects CAs to provide an initial response/report as soon as possible, and then follow up with an incident report as soon as the incident has been "diagnosed and (temporary or permanent) measures have been put in place," but "certainly within two weeks of the initial issue report".[3] Thorough communication especially requires detailed responses to items 6 and 7 of the "Incident Report" template. Ask and answer the whys, whats, hows, and whens, then identify and disclose systemic issues and root cause(s) and provide a detailed timeline of remediation tasks.[4]

Communicate status updates frequently. A bug's "whiteboard" entry will indicate whether a "next update" has been set (e.g. [ca-compliance] - Next Update - 1-June 2020), then it is expected that action will be taken by the CA and that an updated status will be reported by then, or sooner. If no "next update" is listed, then the CA is expected to provide a weekly status update (e.g. Chunghwa Telecom's weekly updates[5]). If resolution will be delayed due to mandated restrictions regarding COVID-19, use Whiteboard = [ca-compliance][covid-19]. [6]

[3] https://wiki.mozilla.org/CA/Responding_To_An_Incident

[4] Filing a Compliance Bug: https://bugzilla.mozilla.org/enter_bug.cgi?product=NSS&component=CA%20Certificate%20Compliance&version=other
[5] https://bugzilla.mozilla.org/show_bug.cgi?id=1532436
[6] E.g. https://wiki.mozilla.org/CA/Audit_Statements#Audit_Delay

D Root Store Policy

We plan to update Mozilla's Root Store Policy this summer. Items to be considered are in GitHub with the 2.7.1 label.[7] Discussion will happen in the mozilla.dev.security.policy forum.

[7] https://github.com/mozilla/pkipolicy/issues?q=is%3Aissue+is%3Aopen+label%3A2.7.1

E CA Communication Survey Results

Mozilla sent a communication and survey to all CAs in our program in May with a response deadline of May 31st. We wanted to gauge the impact of COVID-19 on CA implementation of the Root Store Policy and to see where CAs stood with regard to certificate lifetimes and the draft browser alignment ballot. The responses have been published on the CCADB accessible through a Mozilla wiki page.[8] A summary of the responses and, as a result, Mozilla's position with respect to the browser alignment ballot, are available in m.d.s.p.[9]

Mozilla plans to proceed with reducing the re-use timeframe for domain and IP address verification results. While this can go directly into our root store policy, we think it would ideally be part of the BRs so that auditors will add this to their audit criteria. We will soon be drafting and proposing a ballot to accomplish this. To make this transition easier, we encourage all CAs to be working towards automation (for example ACME) of the verification of domain names and IP addresses. Don't wait, as we understand it takes time to migrate customers to new tools.

[8] https://wiki.mozilla.org/CA/Communications#May_2020_Responses
[9] https://groups.google.com/forum/#!msg/mozilla.dev.security.policy/J9IC3FgRatw/nNH9KRW3AQAJ

F Distrust After

Enforcement of distrust-after dates (NSS CKA_NSS_SERVER_DISTRUST_AFTER) has been implemented in Firefox Beta (Firefox 78 to be released 30-June-2020[10]). This makes it easier for Mozilla to distrust certificates issued after a particular 'valid from' date and chaining to a particular root. Distrust-after dates have been set for a few root certs as previously discussed with the affected CAs[11].

[10] https://wiki.mozilla.org/Release_Management/Calendar
[11] Symantec - https://bugzilla.mozilla.org/show_bug.cgi?id=1618404 and others https://bugzilla.mozilla.org/show_bug.cgi?id=1621159

G TLS 1.0 and 1.1 Deprecation

The default version of TLS is set to 1.2 in Firefox Beta (Firefox 78). There is an override button on the error page that will allow users to revert to an earlier version if needed. See e.g. https://tls-v1-0.badssl.com:1010/. Over time, based on telemetry and beta testing, the override button will be removed.

H Intermediate Preloading

Intermediate Preloading[12] was enabled in Firefox 75, which was released in April. Our Intermediate Preloading feature consists of preloading all intermediate CAs known to the Mozilla Root Program into users' profiles. This feature is intended to resolve missing intermediate errors without the privacy compromise of AIA-fetching, and to ensure that Firefox only trusts intermediates which have been disclosed by CAs.

[12] https://wiki.mozilla.org/Security/CryptoEngineering/Intermediate_Preloading

I CRLite

CRLite is enabled in Firefox Nightly and Beta for gathering telemetry, but not yet used to enforce revocation checks. CRLite pushes end-entity revocation information to clients, allowing clients to do revocation checking in a fast and private way. Please refer to the series of Mozilla Security Blog posts,[13] and Thyla van der Merwe's presentation at the Real World Crypto conference[14] for more information.

[13] https://blog.mozilla.org/security/tag/crlite/
[14] https://totalwebcasting.com/view/?func=VOFF&id=columbia&date=2020-01-08&seq=1