Browser News - Mozilla

CA/B Forum Virtual F2F
March 2021

Ben Wilson

PDF Link to Previous October 2020 Face-to-Face briefing - https://cabforum.org/wp-content/uploads/13.CAB-Forum-October-2020-Mozilla-Update.pdf

A Root Store Policy

Over the last several months we have been working to finalize version 2.7.1 of the Mozilla Root Store Policy (MRSP). This is tracked in GitHub, and discussions have been held on the mozilla.dev.security.policy list. As mentioned at the last Face-to-Face meeting in October, proposed changes are indicated in GitHub with the 2.7.1 label and are also tracked in this GitHub redline - https://github.com/mozilla/pkipolicy/compare/master...BenWilson-Mozilla:2.7.1. (Future proposed changes have now been flagged with the 2.8 label.) We expect to be done with the comment process soon, and we will also be publishing CA communication and a survey pertaining to version 2.7.1 of the MRSP. We are targeting to have this done before June 30, 2021.

B CA Inclusion Requests

Prioritization

Ben Wilson has been working to refine the inclusion process and to establish a set of criteria to use when prioritizing work on root inclusion requests. The prioritization scale will use levels P1 through P5 under the "Priority" category for each inclusion request in Bugzilla.

Criteria will include, but not be limited to:

- compliance history,
- existing CA root replacements,
- responsiveness,
- single-purpose roots,
- CA hierarchy control,
- completeness,
- enablement-only, and
- CPS quality.

CA Inclusion Queue

There are about 35 active CA applications that are in the root inclusion process - https://wiki.mozilla.org/CA/Dashboard and https://wiki.mozilla.org/CA/Application_Process

Ben is reviewing CAs in the information verification and detailed review phases, and leading the public discussion phase:

Initial Phase - 5 CAs

- Initial request received - 4 (D-Trust, Sudan, DigitalSign, Sri Lanka, HARICA)

Information Verification Phase - 17 CAs

- Updating information in the CCADB - 4 (SERPRO, LawTrust, Byte, MSC Trustgate)
- Amending CPS - 5 (SISP, Thailand, Notarius, Post Signum, Cybertrust Japan)
- Test websites - 2 (SECOM, Pos Digicert)
- Waiting for Mozilla to conduct more verification - 3 (Fina, ACIN, Macao Post)
- Unresponsive - 1 (Certisign)
- On Hold - 2 (Athex, OATI)

Detailed Review Phase - 13 CAs

- Amending CPS - 2 (Google Trust Services, UAE/Dubai)
- Awaiting CPS Review - 9 (iTrus China, TunTrust, Asseco/Certum. NetLock, Web.com, Firmaprofesional, Telia, HARICA, BJCA)
- Final review before public discussion phase - 2 (Chunghwa Telecom, ANF)

As noted above, nine CAs in the Detailed Review Phase are waiting for their CPSes to be reviewed. There is also a backlog of CAs that will need to be queued up for public discussion. Ben will be spending more time working on CAs in the detailed review phase to get more of them into the public discussion phase.

Completed Public Discussions

Naver Cloud - NAVER Global Root Certification Authority (Completed)

FNMT - AC RAIZ FNMT-RCM SERVIDORES SEGUROS

GlobalSign - GlobalSign Root R46/E46 and GlobalSign Secure Mail Root R45/E45

e-commerce monitoring - GLOBAL TRUST 2020 Root

C CA Compliance

Camerfirma

From December 2020 through January 2021, we reviewed the Bugzilla case history of Camerfirma's compliance issues, and we held public discussions about continued trust in Camerfirma's operations as a publicly trusted CA. We concluded that it was in the best interests of our users to distrust the server certificates issued by Camerfirma's Chambers of Commerce Root - 2008 and its Global Chambersign Root - 2008. Camerfirma's older root certificates (which only had the Email trust bit enabled) are being phased out with a "Distrust After" date of March 1, 2021. See https://groups.google.com/g/mozilla.dev.security.policy/c/PnAAWnxyosM/m/cImb78jnBAAJ.

Kathleen filed https://bugzilla.mozilla.org/show_bug.cgi?id=1692094 to turn off the websites trust bit for Camerfirma's 2008 root certs (as of Firefox 88) and to set the "Distrust for S/MIME After Date" for the older root certificates as of March 1, 2021. Firefox 88 is currently in Nightly and will be released on or about April 20, 2021.

A new bug was created to store documents submitted by Camerfirma related to their continued trust by Mozilla. https://bugzilla.mozilla.org/show_bug.cgi?id=1693113

Compliance Bugs

Approximately 90 CA compliance bugs were closed between 1-October-2020 and 1-March-2021. We currently have about 65 CA compliance bugs open in Bugzilla. They fall into the following general categories:

Audit Issues: (1) not including all intermediate CAs "capable of issuing server certificates" in the audit scope and (2) delayed audit results.

Awareness, interpretation, and implementation of requirements: (1) certificate profile errors, (2) misinterpretation, and (3) lack of policy awareness.

Certificate Contents: (1) incorrect EV business categories, (2) validity periods greater than 398 days, (3) lack of or misapplication of CA/Browser Forum OIDs, (4) wrong key usage or algorithm, (5) lack of pre-issuance compliance checking (linting), and (6) locality, state/province, postal code errors.

Communication: (1) delayed response to certificate problem reports, (2) delayed incident reporting (including delayed preliminary reporting), and (3) failure to update CPSes.

Delayed Revocation: (1) customer disruption and (2) system or process errors.

Domain Validation: (1) non-FQDNs/internal names and (2) failure to perform Domain Validation.

System, process and operational issues: (1) DNS outage, (2) OCSP service patching (human error), (3) OCSP publishing, (4) formatting of OCSP responses, and (5) software bugs/gremlins.

D CRLite, OneCRL and Intermediate Preloading

Intermediate CA certificates are being preloaded from the CCADB into Firefox via our Remote Settings infrastructure (https://wiki.mozilla.org/Firefox/RemoteSettings), which also supports OneCRL and CRLite.

We published another blog post on CRLite in December on the Design of the CRLite Infrastructure. CRLite is still gathering telemetry, but not yet used to enforce revocation checks. Work to improve CRLite is currently on hold until we can backfill for our 2 NSS engineers who recently left Mozilla for other opportunities. Here is a previous job listing for a Staff Cryptography Engineer to support work on the NSS security library. Contact me or Kathleen if you have any recommendations.

E Root Store Data

We are now publishing Mozilla's root store in a way that is easy to consume by others, and added data-usage terms. Mozilla's root store data can be found via new links in https://wiki.mozilla.org/CA/Included_Certificates which are made available via Common CA Database (CCADB) reports.

F eIDAS

In October 2020, we published a blog post explaining our response to the European Commission on its survey and public consultation regarding the eIDAS regulation, advocating for an interpretation of eIDAS that is better for user security and retains innovation and interoperability of the global Internet.

G Feedback on RSASSA-PSS (RSA Probabilistic Signature Scheme)

Looking for input on RSASSA-PSS.
What are the benefits of RSASSA-PSS?
Do CAs have plans to implement RSASSA-PSS?

Email: certificates@mozilla.org