Browser News - Mozilla

CA/B Forum Virtual F2F
October 2021

Ben Wilson

Link to Previous June 2021 Face-to-Face briefing - https://docs.google.com/document/d/1RFAsizaxCYQCgjXGcLXzwlyT_4veXuic59jK1fhcOz0/preview

A Root Store Policy 2.8 and Wiki Updates

There are 62 open issues in GitHub concerning the Mozilla Root Store Policy. We have identified 22 of these that we would like to address in version 2.8 of the MRSP. See MDSP email of 1-October-2021.

We've published a draft "Process for Considering Externally Operated Subordinate CAs". We will soon revise it and re-circulate it on the Mozilla Dev-Security-Policy list. (GitHub Issue #233)

Subordinate CAs / Trust Transfer

#195 - Require public discussion when an external third party receives a new subCA

#230 - MRSP section 8 will read, "CAs SHALL NOT assume that trust is transferable"

#229 - Require disclosure of Technically Constrained Sub-CAs in the CCADB

#228 - Clarify language regarding use of EKUs with Technically Constrained Sub-CAs

Document Improvements

#131 - Replace "CA" with "CA Operator" when referring to an organization and make lists more consistent (semicolons, "and" or "or", and bullets and numbering).

#227 - Clarify Meaning of "CP/CPS"

#184 - Change Terminology from "SSL" to "TLS"

#198 - Outline Policy Update Process in MRSP

#138 - Make it clear that RFC6962 pre-certificates are covered by Mozilla policy. Mozilla considers pre-certificates to be a binding intent to issue as described in the RFC, and thus in-scope for our policy.

S/MIME Certificates

#178 - Sunset SHA-1. Set a date after which SHA-1 may no longer be issued for S/MIME or other signing operations. Question: Where is SHA-1 still being used effectively?

#95 - Require CAs to reject keys in certificates which are revoked for keyCompromise. (SC35 already handled this case for server authentication certificates, but this would be for S/MIME certificates, too.)

CRLs

#226 - Clarify certificate and CRL profile items (AKIs) in MRSP sections 5.2, 6, and elsewhere. See MDSP Discussion.

#234 - Add Policy about CRL Revocation Reason Codes, mainly to flag revocations due to key compromise, but also to mark revocations based on other reasons.

#218 – Required CRL distribution information in the CCADB and otherwise improve Mozilla's statements of policy on CRLs.

#235 - Add Policy requiring Full CRLs (or equivalent JSON array) be disclosed in CCADB for CRLite

Audits and Auditors

#155 - Describe actions Mozilla may take upon receipt of a qualified audit

#219 - Require ETSI auditors to be members of ACAB'c

Additional Requirements of CAs

#232 - Add Policy about removal of old Root CA certificates. See current listing of 131 roots enabled for TLS/SSL Server certificate issuance. And see discussions here - CA Survey Item 8 and Item 8 Timelines.

#185 - Require CA to maintain availability of previous CA policy documents applicable to CA certificate hierarchies that are currently included in the Mozilla root program.

#129 - Require non-discriminatory CA conduct (i.e. CAs should not DoS or censor websites by arbitrarily revoking certificates or by refusing to issue certificates).

B CA Inclusion Requests

The BR Self-Assessment has been renamed the Compliance Self-Assessment. It now references the Mozilla Root Store Policy and the EV Guidelines, in addition to the Baseline Requirements. And adds a column for the Detailed Root Program Review, so that both the CA self assessment and the detailed CP/CPS review results may be seen in one place.

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)	19
Detailed CP/CPS Review (CA's CP and CPS are being reviewed and updated)	9
Waiting Public Discussion (CA is in queue for public discussion)	3
In Public Discussion (CA is in period of public review and comment)	3
TOTAL	**41**

C CA Compliance

Compliance Bugs

Approximately 130 CA compliance bugs were opened between 1-January-2021 and 30-September-2021, and we currently have about 50 of these open. (There is some overlap between this report and the last one given during F2F 53.) The 130 CA compliance bugs fall into the following general categories:

Anticipated audit report delay (4 incidents) Because of COVID-19 or other reasons, the auditor has advised the CA that it expects that the audit report will be delayed.

Missing CAs in Audit/CCADB (9 incidents) CAs conduct manual / visual inspections and comparison of the CAs that are supposed to be included in the audit report, and some are missed. CAs do not realize that BR audits need to include CAs that are "capable of" server certificate issuance, or that EV audits need to include CAs that are "capable of" EV certificate issuance. CAs involved with cross-signing CA certificates are confused about who is responsible for including the certificate in which audit.

CA Misissuance (6 incidents) caused by CA process failures, which have omitted: the CABF certificate policy OIDs in intermediate CAs, or the digitalSignature key usage bit needed for direct OCSP signing by the CA.

Delayed CA Revocation (4 incidents) Usually because key customers will be affected. The reason is usually for a non-TLS-server use case (e.g. the CA supports client authentication, digital signing, government IDs, etc.)

CRL/OCSP Issues (10 incidents) CRL system creates CRLs with one extra second. CRL system developed in-house with faulty signature process. OCSP responses out of date because alerting system failed. OCSP responds with “unknown” status.

Validity Period (4 incidents) CA system creates certificates with one extra second. Forward-dating certificates because certificate replacement process could not credit days on renewed certificates.

Domain Control Validation (DCV) Errors (4 incidents) Faulty DCV procedures or systems that allowed misissuance (e.g. DCV reuse past allowed timeframes, test certificates issued from trusted CA during QA processes, etc.).

Delayed Responses /Revocation Leaf (13 incidents) Failure to timely respond to revocation requests and to revoke within 24 hours.

CPS Outdated and Other Documentation Issues (16 incidents) CAs need to remove forbidden domain validation methods, etc.

OV/EV Validation Practices (4 incidents) The Validation Specialist role needs to be adequately defined as a trusted role. Two-person, dual validation controls are needed when issuing EV certificates.

O/OU field (5 incidents) DV certificates with “O” field. Mojibake in certificate Subject fields. Pre-populated “O” field using CSR content before processing by Validation Specialists.

Keys (8 incidents) RSA keys where modulus is not divisible by 8. Elliptic curve certificates with keyEncipherment keyUsage bit instead of keyAgreement.

FQDN/commonName (10 incidents) commonName not in SAN. Multiple commonNames in certificate. SAN is not an FQDN. FQDN is malformed. EV wildcard.

Wrong EV entity category, mismatch between registration number and Jurisdiction of Incorporation, etc. (10 incidents) Certificates listed dates of incorporation even though registration numbers were available. Legacy code truncated registration numbers at 25 characters. Mismatch detected between information source (QGIS) and registration number.

Location values (16 incidents) Lack of data validation function during input. Wrong localityName, invalid stateOrProvinceName and localityName pair, misspellings, postalCode with 0000, etc.

Leaf Certificate Policy OIDs (4 incidents) Missing or incorrect CABF OIDs in leaf certificates.

Test Websites (4 incidents) Certificates loaded on websites to test valid and revoked certificates have expired. Revoked test website was not using a revoked certificate.

D Other News

CRLite - Mozilla is moving forward with CRLite, so we need to get full CRL information for TLS certificates. CRLite currently determines the CRL URIs based on the certificates in CT, but the BRs do not require cRLDistributionPoints to be present in end-entity TLS certificates. So until CAs are required to provide full CRLs (or JSON equivalent) in the CCADB and CRLite is updated to use those CRLs, CRLite will not know about **all** end-entity TLS certificate revocations. (reference: section 7.1.2.3 of the BRs) Therefore, as part of version 2.8 of Mozilla's Root Store Policy, we intend to add the requirement that in the CCADB intermediate certificate records either have the "Full CRL Issued By This CA" or "JSON Array of Partitioned CRLs" filled in.

Firefox 90 updates included:

- Making Client Certificates Available By Default (automatically find and offer to use client authentication certificates provided by the operating system on macOS and Windows)
- Stopping FTP support
- Supporting Fetch Metadata Request Headers
- SmartBlock 2.0 for Private Browsing (enables use of third-party Facebook login buttons)

Firefox 91 updates included:

- HTTPS by Default in Private Browsing
- Enhanced Cookie Clearing (lets you fully erase your browser history for any website)

Firefox 93 updates included:

- Disabled 3DES

Open Policy and Advocacy - Mozilla's netpolicy blog on open Internet policy initiatives and developments, contains an article about Mozilla's recommendations for the EU Digital Markets Act (DMA).

E Our Email Address

Email: certificates@mozilla.org