Browser News - Mozilla

CA/B Forum F2F
February 2022

Ben Wilson

Link to Previous Mozilla October 2021 Face-to-Face briefing -
https://cabforum.org/wp-content/uploads/cab_forum_october_2021_-_mozilla_update.pdf

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

https://github.com/mozilla/pkipolicy/compare/master...BenWilson-Mozilla:2.8

If you have any issues, now is the time to participate in the discussions:
https://groups.google.com/a/mozilla.org/g/dev-security-policy

Effective Dates in the draft of v2.8:

- **July 1, 2022**
  - **Name-constrained intermediate certificates** capable of issuing working server or email certificates that were exempt from disclosure in previous versions of the MRSP **MUST be disclosed in the CCADB** prior to July 1, 2022 (Apple's deadline is April 1, 2022).
  - S/MIME certificates cannot be signed using SHA1 (Apple's deadline is April 1, 2022).
- **October 1, 2022**
  - Revocations that are performed after October 1, 2022, must follow the **new policy about which revocation reason codes to use for TLS end-entity certificates**. Revocation entries that appeared on a CRL prior to October 1, 2022, do NOT need to be changed as a result of the new policy.
  - CA operators with **intermediate CA certificates** that are capable of issuing TLS certificates chaining up to root certificates in Mozilla's root store SHALL **populate the CCADB fields for CRLs under "Pertaining to Certificates Issued by This CA"** with either the CRL Distribution Point for the "Full CRL Issued By This CA" or a "JSON Array of Partitioned CRLs" (Apple's deadline is the same, but Apple is requiring this for all intermediate CAs).
- **July 1, 2023**
  - **All certificates (including OCSP responders), CRLs (including ARLs), and OCSP responses cannot be signed using SHA1.**

Document Improvements

- “CA Operator” replaces “CA” when referring to an organization.
- The term "CP/CPS" has been replaced with the separate terms “CP”, “CPS”, and “combined CP/CPS”.
- “TLS” has replaced “SSL”
- Words having a special “requirement meaning” per RFC 2119 (e.g. “SHALL”) are now in ALL CAPS
- Other editorial changes (lists, punctuation, etc.)

Intermediate CAs: Technical Constraints, EKUs, Public Discussion, and Trust Transfer

- In MRSP section 5.3.1, we’ve added the sentence bolded below:

  For an intermediate certificate to be considered technically constrained, the certificate MUST include an Extended Key Usage extension specifying the extended key usage(s) allowed for the type of end entity certificates that the intermediate CA is authorized to issue. **We also encourage CAs to include only a single KeyPurposeID in the EKU extension of intermediate certificates.**

- We have clarified the language regarding the use of EKUs for SMIME Technically Constrained intermediate CAs by adding the text bolded below to the end of section 5.3.1:

  If the intermediate CA certificate includes the id-kp-emailProtection extended key usage, then to be considered technically constrained, it MUST include the Name Constraints X.509v3 extension with constraints on rfc822Name, with at least one name in permittedSubtrees, each such name having its ownership validated according to section 3.2.2.4 of the Baseline Requirements. **The values id-kp-serverAuth and anyExtendedKeyUsage MUST NOT be present. id-kp-clientAuth MAY be present. Other values that the CA is allowed to use and are documented in the CA’s CP, CPS, or combined CP/CPS MAY be present.**

- As mentioned above, we have reorganized MRSP section 5.3.2 and also clarified that name-constrained intermediate certificates capable of issuing working server or email certificates MUST be disclosed in the CCADB (new language in bold):

  The operator of a CA certificate trusted in Mozilla’s CA Certificate Program MUST publicly disclose in the CCADB all CA certificates they issue that chain up to that CA certificate trusted in Mozilla’s CA Certificate Program that are technically capable of issuing working server or email certificates, including those CA certificates that share the same key pair whether they are self-signed, doppelgänger, reissued, cross-signed, or other roots. The CA with a certificate included in Mozilla’s root program MUST disclose such CA certificate within one week of certificate creation, and before any such CA is allowed to issue certificates. **Name-constrained CA certificates that are technically capable of issuing working server or email certificates that**

were exempt from disclosure in previous versions of this policy MUST be disclosed in the CCADB prior to July 1, 2022.

- MRSP § 8 is modified to read, "CA operators **SHALL** NOT assume that trust is transferable."
- Also in section 8, we have clarified the process for **public discussion when an external third party will receive an unconstrained subordinate CA or cross-certificate** by including a cross-reference to the following new wiki page: **https://wiki.mozilla.org/CA/External_Sub_CAs_not_Technically_Constrained**

CT Precertificates

We are moving language from the wiki page discussing Certificate Transparency into the MRSP. While Mozilla does not require the publication of precertificates for purposes of Certificate Transparency, **we're adding a new section 5.4 called "Precertificates"**, which says:

> Certificate Transparency precertificates are considered by Mozilla to be a binding intent to issue a certificate, as described in section 3.2.1 of RFC 9162, and thus in-scope for enforcing compliance with these requirements. Thus,
>
> * if any certificates with the same serial number and issuer exist, and one cannot be verified as the precertificate matching the final certificate using the algorithms in RFC 9162, this will be considered misissuance;
>
> * issuance of a precertificate that does not comply with this policy is considered equal to misissuance of a final certificate;
>
> * a CA must be able to revoke a certificate presumed to exist, if revocation of the certificate is required under this policy, even if the final certificate does not actually exist; **and**
>
> * a CA must provide CRL and OCSP services and responses in accordance with this policy for all certificates presumed to exist based on the presence of a precertificate, even if the certificate does not actually exist.

Forbidden Practices

We have cleaned up the list of certificate formatting problems in MRSP section 5.2 and split it into two lists (to include CRL and OCSP response issues) so that it now reads:

> CAs MUST NOT issue certificates, **CRLs, or OCSP responses**, that have:
> * ASN.1 DER encoding errors;
> * invalid public keys (e.g., RSA certificates with public exponent equal to 1); **or**
> * missing or incorrect extensions (e.g., **TLS certificates with no subjectAltName extension, delegated OCSP responders without the id-pkix-ocsp-nocheck extension, partial/scoped CRLs that lack a distributionPoint in a critical issuingDistributionPoint extension**).

CAs MUST NOT issue certificates that have:

* duplicate issuer names and serial numbers (except that a Certificate Transparency pre-certificate is allowed to match the corresponding certificate); **or**
* cRLDistributionPoints or OCSP authorityInfoAccess extensions for which no operational CRL or OCSP service exists.

CRLs

As mentioned above, we're addressing Issue #234 by adding a section that specifies which CRL Revocation Reason Codes can be used for TLS end-entity certificates. See draft at https://docs.google.com/document/d/1ESakR4MiwyENyuLefyH2wG8rYbtnmG1xeSYvDNpS-EI

Also, as already mentioned above, MRSP section 4.1 will state, "Effective October 1, 2022, CA operators with intermediate CA certificates that are capable of issuing TLS certificates chaining up to root certificates in Mozilla's root store SHALL populate the CCADB fields under "Pertaining to Certificates Issued by This CA" with either the CRL Distribution Point for the "Full CRL Issued By This CA" or a "JSON Array of Partitioned CRLs"."

Audits and Auditors

In Section 2.4 Incidents, we've added the following language, indicated in bold:

> When a CA operator fails to comply with any requirement of this policy - whether it be a misissuance, a procedural or operational issue, or any other variety of non-compliance - the event is classified as an incident and MUST be reported to Mozilla as soon as the CA operator is made aware. At a minimum, CA operators MUST promptly report all incidents to Mozilla in the form of an Incident Report. **Any matter documented in an audit as a qualification, a modified opinion, or a non-conformity is also considered an incident and MUST have a corresponding Incident Report.** CA operators MUST regularly update the Incident Report until the corresponding bug is marked as resolved in the mozilla.org Bugzilla system by a Mozilla representative. CAs SHOULD cease issuance until the problem has been prevented from reoccurring.
>
> **Mozilla expects the timely remediation of the problems that caused or gave rise to the incident. In response to incidents, Mozilla MAY require the CA operator to submit a plan of action with milestones or to submit one or more additional audits to provide sufficient assurance that the incident has been remediated. Such audits MAY be expected sooner than the CA operator's next scheduled audit, and thus MAY be expected to be for a period less than a year.**

Then, in Section 3.1.4, we've also added, "**If Mozilla determines that an audit provided does not meet the requirements of this policy, then Mozilla MAY require CA operators to obtain a new audit, at the CA operator's expense, for the period of time in question. Additionally, depending on the nature of concerns with the audit, Mozilla MAY require that the CA operator obtain such an audit from a new auditor.**"

We are also considering adding to Section 3.2: “ETSI auditors MUST be members of the Accredited Conformity Assessment Bodies' Council. WebTrust auditors MUST be enrolled by CPA Canada in the WebTrust for Certification Authorities program.”

Maintaining Access to Older CPs and CPSes

We are adding a new item # 7 to MRSP Section 3.3:

> “7. CAs SHALL maintain links to older versions of each CP and CPS (or CP/CPS) until all root CA certificate hierarchies operated in accordance with such documents are no longer trusted in the Mozilla root program.”

Sunsetting SHA-1

We are updating section 5.1.3 to set dates after which SHA-1 may no longer be used to sign S/MIME certificates (7/1/2022) or for other signing operations (7/1/2023).

Removing Old Roots

We continue working on a plan and criteria for removing older Root CA certificates. See current listing of roots enabled to support issuance of TLS Server certificates. And see discussions here - CA Survey Item 8, Item 8 Timelines, Github Issue # 232, and here: https://groups.google.com/a/mozilla.org/g/dev-security-policy/c/PuI1ZILqZ7o/m/E-cKaw_jBAAJ.

B CA Inclusion Requests

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

Status	Count
Received - Initial Status (CA hasn’t provided enough information to begin review process)	8
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)	10
Waiting Public Discussion (CA is in queue for public discussion)	0
In Public Discussion (CA is in period of public review and comment)	1
TOTAL	**33**

C CA Compliance

Compliance Bugs

There are about 25 compliance bugs currently open and about 50 compliance incidents reported since October 1, 2021. Here are some of the categories that they fall under:

Problem / Type of Incident	**Count**
CRL/OCSP one second beyond stated validity period	7
Delayed leaf revocations and delayed response to problem report (manual checking of email, etc.)	6
Certificate content errors (OU field, address fields, JOI, and locality), some caused by manual inputting or visual comparison of values	6
Domain validation - erroneous email addresses used, delayed sunsetting of DV methods, and implementation issues with ALPN validation method (TLS version, challenge certificate contents)	5
Domain name issues (Disallowed LDH labels in domain names, hostnames not in preferred name syntax)	3
System development, coding issues, old code, code complexity, bugs not detected during code review, and certificate profile issues	3
Subordinate CA misissuance (notAfter date of certificate beyond notAfter date of issuer and wrong EKU encoding)	2
System unavailability (e.g. expired root led to atypical DNS routing and high traffic volume, OCSP outage)	2
Document reuse beyond 398 days	2
CP/CPS inaccuracy, CPS out-of-date, or undisclosed EV sources	2
Subordinate CA unrevocation	1
Non-NIST curves	1

D CRLite

Mozilla continues to improve CRLite. In Firefox 99, currently planned for release on April 5, 2022, we are planning to turn on CRLite in a monitoring mode (about:config → security.pki.crlite_mode = 1). We are also implementing a mode that will double-check a CRLite “revoked” result with OCSP. This mode will give users most of the performance and privacy benefits of CRLite while eliminating the risk of being blocked for a false positive. We will also be collecting telemetry about when CRLite and OCSP differ in this mode.

E Our Email Address

Email: certificates@mozilla.org