Mozilla News

CA/B Forum F2F, Meeting 64 in Tokyo, Japan
March 25, 2025

Ben Wilson

Link to Previous Mozilla October 2024 Face-to-Face briefing -
https://cabforum.org/2024/10/08/minutes-of-the-f2f-63-meeting-in-seattle-wa-usa-october-8-10-2024/5-October-2024-Mozilla-News.pdf

Mozilla Root Store Policy v. 3.0

Mozilla Security Blog Post: Enhancing CA Practices: Key Updates in MRSP v. 3.0

Version 3.0 of the Mozilla Root Store Policy, effective March 15, 2025, is located here: https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/.

Delayed revocation

Stronger revocation expectations—CAs must revoke certificates promptly in accordance with section 4.9.1.1 of the TLS Baseline Requirements (TLS BRs).
Subscriber education requirements—CAs must clearly communicate revocation requirements to subscribers.
Contract updates—Subscriber Agreements must explicitly require cooperation with revocation timelines.
Mass revocation preparedness—CAs must develop, maintain, and test large-scale revocation plans to ensure readiness for high-volume revocation events.
Third-party assessments—Independent reviews will verify that CAs have effective processes for rapid revocation.

Guidance for Complying with MRSP § 6.1.3 -
https://wiki.mozilla.org/CA/Mass_Revocation_Events

Phase-Out of Dual-Purpose (TLS + S/MIME) Root CAs

This requirement will ensure that trust and distrust decisions apply only to the relevant certificate type, avoiding unintended impact on unrelated services.
New root applications must specify either “websites” or “email” trust bit
Existing dual-purpose roots must submit a transition plan by **April 15, 2026**, and complete migration by **December 31, 2028**.

Automation for TLS Certificate Issuance & Renewal

Automation is critical for certificate agility and shorter certificate lifetimes.

- New root CAs must offer automated domain validation, issuance, and renewal.
- New root CAs must demonstrate automated certificate replacement at least every 30 days via a publicly accessible test website.
- Test website details must be disclosed in Inclusion Cases in the CCADB.

Mozilla has not yet determined if or how this requirement will apply to existing root CAs.

"Parked" CA Keys

Keys generated but not yet used in a CA certificate. This ensures that key management is transparent and secure, reducing the risk of undetected key compromise or misuse. CAs must report the SHA256 public hashes of DER-encoded SubjectPublicKeyInfo in annual audits or in similar CA certificate lifetime audit reports.

February 2025 CA Survey Results

There are two collections of data in the February 2025 CA Survey results: narrative CA responses and "Level of Concern" results.

Narrative Responses:

All CAs indicated that they would comply with MRSP version 3.0. Nearly all CA operators confirmed their readiness to document and report delayed revocation per the CCADB's version 3.0 Incident Reporting Guidelines. A few asked for a definition of "extensive harm", but hopefully with our updated statements about required revocation, the number of delayed revocation incidents will be minimized.

Mass revocation planning and auditing will be a challenge for CA operators. Guidance was requested regarding expectations for mass revocation preparedness and auditing. Timely cooperation of subscribers remains a concern. A few respondents indicated that they anticipate pushback from customers when enforcing compliance-related changes to subscriber agreements.

Several CAs asked for guidance on lifecycle management for parked CA keys and audit verification. Others indicated that current audit frameworks might not address parked keys sufficiently.

"Level of Concern" Responses: Most responses to the "Level of Concern" questions ranged between 1 (Not Concerned) and 3 (Moderately Concerned). Some CAs indicated moderate concern about ability to conduct incident investigations and root cause analysis within short timeframes. Lowest concern was expressed for meeting the test websites automation requirements for new root CAs and in meeting RFC-3647 requirements for CPs and CPSes.

CA Compliance - https://wiki.mozilla.org/CA/Incident_Dashboard

Current open bugs can be found in the Incident Dashboard (approximately 59 are currently open).

Approximately ninety CA compliance incidents were closed between October 1, 2024, and March 17, 2025. So, about 150 compliance incidents were open at any time between October 1 and March 25. They have been categorized as follows:

Type of Incident	Count
Audit Delays, Failures and Findings	**11**
CA Misissuance	**2**
CRL Failures	**13**
Disclosure Failures	**8**
DV Misissuance	**11**
EV Misissuance	**5**
Leaf Revocation Delays	**26**
OCSP Failures	**8**
OV Misissuance	**26**
Policy Failures	**23**
S/MIME Misissuance	**16**
Uncategorized	**5**

Audit Delays, Failures and Findings (11): Includes “Missing or Inconsistent Disclosure of S/MIME BR Audits”

CA Misissuance (2): KIR’s SZAFIR Trusted CA3 and CA4 - Reserved Certificate Policy Identifiers missing that indicated adherence and compliance with TLS BRs.

CRL Failures (13): Expired CRLs, CRL formatting, and wrong revocation reason codes.

Disclosure Failures (8): Late disclosures of policy updates, self assessments, and other information in the CCADB

DV Misissuance (11): Domain validation and certificate format errors.

EV Misissuance (5): Domain validation and certificate format errors.

Leaf Revocation Delays (26): Many of these we carried forward into 2025 and required completion of action items and submission of an Incident Closure Summary.

OCSP Failures (8): OCSP publication delays and incorrect OCSP responses.

OV Misissuance (26): LDAP CDP in certificates, improper domain validation, failure to check for compromised private keys, and incorrect or non-compliant certificate fields.

Policy/Practice Failures (23): Often combined with disclosure failures, delayed responses to Certificate Problem Reports, insufficient revocation response processes, divergence from stated or established policy or practice.

S/MIME Misissuance (16): Incorrect subject alternative names, non-compliant organization identifiers, other formatting errors. (Improved linting and validation workflows needed).

Uncategorized (5): Service outages, MPIC verification inconsistency, issue with revocation as part of automated reissuance, VMC and code-signing issuance issues

CA Inclusion Requests - https://wiki.mozilla.org/CA/Dashboard

Status	Count
Received - Initial Status	17
Information Verification	11
In Public Discussion	0
CP/CPS Review	1
TOTAL	**29**

Mozilla CA Certificate Program: https://wiki.mozilla.org/CA

Our Email Address: certificates@mozilla.org

Thanks!