Mozilla News

CA/B Forum F2F, Meeting 65 in Toronto, Ontario
June 10, 2025

Ben Wilson

Link to Previous Mozilla March 2025 Face-to-Face briefing - https://cabforum.org/2025/03/27/minutes-of-the-f2f-64-meeting-in-tokyo-japan-forum-level-march-25-26-2025/4-March-2025-Mozilla-News.pdf

CA Roundtable – May 16, 2025

- First industry-wide roundtable held under Mozilla's CA program
- Discussed CPSes, revocation, incident expectations, and automation
- Summary and minutes published
- Positive engagement and sharing of useful information

Root Inclusion Process Improvements

- **Goal:** Speed up processes from *"CA Providing Data"* to *"Public Discussion"*
- *Verification by Root Store* Phase: Reduce duration by clarifying and improving internal processes.
- *"CA Providing Data"* Phase: Encourage CAs to provide missing information to avoid verification delays

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

Status	Count
Received - Initial Status (CA Providing Data)	7
Information Verification (Verification by Root Store)	15
CP/CPS Review	5
In Public Discussion	1
Pending Approval	1
TOTAL	**29**

CA Compliance Improvements

Recent Improvements

- New **guidance on incident reporting**, including for delayed revocation
- Clearer expectations on Root Cause Analysis and Lessons Learned
- Updated "**Lessons Learned**" wiki page

Future Improvements to be Made

- Quicker response when bugs are initially filed
- More digging, scrutiny, and follow-up questions for CAs
- More frequent interjection when there are ambiguous or speculative comments
- More use of CCADB Public or Mozilla dev-security-policy list for in-depth discussions of systemic issues or policy changes that extend beyond a single incident
- Better written procedures for closing incidents, including handling of questions brought post-closure summary
- Improvements to the "Responding to an Incident" wiki page

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

Current open bugs can be found in the **Incident Dashboard** (approximately 52 are currently open, less about 12 that are scheduled to be closed soon).

In the past year, there have been roughly 160 CA compliance incidents. The following summary information is based on a report run in May 2025 and subsequent updating of the **"Lessons Learned"** wiki page.

1. Revocation Failures and Delays

Issues Observed
CAs failed to revoke certificates within required timelines. Several incidents involved misrouted Certificate Problem Reports (CPRs), customer unresponsiveness, or misunderstandings of revocation deadlines.

Root Causes
Many CAs lacked robust escalation procedures for CPRs, had outdated CPR contact information in CCADB, or relied too heavily on manual processing.

Corrective Measures and Lessons Learned
CAs implemented automated workflows for CPR handling, including webform submission systems and routing logic for immediate triage. Revocation policies were clarified to remove exceptions or delays. Email configurations were updated to accept relevant attachment types. Some CAs adopted ACME ARI or internal equivalents to enable subscriber-initiated automated replacement and revocation. Internal escalation procedures were reconfigured to trigger revocation based on CPR receipt, not after investigation completion.

2. Audit Gaps and Failures

Issues Observed
Several audit reports failed to include all in-scope CA certificates. S/MIME audits omitted technically capable roots or failed to meet expectations based on trust store inclusion rather than issuance activity.

Root Causes
CAs misunderstood scope requirements (i.e. if the CA is “capable of issuing” an S/MIME certificate because it lacks any EKU restrictions, etc.) and failed to communicate effectively with their auditors, or audit planning lacked formal scoping confirmations. In some cases, CAs could have used the CCADB's “All Certificates” report or the ALV tool.

Corrective Measures and Lessons Learned
CAs updated audit planning procedures to confirm certificate scope in writing with auditors before engagement. They began using CCADB’s “All Certificates” report and the ALV tool to catch issues before submission. Root CA audit requirements are now aligned with trust bit presence, and cross-certificates are evaluated for their key usages and EKUs. Auditor engagement letters and timelines are reviewed in advance to avoid submission delays.

3. Certificate Profile Noncompliance

Issues Observed
Numerous CA and subscriber certificates were issued with incorrect or outdated profiles. Common problems included: HTTPS or LDAP URLs in AIA/CDP fields, incorrect or multiple CP OIDs, improper key usages, duplicate serial numbers, and use of deprecated algorithms.

Root Causes
Many CAs lacked centralized profile management or automated checks for linting prior to issuance. Manual overrides or legacy profiles continued to be used without review. Developers and issuing staff were often unaware of recent BR changes.

Corrective Measures and Lessons Learned
CAs replaced manual profile selection with validated templates and automated issuance linting. They reviewed all profiles for compliance with BRs and Mozilla requirements, updated certificate generation logic, and retrained staff. Deprecated profiles were archived, and test environments were configured to reflect production lint behavior to avoid discrepancies.

4. S/MIME Certificate Misissuance

Issues Observed
CAs misissued S/MIME certificates by using invalid or mismatched email addresses, incorrect or unverified subject fields, and incorrect key usages or OIDs. Several certificates lacked the required alignment between OrgID and subject fields or included non-IA5STRING characters.

Root Causes
Validation systems were not fully updated for the S/MIME BRs, and legacy renewal processes

reused invalid configurations. Manual entry or bypasses led to inconsistencies. In some cases, updated linter tools were not deployed in production.

Corrective Measures and Lessons Learned
CAs deployed pkilint as a pre-issuance check in production and enforced stricter subject validation rules. They restricted renewal flows to avoid legacy profile use, introduced controls to ensure alignment between OrgID and country code, and expanded test cases for subject field validation. Sponsor-validated workflows were revised to reject ambiguous or misaligned email attributes.

5. Disclosure and Reporting Failures

Issues Observed
Intermediate CA certificates, revocation statuses, and updated CP/CPS documents were not disclosed to the CCADB within required timeframes. Other failures included outdated CA owner information and missed survey responses.

Root Causes
Disclosure responsibilities were often fragmented between operational and compliance teams. Procedures lacked explicit references to CCADB timelines. In some cases, tasks were completed, but documentation was not published or submitted to the CCADB on a timely basis.

Corrective Measures and Lessons Learned
CAs established standing coordination calls with third parties. Disclosure procedures were updated to include all document types and revocation status updates. CAs cross-check CCADB records during CP/CPS updates and review contact information regularly.

6. DV/OV/EV Misissuance and Validation Errors

Issues Observed
Misissuance occurred due to failures in domain validation, CAA checking, WHOIS use, and subject field verification. Examples included reused compromised keys, unverified FQDNs, and incorrect organization or locality names.

Root Causes
Validation code often lacked automated enforcement of CAA and DCV rules. WHOIS was used after deprecation, and fallback behaviors allowed misissuance. CAs relied too heavily on manual review or customer-submitted data.

Corrective Measures and Lessons Learned
CAs replaced WHOIS-based logic with DNS-based or ACME-compliant methods. CAA checks were re-engineered to enforce rejection if records were ambiguous or misconfigured. Manual approval steps were restructured to include UI constraints, and fallback methods were either documented or disabled. Tools now track reused public keys and block certificate issuance.

7. CRL and OCSP Availability Failures

Issues Observed
CRL files were not published, expired early, or were malformed (e.g., PEM instead of DER, duplicate serials). OCSP responses failed due to database replication lag, infrastructure outages, or incorrect timestamp logic.

Root Causes
Changes in hosting infrastructure or CDN setup were rolled out without end-to-end testing. Monitoring systems were limited to basic availability checks or lacked coverage for header accuracy. Alerting failed to catch issues due to misconfigured thresholds or expired domain names.

Corrective Measures and Lessons Learned
CAs restructured CRL publishing pipelines to enforce DER encoding, eliminated manual upload scripts, and published to CDNs with failover. OCSP and CRL alerts were enhanced to track replication delay, response correctness, and header consistency. CA systems now track all AIA/CDP domains and monitor for expiration.

General Recommendations

1. **Automate Critical Path Operations**
    - Adopt ACME/ARI-based tooling for revocation and replacement.
    - Automate CPR intake and response escalation with webforms and ticketing.
2. **Align Policy with Practice in Real Time**
    - Establish review checkpoints when any system configuration changes.
    - Ensure CP/CPS edits precede production changes, especially for EKUs and extensions.
3. **Create Centralized Linting and Disclosure Dashboards**
    - Monitor pre-issuance compliance, disclosure timelines, and revocation SLAs.
    - Track all CA task items in the CCADB using a shared internal calendar or tickler system.
4. **Institutionalize Audit Scoping and Planning**
    - Provide written confirmation of scope and trust bit mapping of all CA certificates to auditors.
    - Treat test roots, cross-certificates, and non-active hierarchies as in-scope if trusted.

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

Our Email Address: certificates@mozilla.org

Thanks!