Mozilla News

CA/B Forum F2F, Meeting 67 in Houston, Texas
March 11, 2026

Ben Wilson

Link to Previous Mozilla October 2025 Face-to-Face 66 briefing - https://cabforum.org/uploads/2025/2025-10_OctoberF2F/October-2025-Mozilla-News.pdf

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

Status	Count
Received - Initial Status (CA Providing Data)	10
Information Verification (Verification by Root Store)	15
Ready for Discussion / CP/CPS Review	3
In Public Discussion (Cybertrust Japan CA16)	1
Pending Approval	0
Recently Approved (JPRS External Subordinate CA)	1
TOTAL	**30**

CA Root or Trust-Bit Removals

Description	Count
Roots with Both Websites and Email Trust Bits	70
Roots created in 2006-2007 with Websites Trust Bit	14
Action Postponed on Removing Trust Bit	39
Bug 2017317 - Roots with March-April NSS Changes	33
Root Removals	13
Websites Trust Bit Removals	11
Email Trust Bit Removals	8
Distrust-After for Websites	1

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

Type	Count
Audit Delay	1
Audit Failure	1
Audit Finding	19
CA Misissuance	3
CRL Failure	4
Disclosure Failure	14
DV Misissuance	5
EV Misissuance	2
Leaf Revocation Delay	3
OCSP Failure	2
OV Misissuance	5
Policy Failure	9
S/MIME Misissuance	2
Uncategorized	5
Total	**75**

Recent Compliance Observations (Posted on CCADB Public)

- **Shift from manual procedural errors to automation design risks**

  – Previously, incidents were driven by manual process failures
  – Now, it's how systems were designed, integrated, or configured

- **Incomplete translation of policy into automated issuance controls**
  – CA systems don't closely implement Baseline Requirements

- **Increasing system complexity and reporting problems**
  – Higher dependence on synchronization between systems
  – Erroneous CCADB entries, metadata, URL disclosure, CRL publication, and disclosure timing

Improvements:

- Make sure information is checked for accuracy before it is made public (including CCADB records and CP/CPS postings).
- Ensure that policy requirements are clearly built into systems, so the software automatically enforces the rules rather than relying on manual interpretation.
- Strengthen automated checks so that systems can catch issues that linting tools might otherwise miss.
- Put comparison checks in place to ensure that what is issued in certificates matches what is disclosed publicly.
- Build clearer automated reminders and triggers so required incident disclosures happen on time.
- Tighten controls around system changes to reduce the chance that configuration updates introduce new compliance issues.

Other Items

- Mozilla Root Store Policy - beginning to look at issues and areas for improvement

- **Revocation Reason Codes**

Why? To enable stronger, more reliable browser-side revocation enforcement by:

- Preserving high-fidelity signals for security-significant events
- Reducing noise from purely administrative lifecycle revocations
- Improving CRLite scalability, freshness, and performance

What? Define two operational classes of revocation:

- **Security-Significant:** Key compromises, misissuances, unauthorized issuances, and validation failures

- **Administrative / Certificate Lifecycle:** superseded, cessation of operation, affiliation changes, subscriber-request

(no compromise), and routine cleanups

- **How?** Normalize reason codes into “Security” vs “Administrative” and align BR §4.9.1.1 revocation reasons with this risk mode.

Questions?

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

Our Email Address: certificates@mozilla.org

Thanks!