S/MIME Certificate Working Group

May 30, 2024
F2F #60 Bergamo

CA/BROWSER FORUM

Antitrust Compliance

CA/BROWSER FORUM

NOTE WELL

All participants are reminded that they must comply with the CA/Browser Forum's Bylaws, which include an antitrust policy, a code of conduct, and an intellectual property rights agreement.

Please contact the Forum Chair with any comments or concerns about the Bylaws or these policies.

Agenda

CA/BROWSER FORUM

1. Roll Call
2. Note well: Antitrust / Compliance Statement
3. Review Agenda
4. Approval of prior meeting minutes (May 8)
5. Overview of recent activity
6. Review of proposed ballot on logging
7. Discussion of Legacy deprecation
8. Review of Issues board
9. Charter review re by-laws
10. Any other business
11. Next teleconference: tentative June 5
12. Adjourn

Upcoming Dates

CA/BROWSER FORUM

- Sept 15 - Transition end for Extant S/MIME CAs
- Sept 15 - CAs should support CAA
- Sept 15 - CAs must declare CAA practices in their CPS
- Sept 15 - Only “active” Orgs
- March 15 - CAs must support CAA

Recent Activity

CA/BROWSER FORUM

- Ballot SMC06 - Post implementation clarification and corrections
- Parity on TLS BR ballots (for logging, MPIC, DTP etc.)
- Introducing method to rely upon eIDAS Qualified certificates
- Deprecation of Legacy generation
    - Review of differences between the Legacy and Strict/Multipurpose
    - Requests for feedback from CAs regarding issues that hinder migration

SMC07

- SMC07 - Align Logging Requirement and Key Escrow clarification
  https://github.com/cabforum/smime/pull/249

This ballot aims to clarify what data needs to be logged as part of the "Firewall and router activities" logging requirement in the S/MIME Baseline Requirements and align with a recent update within the TLS BRs.

This ballot additionally aims to clarify that maximum certificate validity periods do not affect maximum key escrow duration periods.

- Discussion ends 2024-06-05 12:30:00 UTC

Legacy Deprecation

CA/BROWSER FORUM

Feedback from Issuers/Users

- Sufficient headsup is required for ERAs with integrations
- Shorter validity accentuates the key management challenges of S/MIME
- Shorter validity creates an obstacle for large ecosystems using tokens
  - Hardware limitations
  - Support costs
- When split keys, why disallow Encryption being combined with EFS/BitLocker?

“Go fish or cut bait”

- Draft ballot

Other Topics

CA/BROWSER FORUM

- Issues list: https://github.com/cabforum/smime/issues
  - Plan is to do another rollup ballot

- Charter review
  - https://github.com/cabforum/forum/blob/main/SMCWG-charter.md
  - Described “start up goals” that have largely been met
  - Refine topics that are already covered in by-laws
  - Make a proposal to the Forum