S/MIME Certificate Working Group

CABF F2F #61, New Delhi

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
    a. Membership confirmation of DiSig, a.s.
5. Overview of recent activity
6. Review of proposed Ballot SMC06
7. Roadmap of 2024 activity
8. Any other business
9. Next teleconference: Adjourn

Overview of recent activity

CA/BROWSER FORUM

- Ballot SMC04: Addition of ETSI TS 119 411-6 to audit standards
- Ballot SMC05: Adoption of CAA for S/MIME incorporating new RFC 9495, *CAA Processing for Email Addresses*
- Feedback from implementation of SBR including audit preparations
- Feedback from pkilint, see https://github.com/digicert/pkilint
- Clarifications ballot prepared as SMC06

Dates

September 15, 2024

- Extant CA replacement
- SHOULD for CAA adoption, update CPS for CAA
- SMC06 - Proposed requirement to check Active status of Legal Entity Applicants

March 15, 2025

- SHALL for CAA adoption

Overview of Ballot SMC06

CA/BROWSER FORUM

https://github.com/srdavidson/smime/compare/ed36440d7c967732aa08739b14cc29bed257a67d...345a2358e1c6960bf3dcfc0ca5d400096ba59267

1. Clarification on use of Pseudonym (issue 203)
2. Clarification of GOV and INT identifiers in Appendix A (issue 206)
3. Clarification on keyUsage table (issue 208)
4. Clarification on tiering of Subject geographic fields (issue 211)
5. Clarification on Intermediate CAs as Extant SMIME CAs (issue 215)
6. Clarifications and new definitions regarding LEI and INT (issue 216)
7. OrgID requires subject:countryName to be present (issue 222)
8. subject:countryName value when verified country doesn't have an ISO 3166-1 country code (issue 223)
9. Clarifications on use of OU (issue 226)
10. Correction to description of Mailbox-validated (issue 227)
11. Use of alternate registration scheme country codes (issue 229)
12. Clarification on issuance to ceased orgs (issue 232)
13. Clarification of private key delivery to subscriber (issue 225, 234)
14. Clarification of open standards extensions (issue 235)
15. Correction of 7.1.4.2.2 n to MUST to match changed TLS BR

Roadmap

- At #62 F2F, workshop on Key Transparency possibilities for S/MIME
- Ballot SMC06
- Consideration of possible new methods for email control
  - Use of DNS for Sponsor-validated
  - Use of OAuth
- Deprecation of Legacy profiles
- e-Signature method for eIDAS (and EUDI Wallet)
- Issues list

Key Transparency possibilities

CA/BROWSER FORUM

- Addresses key discovery and key history, two of the biggest issues in S/MIME deployments
  - See https://github.com/google/keytransparency/blob/master/docs/overview.md
  - (CONIKS) https://eprint.iacr.org/2014/1004.pdf

- Implementations include Whatsapp, Signal, ProtonMail, KeyBase, Apple, and others
  - See email example at https://proton.me/support/key-transparency

- As cloud service providers are now the dominant mode for email services, both personal and enterprise, Key Transparency becomes a possible enhancement for S/MIME certificates
  - Better lifecycle support for rotation/shorter life
  - Improves the “cert was good at this time” issue

- Interest in workshop to discuss Key Transparency at #62 F2F?
  - Opportunity to have “right people in the room” … invited guests?