

CA/Browser Forum

Status and future activities

Dimitris Zacharopoulos
CA/Browser Forum Chair

What is the CA/Browser Forum?

- Global “Standards Defining Organization (SDO)” but not an incorporated entity
- Competing Organizations get together to agree on mutual policies/practices for the provisioning/issuance/governance of Publicly-Trusted SSL/TLS, Code Signing,.... Certificates
- Produces “Guidelines” which are incorporated into:
 - WebTrust for CAs Standards by WebTrust Task Force
 - ETSI Standards by ESI
 - ... other Standards/national policies
- Guidelines are licensed under [Creative Commons Attribution 4.0](https://creativecommons.org/licenses/by/4.0/)

Sampling of CA/B Forum members

48 CAs, 8 Browsers



Current Governance

- CA/B Forum Plenary → <https://cabforum.org/>
 - [Server Certificate Working Group](#)
 - [Validation Subcommittee](#)
 - [Network Security Subcommittee](#)
 - [Code Signing Certificate Working Group](#)
 - [S/MIME Certificate Working Group](#)
- Each WG has some level of independence (via charter)
- More Working Groups can be created depending on Industry interest

Expectations to comply with Guidelines

- CA/B Forum Maintenance Guidelines are voted and become effective usually 30 days after initial vote
- WebTrust and ETSI take more time to update their respective standards
- Certificate Consumers expect Certificate Issuers to **comply to the latest Guidelines when they become effective!**
- Some Maintenance Guidelines contain **fixed effective dates!**

Latest News in Server Certificate WG

- Update Domain Validation Methods
 - [SC25](#): Define New HTTP Domain Validation Methods v2 (2020-03-03)
 - [SC27](#): Version 3 Onion Certificates (2020-03-27)
 - [SC33](#) - TLS Using ALPN Method (to be published)
- Other topics
 - [SC23](#): Precertificates (2019-12-19)
 - [SC24](#): Fall cleanup v2 (2019-12-19)
 - [SC26](#) - Pandoc-Friendly Markdown Formatting Changes (2020-05-04)
 - [SC28](#) - Logging and Log Retention (in IPR Review Period)
 - [SC29](#) - Configuration Management (2020-06-08)
 - [SC30](#) - Disclosure of Registration/Incorporating Agency (2020-08-20)
 - [SC31](#) - Browser Alignment (2020-08-20)
 - [SC35](#) - Cleanups and Clarifications (in IPR Review Period)
- Ballots under consideration
 - NCSSRs Zones
 - SC34 - Account Management
 - Minimum expectations regarding weak keys
 - Security Requirements for Air-Gapped CA Systems

Latest News in Code Signing WG

- “Baseline Requirements for Code-Signing Certificate” v2.0 (2020-09-02)
 - Combines EV Guidelines for Code-Signing
- Convert to RFC 3647 structure
- EV vs. Non-EV items will be reviewed
- **Move deadline for transition of RSA-3072 to end of Q2 2021**
- Discussions about how to handle “high-risk” certificates

Latest News in S/MIME Certificate WG

- Collecting various existing international/national standards (ETSI, RFC 5280, government documents) related to S/MIME Certificates
- Define a basic Certificate Profile
- Describe major use cases and solicit feedback from other WGs and/or the public
- Individual S/MIME certs versus those used on gateways

Other resources

- Meeting minutes (including F2F) <https://cabforum.org/category/minutes/>
- Mailing-list archives
 - CABF Plenary public list <https://cabforum.org/pipermail/public/>
 - Server Certificate WG public list <https://cabforum.org/pipermail/servercert-wg/>
 - Validation Subcommittee public list <https://cabforum.org/pipermail/validation/>
 - NetSec Subcommittee public list <https://cabforum.org/pipermail/netsec/>
 - Code Signing Certificate WG public list <https://cabforum.org/pipermail/cscwg-public/>
 - S/MIME Certificate WG public list <https://lists.cabforum.org/pipermail/smcwg-public/>
- How to join the CA/B Forum
 - <https://cabforum.org/information-for-potential-members/>



Thank you

Dimitris Zacharopoulos
dzacharo@harica.gr