

CA/Browser Forum

Status and future activities

Dimitris Zacharopoulos
CA/Browser Forum Chair

What is the CA/Browser Forum?

- Global “Standards Organization” 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](#)

CA/Browser Forum Participants

- Members
 - Certificate Issuers (Certification Authorities == Trust Service Providers)
 - Certificate Consumers
- Associate Members
 - ACAB'c (Association of Accredited ETSI Auditors)
 - CPA Canada and WebTrust Task Force
 - European Telecommunications Standards Institute (ETSI)
 - US Federal PKI
- Interested Parties (personal and legal entities)
- ALL PARTICIPANTS SIGN AN IPR AGREEMENT

Current Governance

- CA/B Forum Plenary → <https://cabforum.org/>
 - [Server Certificate Working Group](#)
 - [Validation Subcommittee](#)
 - [Network Security Subcommittee](#)
 - [Code Signing Certificate Working Group](#)
 - No Subcommittees yet
- Each WG has some level of independence (via charter)
- Pending Creation of S/MIME Working Group
- More Working Groups can be created depending on Industry interest

Who oversees the TSPs?

- The CA/B Forum **IS NOT** a regulatory or supervisory body
- Certificate Consumers (“Application Software Suppliers”, “the Browsers”) effectively "**supervise**" the Trust Service Providers for SSL/TLS or Code Signing Trust Services via their “**Root Programs**”
- In addition to “Root Programs”, QWACs are regulated in EU
 - Each Member State has a “Supervisory Body” to monitor adherence to eIDAS
- Transparency
 - Certificate Transparency for SSL/TLS Certificates
 - Public reporting (anonymous or not), by TSPs, Relying Parties, Researchers

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!**

Latest News in Server Certificate WG

- Update Domain Validation Methods
 - SC14: Updated phone validation methods (16 Mar 2019)
 - SC15: Remove Validation Method Number 9 (16 Mar 2019)
 - SC7: Update IP Address Validation Methods (16 Mar 2019)
 - SC19: Phone Contact with DNS CAA Phone Contact (9 Sep 2019)
- Other topics
 - SC16: Other Subject attributes (16 Apr 2019)
 - SC17: Alternative registration numbers for EV certificates (21 June 2019)
 - SC22: Reduce lifetime of Certificates (Failed)
- Ballots being discussed
 - SC20: System Configuration Management
 - SC21: Log Integrity Controls
 - Incorporation of LEIs in EV Certificates

Latest News in Code Signing WG

- “Guidelines for the Issuance and Management of Publicly-Trusted Code Signing Certificate” v1.2
- List of improvements already in place for ballots
- Expecting input from Antivirus/Malware detection industry
- Expecting Oracle to participate as a Certificate Consumer
- Time-stamping requirements related to Code Signing
 - Probably spin up a new WG to deal with Time-stamping requirements

Discussions around S/MIME Certificate WG

- Open discussion about the scope of the charter (whether to include identity issues in the charter or not)
- First efforts will be to create requirements/practices for validating e-mail addresses to be included in digital certificates
- Binding identities to e-mail addresses is a second goal
- General consensus that the first guideline should not include identity validation requirements

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/>
- How to join the CA/B Forum
 - <https://cabforum.org/information-for-potential-members/>

Thank you

Dimitris Zacharopoulos
dzacharo@harica.gr