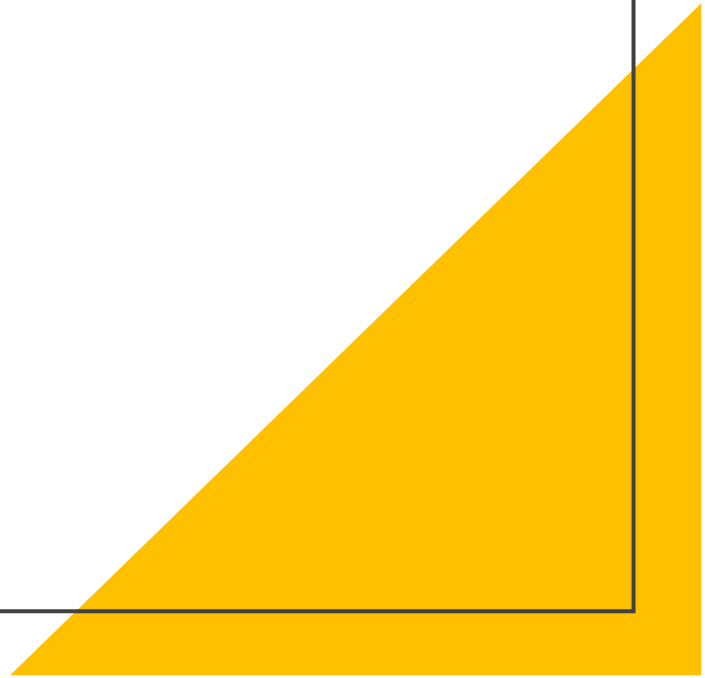




CA/BROWSER FORUM

CA/Browser Forum
Publicly-Trusted Certificates
Global PKIs

Dimitris Zacharopoulos
GUnet/HARICA
CA/B Forum Chair



- Voluntary
- Not an incorporated entity or an association, it's simply a group
- The Forum has no regulatory or industry powers over its members or others
- Global "Standards Defining Organization" (SDO)
- Collaboration of Certificate Issuers and Certificate Consumers
- SSL/TLS, Code Signing, S/MIME
- Produces "Guidelines" incorporated into Global audit schemes:
 - WebTrust
 - ETSI
- Guidelines are licensed under [Creative Commons Attribution 4.0](#)

What is the CA/Browser Forum?

- CA/B Forum Plenary → <https://cabforum.org/>
 - [Server Certificate Working Group](#)
 - [Validation Subcommittee](#)
 - [Code Signing Certificate Working Group](#)
 - [S/MIME Certificate Working Group](#)
 - [Network Security Working Group](#)
- Each WG has some level of [independence](#) (via charter)
- More Working Groups can be created depending on industry interest
- Next F2F scheduled for June 6-8, 2023

Current Governance

Server Certificate WG

- Two documents:
 - [Baseline Requirements \(for SSL/TLS Certificates\)](#)
 - Based on Recommendation ITU-T X.509 (**08/2005**) and RFC 5280
 - [Extended Validation Guidelines \(for SSL/TLS Certificates\)](#)
- Recent ballots: [Server Certificate Ballots](#)
- Points of interest
 - Short-lived certificates
 - Multi-perspective domain validation
 - Reformat the EVGs in RFC 3647 structure

Code Signing WG

- [Baseline Requirements for Code-Signing Certificate](#)
 - Based on Recommendation ITU-T X.509 (08/2005) and RFC 5280
- Recent Ballots: [Code Signing Ballots](#)
- Next steps
 - Removing SSL BR references
 - Remote signing services
 - Time-stamp Authority issues

S/MIME Certificate WG

- [S/MIME Baseline Requirements](#) version 1.0.0
 - Based on Recommendation ITU-T X.509 (**10/2012**) and RFC 5280
- Effective date **September 1, 2023**
- Next steps
 - Erratum ballot
 - Enterprise RA and external email domains

NetSec WG

- Documentation:
 - [Network Security Requirements – CAB Forum](#)
- Prepare work for other WGs to include into their respective Guidelines
- Recent activity:
 - Security Requirements for Air-Gapped CA Systems
 - Looking at importing some controls from the Cloud Controls Matrix ([CCM](#))

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/>
 - Code Signing Certificate WG public list <https://cabforum.org/pipermail/cscwg-public/>
 - S/MIME Certificate WG public list <https://cabforum.org/pipermail/smcwg-public/>
 - NetSec WG public list <https://cabforum.org/pipermail/netsec/>
- How to join the CA/B Forum (anyone can join, no fees)
 - <https://cabforum.org/information-for-potential-members>



Thank you

Dimitris Zacharopoulos

dzacharo@harica.gr