HARICA

CA/BROWSER FORUM

CA/Browser Forum

Status and future activities

Dimitris Zacharopoulos

CA/Browser Forum Chair

Current Governance

- CA/B Forum
  - Infrastructure Subcommittee
- Server Certificate Working Group
  - Network security Subcommittee
  - Validation Subcommittee
- Code Signing Working Group
  - No Subcommittees
- Pending Creation of S/MIME Working Group
  - Deciding the charter language around the scope of “Identity” in S/MIME Certs

Server Certificate Working Group

- Ballots passed **since May 2019** (effective dates)
  - SC17: Alternative registration numbers for EV certificates (2019-06-21)
  - SC19: Phone Contact with DNS CAA Phone Contact (2019-09-09)
  - SC21: The Network and Certificate Systems Security Requirements section 3 (Log Integrity Controls) (2019-11-04)
  - SC23: Precertificates (2019-12-19)
  - SC24: Fall cleanup v2 (2019-12-19)
  - SC25: Define New HTTP Domain Validation Methods v2 (under IPR Review)

Server Certificate Working Group

- Ballots in Discussion Period
  - SC20: Configuration Management (Network Security Requirements)
  - SC27: Version 3 Onion Certificates
- Draft Ballots under Consideration
  - SC26 - Pandoc-Friendly Markdown Formatting Changes
  - LEI Ballot
  - Aligning the BRs with existing Browser Requirements
- Contribution from the WebTrust TF in the NetSec Subcommittee
  - Getting input from Auditors is extremely valuable!

Server Certificate Working Group

- Topics of Interest
  - Default Deny/Default Allow interpretation of the Baseline Requirements.
    - CAs have expressed objections on this process because such a blanket interpretation would effectively “change" the existing requirements.
    - Browsers asked for CAs to review all their CP/CPS documents and the BRs to identify possible sections that would have different interpretations if read under the “default deny” perspective, for example the subjectDN of CA Certificates (C, O, CN)
    - CAs have stated that "the requirements are the requirements", not default allow nor default deny. If the WG wants to prohibit something or make a requirement stricter, this should be introduced via the ballot process, just like we limited the number of subjectDN attributes in EV TLS Certificates
    - The minutes of this discussion are currently only on the CA/B Forum Member’s Website but will soon be approved and published
  - Incorporation of individual Root Store Program requirements/policies into the BRs
    - No discussion yet

Code Signing Certificate Working Group

- Identify possible overlaps between the Code Signing BRs and Code Signing EV Guidelines
- Possibly merge the two documents
- Convert to RFC 3647 structure
- Remote Key Attestation for Subscriber-generated Keys in FIPS/HSM/Cloud HSM devices/services
- Planning for a CSCWG Summit in March 2020 hosted by Microsoft

Next F2F in Bratislava
Feb 18-20

Thank you

Dimitris Zacharopoulos
dzacharo@harica.gr