CA/Browser Forum

Status and future activities

Dimitris Zacharopoulos
CA/Browser Forum Chair
Current Governance

• CA/B Forum →
  • Server Certificate Working Group
    • Subcommittees
    • CAs → Certificate Issuers
    • Browsers → Certificate Consumers
  • Code Signing Working Group
    • CAs → Certificate Issuers
    • Application Software Suppliers → Certificate Consumers

• Each WG has some level of independence (via charter)

• Pending Creation of S/MIME Working Group
Server Certificate Working Group

• Ballots passed **since September 2018** (effective dates)
  • SC3: Two-Factor Authentication and Password Improvements (15 Sep 2018)
  • SC6: Revocation Timeline extension (14 Oct 2018)
  • SC12: Subset of Underscores in dNSNames (10 Dec 2018)
  • SC13: CAA Contact property and associated email validation methods (1 Feb 2019)
  • 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)
  • SC16: Other Subject attributes (16 Apr 2019)
  • SC17: Alternative registration numbers for EV certificates (Under IP Review)
  • SC19: Phone Contact with DNS CAA Phone Contact (Under IP Review)
Code Signing Certificate Working Group

• Adoption of Minimum Requirements for Code Signing as an official CA/B Forum document under the name “Baseline Requirements for the Issuance and Management of Publicly- Trusted Code Signing Certificates”

• Resolve any Intellectual Property issues (IP Review period is 60 days after initial vote for adopting a Full Guideline)

• Work on EV Code Signing Guidelines in parallel

• Solicit more Certificate Consumers
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
Audit Convergence (ETSI/WebTrust)

• Relying Parties should have a similar level of assurance for Trust Services offered by ETSI or WT audited TSPs
  • “Point in time audit”, “period of time audit”, “performance audit” and “point in time readiness assessment”, “key ceremony report”, “currently valid audit report”, “full surveillance”, “publicly-trusted certificate”, and “fail to pass an audit”

• Both ETSI/WebTrust schemes have similar history
  • X9.79 group developed Annex B for PKI Practices and Policy Framework, evolved into WebTrust for CAs 1.0. IETF had the PKIX RFC 2527. The American Bar Association was involved with the PKI Assessment Guidelines (PAG). It espoused XML for CPs and CPSs for processing comparisons. Followed by ISO 21188. The ABA’s PAG discussed “assessment” and led to WebTrust for CAs 1.0
  • In the EU, there was the Electronic Signatures Directive 1999/93/EC. This then brought about ETSI TS 101 456 and TS 102 042
  • The Forum or “WeTSI” should attempt to reach a common vocabulary and understanding of the audit process and clearly communicate this to CAs/TSPs.
Thank you

Dimitris Zacharopoulos
dzacharo@harica.gr