HARICA

CAB CA/BROWSER FORUM

CA/Browser Forum

Status and future activities

Dimitris Zacharopoulos

Elected Chair CA/Browser Forum

What is the CA/Browser Forum?

- It **IS NOT** a regulatory or supervisory body
- It is closer to a Global “Standards Organization”
- Competing Organizations get together to agree on mutual policies/practices for the provisioning/issuance/governance of Publicly-Trusted SSL/TLS Certificates
- Application Software Suppliers (i.e. "the Browsers") are the ones that effectively "supervise" the Trust Service Providers for SSL/TLS Trust Services via their “**Root Programs**”

New Governance

- CA/B Forum → Server Certificate Working Group
  - Working Groups → Subcommittees
  - CAs → Certificate Issuers
  - Browsers → Certificate Consumers
- Each WG has some level of independence (via charter)
- Pending Creation of S/MIME and Code Signing Working Groups
- Document Signing? Which "Certificate Consumers" would be interested?
  - Adobe?
  - Others?

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 agreed to start with a **common vocabulary** and understanding of the audit process of each standard

Effective Supervision

- EA → National Accreditation Body → Conformity Assessment Body
- Supervisory Body only for eIDAS → EU TSL
- NAB is not necessarily the "Supervisory Body"
- Does it work effectively? Tested?
- Browsers that detect mis-issued certificates, not-compliant CP/CPS that are **not detected/reported by CABs**, will likely start sending official complaints to **CABs**, **Supervisory Bodies**, **NABs**, just to "test" the eIDAS/ETSI scheme's processes:
    - How will the industry react?
    - Is the program sufficiently "policed"?
    - Are Relying Parties sufficiently protected and place trust in Certificate "Products"?

Supervision is never enough…

- Current picture for non SSL/TLS Certificates is… not looking good
  - Public CP/CPS documents not updated for years
  - Qualified Certificates with questionable Subject Information and extensions
  - Audit Reports with critical findings that are classified as “minor” Non-Conformities
  - Qualified Timestamps which are not… timestamps (RFC 3161)
  - Violations of RFC 5280
- Does more transparency improve the ecosystem security?
  - Certificate Transparency for SSL/TLS Certificates
  - Public reporting (anonymous or not)?
  - Are TSPs afraid of self-reporting mistakes? Non-compliances? Are eIDAS TSPs mature enough to use “transparency” as a security tool?

Thank you

Dimitris Zacharopoulos

dzacharo@harica.gr