CA/BROWSER FORUM

Server Certificate Working Group Update since last F2F

F2F#67 10-March-2026 | Houston, Texas

Presenter: Dimitris Zacharopoulos (HARICA)

Ballots

- **Passed (effective date)**
  - SC086: Sunset the Inclusion of IP Reverse Address Domain Names (2025-12-15)
  - SC091: DNS TXT Record with Persistent Value Validation Method for IP Addresses and Sunset 3.2.2.5.3 (2025-12-16)
  - SC090: Gradually sunset all remaining email-based, phone-based, and 'crossover' validation methods from Sections 3.2.2.4 and 3.2.2.5 (2026-01-12)
  - SC094v2: DNSSEC exception for email DCV methods (2026-02-16)
  - SC096: Carve-out for DNSSEC verification logging requirements (2026-02-17)
  - SC097: Sunset all remaining use of SHA-1 signatures in Certificates and CRLs (2026-02-25)
  - SC095: Clean-up 2025 (IPR ends 2026-03-29)
- **In Discussion Period**
  - None

Ballots

- **Under consideration**
  - SC087: Registration Number Improvement for EV Certificates
  - SC098: Process RFC 8657 CAA Parameters
  - SC0XX: Cleanup for ADN CNAME use
  - SC0XX: Improve Certificate Problem Reports and Clarify the Meaning of Revocation
  - SC0XX: Update Revocation timeline for errors affecting CP/CPS deviations but in accordance with the BRs
  - SC0XX: CA Resource Availability

Attention: Effective dates for certain requirements

Compliance	Section	Summary Description (See Full Text for Details)
2026-03-15	3.2.2.4	DNSSEC validation back to the IANA DNSSEC root trust anchor MUST be performed on all DNS queries associated with the validation of domain authorization or control by the Primary Network
2026-03-15	3.2.2.4	CAs MUST NOT use local policy to disable DNSSEC validation on any DNS query associated with the validation of domain authorization or control.
2026-03-15	3.2.2.4	CAs MUST NOT rely on Method 3.2.2.4.8 to issue Subscriber Certificates.
2026-03-15	3.2.2.8.1	DNSSEC validation back to the IANA DNSSEC root trust anchor MUST be performed on all DNS queries associated with CAA record lookups performed by the Primary Network Perspective.
2026-03-15	3.2.2.8.1	CAs MUST NOT use local policy to disable DNSSEC validation on any DNS query associated CAA record lookups.
2026-03-15	3.2.2.8.1	DNSSEC-validation errors observed by the Primary Network Perspective (e.g., SERVFAIL) MUST NOT be treated as permission to issue.
2026-03-15	4.2.2	CAs SHALL NOT issue Certificates containing Domain Names that end in an IP Reverse Zone Suffix.
2026-03-15	4.2.1	Subject Identity Information validation maximum data reuse period is 398 days.
2026-03-15	4.2.1	Domain Name and IP Address validation maximum data reuse period is 200 days.
2026-03-15	6.3.2	Maximum validity period of Subscriber Certificates is 200 days.
2026-03-15	7.1.2.4	CAs MUST NOT use Precertificate Signing CAs to issue Precertificates. CAs MUST NOT issue certificates using the Technically Constrained Precertificate Signing CA Certificate Profile specified in Section 7.1.2.4.
2026-09-15	7.1.3.2.1	Sunset all remaining use of SHA-1 in Certificates and CRLs.

Other updates

- New TLS BRs versions:
  - 2.1.8 (SC092)
  - 2.1.9 (SC088)
  - 2.2.0 (SC086)
  - 2.2.1 (SC091)
  - 2.2.2 (SC090)
  - 2.2.3 (SC094)
  - 2.2.4 (SC096)
  - 2.2.5 (SC097)

- New EVGs versions:
  - No new versions
- GitHub open issues (92)
  - Triage
  - Tags and assignments
  - 32 “clean-up”, 2 “editorial”, 20 “validation-sc”