What's going on in DNS Security?

ICANN 85 – DNSSEC Workshop
March 11, 2026

Peter Thomassen <peter@desec.io>

DNSSEC Maintenance at IETF

- Handling of algorithm requirements moved to IANA registry
  → RFC 9904 “DNSSEC Cryptographic Algorithm Recommendation Update Process“
- Specifications deprecating SHA-1-based and GOST cryptography published
  → RFC 9905 “Deprecating the Use of SHA-1 in DNSSEC Signature Algorithms”
  → RFC 9906 “Deprecate Usage of ECC-GOST within DNSSEC”

DNSSEC Maintenance at IETF (2)

- Roy Arends et al. proposing type range for parent-side delegation point RRs
  - Signed by the parent (like DS)
    → facilitates signing the new DELEG delegation record
  - Downgrade prevention via DNSKEY flag
  - draft-ietf-dnsop-delext (recently adopted by DNSOP WG)
- Yorgos Thessalonikefs et al. proposing “dry-run” to test DNSSEC (soft-fail)
  - Dry-run mode is signaled in DS record (no child-side changes needed)
  - draft-ietf-dnsop-dry-run-dnssec (recently adopted by DNSOP WG)
- Paul Hoffman proposing RFC9364-bis, listing all DNSSEC RFCs in one place
  - draft-ietf-dnsop-rfc9364bis (recently adopted by DNSOP WG)

DNSSEC Automation at IETF

- Peter Thomassen proposing consistency checks for CDS/CDNSKEY & CSYNC
  - Prevents breakage when zone owner intent is ambiguous
  - draft-ietf-dnsop-cds-consistency (in RFC Editor Queue)
- … as well as “Operational Recommendations for DS Automation”
  - Designed to address concerns around DS automation interoperability in gTLDs
  - draft-ietf-dnsop-ds-automation (finished DNSOP WG Last Call)
- Johan Stenstam et al. proposing a way to apply delegation updates via DDNS
  - Works with signed and unsigned children
  - Establishes secure channel via `_signal` mechanism below each NS domain (see RFC 9615)
  - draft-ietf-dnsop-delegation-mgmt-via-ddns (recently adopted by DNSOP WG)

DNSSEC Future at IETF

- DELEG Working Group making progress on new way of delegating a domain
  - Better security properties (signed referral)
  - Indirect mode, allowing to point to operator for transport and key configuration
  - SVCB-style syntax
- DCONN Working Group started standardizing Domain Connect
  - Protocol for simplified provisioning of 3rd-party records (e.g., MX or TXT verification records)
- New work on Post-Quantum DNSSEC will be presented at IETF side meeting
  - Tuesday March 17, 2026, 08:00–09:00am CST
    → join via https://sidemeetings.ietf.org/
  - For more content see https://wiki.ietf.org/en/group/pq-dnssec