What's going on in DNS Security?

ICANN 84 – DNSSEC Workshop
October 29, 2025

Peter Thomassen <peter@desec.io>

Recently in the News: DNS Poisoning Revisited

- Under certain circumstances, attackers could predict supposedly random response characteristics or otherwise trick resolvers
- Several resolver vendors affected (all fixed):
  - BIND, tracked here and here
  - PowerDNS Recursor, see advisory
  - Unbound, see advisory
- Ars Technica article on the topic

DNSSEC Maintenance at IETF

- Specifications deprecating SHA-1-based and GOST signing algorithms now with the RFC Editor

Document links:

- draft-ietf-dnsop-must-not-sha1
  “MUST NOT use RSASHA1 (5) and RSASHA1-NSEC3-SHA1 (7)” for signing and delegation
- draft-ietf-dnsop-must-not-ecc-gost
  “MUST NOT use ECC-GOST (12)” signature algorithm
  “MUST NOT use GOST R 34.11-94 (3)” digest type

DNSSEC Maintenance at IETF (2)

- Mark Andrews proposing a way to advertise private algorithms in a DS record
  - Previously only supported on child side (DNSKEY), i.e., not as a secure entry point (SEP)
  - draft-andrews-ds-support-for-private-algorithms
- Steve Crocker et al. proposing an algorithm lifecycle model
  - For DNSSEC and beyond
  - draft-crocker-dnsop-dnssec-algorithm-lifecycle
- Joe Abley et al. proposing a way to have a “zone cut to nowhere”
  - For external view in split-horizon setups, or as a .internal carve-out
  - Syntax: `example. IN NS . ; assuming the root has not address`
  - draft-jabley-dnsop-zone-cut-to-nowhere

DNSSEC Maintenance at IETF (3)

- Shumon Huque et al.: RFC 9824 on “Compact Denial of Existence”
  - Makes negative responses more privacy-conserving
  - Makes negative responses cheaper for on-line signers
  - NXDOMAIN looks like NOERROR/NODATA, but spec include a signal to restore NXDOMAIN
- Johan Stenstam et al. proposing a way to have signal authoritative transports
  - By opportunistically including an SVCB record in certain responses
  - draft-johani-dnsop-transport-signaling

DNSSEC Maintenance (4): draft-huque-dnsop-multi-alg-rules

1. tl;dr: Nutshell Proof of Sanity

It is well known that

1. validator implementations MUST support certain mainstream algorithms ([DNSKEY-IANA]);
2. validators MUST accept any valid path ([RFC6840] Section 5.11).

Thus, when a zone advertises several algorithms which MUST be supported for validation, the zone operator can reasonably expect that validation will work, even when only serving signatures for one of them. (For use cases see below.)

Therefore,

3. if a mainstream algorithm is disabled in a validator (as a matter of local policy), the validator still ought to accept a path using this algorithm, and treat responses as insecure – regardless of other algorithms advertised for the zone.

This is because the zone operator has a reasonable expectation that the algorithm is supported in all validators. The zone operator should not have to expect that serving this path would lead to "bogus" security status / SERVFAIL.

Rather, **if a validator *due to local policy* does not support required mainstream algorithms**, it should **take on responsibility** for that **locally**, and **behave as a non-validating resolver for that zone.**

This document updates validation rules accordingly: primarily as described above, and secondarily to gracefully cover an implicit issue when a mainstream algorithm reaches its end of life. Downgrade protection is preserved.

DNSSEC Automation at IETF

- John Levine et al.: RFC 9859 on “Generalized DNS Notifications”
  - Allows parent to announce where it likes to be nudged by the child when desiring a DS update
  - Currently used to trigger an ad-hoc CDS/CDNSKEY scan (replacing scheduled scanning)
  - May also be used to convey Dynamic Updates; related draft (Johan Stenstam et al.): draft-johani-dnsop-delegation-mgmt-via-ddns
- Peter Thomassen proposing consistency checks for CDS/CDNSKEY & CSYNC
  - Prevents breakage when zone owner intent is ambiguous
  - draft-ietf-dnsop-cds-consistency (IETF Last Call just ended)
- … as well as “Operational Recommendations for DS Automation”
  - Designed to address concerns around DS automation interoperability in gTLDs
  - Most issues resolved, expect WG Last Call soon
  - draft-ietf-dnsop-ds-automation

DNSSEC Future at IETF

- Roy Arends et al. proposing “Protocol Modifications for Delegation Extensions”
  - By adding a range of authoritative record types at the parent (à la DS)
  - Comes with signaling to prevent downgrade attacks
  - draft-arends-dnsop-delext
- DELEG Working Group specifying new way of delegating a domain
  - Better security properties (signed referral)
  - Indirect mode, allowing to point to operator for transport and key configuration
  - Likely based on an SVCB-like record
- DCONN Working Group just launched, to standardize Domain Connect
  - Protocol for simplified provisioning of 3rd-party records (e.g., MX or TXT verification records)

DNSSEC Future at IETF (2): Post-Quantum Cryptography

- Swapneel Sheth et al. proposing Post-Quantum Cryptography Strategy
  - Involving a plug-in PQC algorithm
  - To improve space efficiency, a variant based on Merkle tree ladders is proposed
    → replaces most signatures by a list of hashes (but DNSKEY needs a full signature)
  - draft-sheth-pqc-dnssec-strategy
- Aditya Singh Rawat et al. recently published paper on “Quantum-safe Signatureless DNSSEC”
  - Reduces most signatures to HMACs (but DNSKEY needs a full signature)
  - Requires on-line signing
- Informal IETF research group held “side meetings” during last 4 IETF meetings
  - Research documented at https://wiki.ietf.org/en/group/pq-dnssec
  - No meeting at IETF 124