draft-ppr-dd-auth-delegation-types

- Petr Špaček
- Peter van Dijk
- Roy Arends

Inspired by

draft-peetterr-dnsop-parent-side-auth-types-01

draft-pwouters-parental-rrtype-00

Quick recap

- DNS delegations rely on limited functionality.
  - A hostname that resolves to an address.
- New requirements exposes this limited functionality
  - secure transport
  - operational flexibility
  - Error reporting, additional chains of trust, etc.
- The goal is to modernize delegation without breaking compatibility and allow evolution

Introducing DNS Delegation Extensions

- Not just "an RRtype named DELEG."
- Not a one-RR-fits-all solution.
- A flexible framework that evolves DNS delegation.
- Supports gradual, safe deployment.
- In technical terms, introduces new Delegation RR Types.
  - Baheviour is similar to DS records, signed and only allowed to be present at a delegation point.

Delegation Extensions technical components

- Authoritative Delegation Type (ADT) records
  - New RRtypes that exist only at delegation points
  - EDNS0 “DE” Bit – resolver opt-in signaling of ADT support
  - DNSKEY Flag – securely signals ADT support in zones
  - NSEC/NSEC3 – secure proof of absence of ADT records

Design Lessons from the DNS Record Archive

- One RRtype won't fit all (SRV vs. SVCB)
- NXT → NSEC → NSEC3 evolution required retrofitting each time
- Retrofitting is costly
  - See previous slide
  - Will take a long time to implement
- Shoehorning leads to ambiguity and operational fragility
  - We could put everything in TXT records or DS records.
  - But it comes at a large operational cost

In short:

- Uses the DNSKEY flag and EDNS DE bit for signaling *
- Uses NSEC/3 for secure proof of absence *
- Define a range of RR TYPEs for delegation type records
  - Type DELEG will be assigned from the range.
- Our proposal: Document this independently from the literal DELEG type.

* already in draft-ietf-deleg