parent-only-record-signalling

arends-parent-only-record-signalling

22 July 2024, IETF120, DD WG

roy.arends@icann.org
What is this about

• Document DNSSEC Protocol Changes: the necessary modifications to the DNSSEC protocol to accommodate “Parent-Only” records.

• “Parent-Only” refers to parent-side delegation point records that are signed similarly to DS records.

• The changes are substantial enough to justify a separate specification.
Why separate this from the DELEG draft

• Ensure Future-Proofing: Implement changes that are future-proof to avoid the need for additional modifications (such as another NSEC3 support signalling kludge) for any new parent-only records that may be developed.

• Flexibility Beyond DELEG: Recognize that while DELEG rdata may accommodate various needs, there could be other concepts that do not align with DELEG.
How?

• Document DNSSEC Protocol Changes:
  • Create a stand-alone document detailing the changes needed to support future "Parent-Only" records

• Designate Parent-Only Types:
  • Assign a range of Parent-Only types for future use.
  • This ensures that authoritative servers include these records when present without needing to understand them.

• Require Authenticated Denial Records:
  • Ensure authenticated denial records are present in all delegation responses to prove the absence of these types.
  • Note that these records are currently absent when a DS record is present in a response.

• Provide a Secure Signal:
  • Establish a secure signal so that supporting validators know to expect the NSEC/NSEC3 record.
This is not a new idea:

- 2020: draft-peeterr-dnsop-parent-side-auth-types
- 2024: draft-pwouters-parental-rrtype

These contain the same idea:
set aside a range of RR types for parent-side only use, specify a secure signal, propose changes needed to support it.
Please send suggestions to the DD list