CDS/CDNSKEY Consistency Is Mandatory

draft-thomassen-dnsop-cds-consistency

IETF 114 – DNSOP WG
July 28, 2022

Peter Thomassen (deSEC, Secure Systems Engineering)

The Problem

- RFC 7344
  - specifies automation of DS updates via
    - publication of CDS/CDNSKEY records at the child apex
    - for consumption by the parent (by polling)
  - **does not specify how the parent should be doing poll queries**

- Parent may be tempted to just use a (trusted) validating resolver
  - does not ensure that CDS/CDNSKEY records are compatible across authoritative servers

- In multi-homing setup: **single provider can unilaterally roll DS record set**
  - maliciously or accidentally
  - e.g. when rolling their own key, and then forgetting to publish other parties’ CDS/CDNSKEY

- Single provider **should not be in the position** to remove others’ trust anchors

Solution: Update RFC 7344

Proposed wording:

> “To retrieve a Child's CDS/CDNSKEY RRset for DNSSEC delegation trust maintenance, the **Parental Agent, knowing both the Child zone name and its NS hostnames, MUST ascertain that queries are made against all of the nameservers** listed in the Child's delegation from the Parent, and **ensure that the set of referenced keys is equal**.”

> “... When a key is referenced in the CDS or CDNSKEY record set **returned by one nameserver, but not referenced in the corresponding answers** of all of the other nameservers, the CDS/CDNSKEY state **MUST be considered inconsistent**.
> If an inconsistent CDS/CDNSKEY state is encountered, the Parental Agent **MUST take no action**. Specifically, it MUST NOT delete or alter the existing DS RRset.”

→ Would the WG be interested in adopting this?