CDS initial trust and delete

Paul Wouters RedHat
Ólafur Guðmundsson CloudFlare

draft-ogud-dnsop-maintain-ds-

RFC7344 says

- Parent can poll for CDS/CDNSKEY to keep in sync
- It says nothing about initial trust
- It’s silent on how to remove trust.

Why: Delete DS

- Does not want DNSSEC anymore
- Algorithm rollover
- DNS operator change
- DNS software change no import of old keys possible
- Other ??

How: Delete DS

- Publish single empty CDS/CDNSKEY record with DNSKEY algorithm 0
  - CDS 0 0 0
  - CDNSKEY 0 0 0
- Signed just like CDS
- After parent removes DS, child can turn off Signing

Initial Trust

- TOFU model: Trust On First Use ==> opportunistic
- Publishing CDS/CDNSKEY means ?
    - “Domain wants to enable validation, please help”
- Parent should honor this wish after due diligence
    - Checks that all Name servers agree
    - Monitor over some time period

If trigger is needed

- draft-latour-dnsoperator-to-rrr-protocol-00.txt
  - Simple REST call by “child” to request trust establishment.
  - Extra authentication can be applied here

Deployment

- Many DNS servers support by now.
- CloudFlare publishes CDS/CDNSKEY records for all signed zones.
- IETF hackathon CDS Monitor tool
  - https://github.com/fcelda/cds-monitor.git