Consistency for CDS/CDNSKEY (and CSYNC) is Mandatory

draft-thomassen-dnsop-cds-consistency

IETF 115 – DNSOP WG
November 8, 2022

Peter Thomassen (deSEC, Secure Systems Engineering)

Parent-Child Relationship: How Much Scrutiny is Needed?

- Via **CDS/CDNSKEY**, child tells parent which DS records to publish (RFC 7344)
  - Child publishes, parent consumes (discovery by polling)
  - Good for **DNSSEC-related delegation changes** (key rollovers, bootstrapping)
- Similarly, **CSYNC** signals which other data need update (RFC 7477)
  - Tells parent to fetch child-side records (e.g. NS or glue) and place it in the parent's delegation
  - Good for **non-DNSSEC delegation changes** (hostnames/glue, provider change)
- RFCs do not specify how the parent should be doing poll queries
  - Parent may be tempted to ask just one authoritative server
  - **Does not ensure that records are compatible** across auth servers
- What can possibly go wrong? 🤔

Failure Scenarios: **Multi-homing**

- DS breakage (multi-signer):
  - Provider performs key rollover
  - Accidentally publishes only their own CDS/CDNSKEY record set
  - When used by parent, other providers' keys are removed from chain of trust
    → **broken**

- NS breakage:
  - Provider publishes *incomplete* NS record set (e.g. after changing their hostnames)
  - Then requests update via CSYNC
  - When used by parent, other providers are removed from NS record set
    → **broken**

    … reduced to single-provider setup!

Failure Scenarios: **Provider Change**

- Provider change for secure delegation requires brief multi-signer period
  - Old provider imports new provider's DNSKEY/CDS/CDNSKEY (and vice versa)
  - Then update DS, then update NS

- What if new provider fails to sync CDS/CDNSKEY?
  - Both providers in NS, but new provider serves incomplete CDS/CDNSKEY (only their own)
  - When used by parent, old provider is removed from DS (but not yet from NS)
    → **broken**

❗ **Single provider should not be in the position to remove others' trust anchors** ❗

Better: **Ensure Consistency** before acting on C* Records

- **DNS resolution/validation breaks down** if a *single* provider makes a mistake
  - **Undermines multi-homing guarantees** (operator independence)
  - Can be solved if parent is careful!

- Proposal:
  - **Query** CDS/CDNSKEY/CSYNC (+ related records) **from all authoritative servers**
  - Disregard unresponsive servers
  - **Require consistency across responses**, otherwise abort (or retry)

Adopt draft-thomassen-dnsop-cds-consistency?