Consistency for CDS/CDNSKEY is Mandatory

ICANN 75 – DNSSEC Workshop
September 21, 2022

Peter Thomassen
peter.thomassen@securesystems.de

SSE

Parent-Child Relationship: How Much Scrutiny do you Need?

- Via **CDS/CDNSKEY**, child tell parents which DS records to publish (RFC 7344)
  - child publishes, parent consumes (discovery by polling)
- Similarly, **CSYNC** signals which other data (e.g. NS) 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 hostname and glue changes, and provider change
- RFCs do not specify how the parent should be doing poll queries
  - parent may be tempted to fetch records from just one authoritative server
  - does not ensure that CDS/CDNSKEY/CSYNC 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 the parent is careful!

- General strategy:
  - Query CDS/CDNSKEY/CSYNC (+ related records) **from all authoritative servers**
  - You may disregard unresponsive servers, or servers that say “I don’t serve CDS”
  - Otherwise, **require consistency across responses**
  - If you see an **inconsistency:** → **abort**

- Details: draft-thomassen-dnsop-cds-consistency

Questions?

Thank you!

Questions?