Operational Recommendations for DS Automation

draft-shetho-dnsop-ds-automation

IETF 123 – DNSOP WG
July 25, 2025

Steve Sheng, Peter Thomassen

Motivation

- CDS/CDNSKEY automation defined in RFCs 7344, 8078, 9615
- Number of loose ends:
  - validity checks, timing, error reporting, locks, etc.
- gTLD registries therefore currently are not allowed to deploy it
  - they have tried
- ICANN requires loose ends to be resolved first
  - Maximize interoperability
  - Minimize surprise

Loose ends (or: Operational Considerations from SAC126)

- What is the relationship with other registration parameters, like registry / registrar locks?
- What kind of validity checks should be done on DS parameters? Should those checks be performed upon acceptance, or also continuously when in place?
- How do TTLs / caching impact DS provisioning? How important is timing?
- Should DS automation involve the registrar or the registry, or both?
- How are conflicts resolved when DS parameters are accepted through multiple channels (e.g. via a conventional channel and via automation)?
- Should a successful or rejected DS update trigger a notification to anyone?
- These should be addressed (ideally consistently across TLDs)

Section 2: Validity Checks and Safety Measures

1. Entities performing automated DS maintenance SHOULD verify
    a. the consistency of DS update requests across all authoritative nameservers in the delegation [I-D.ietf-dnsop-cds-consistency], and
    b. that the resulting DS record set would not break DNSSEC validation if deployed,

    and cancel the update if the verifications do not succeed.
2. Parent operators (such as registries) SHOULD reduce a DS record set's TTL to a value between 5–15 minutes when the set of records is changed, and restore the normal TTL value at a later occasion (but not before the previous DS RRset's TTL has expired).

Section 3: Reporting and Transparency

1. For certain DS updates (see analysis (Section 3.2)) and for DS deactivation, relevant points of contact known to the zone operator SHOULD be notified.
2. For error conditions, the domain's technical contact and the DNS operator serving the affected Child zone SHOULD be first notified. The registrant SHOULD NOT be notified unless the problem persists for a prolonged amount of time (e.g., three days).
3. Notifications to humans SHOULD be done via email. Child DNS operators SHOULD be notified using a report query [RFC9567] to the agent domain as described in ([I-D.ietf-dnsop-generalized-notify], Section 4). The same condition SHOULD NOT be reported unnecessarily frequently to the same recipient.
4. In the RRR model, if the registry performs DS automation, the registry SHOULD inform the registrar of any DS record changes via the EPP Change Poll Extension [RFC8590] or a similar channel.
5. The currently active DS configuration as well as the history of DS updates SHOULD be made accessible to the registrant (or their designated party) through the customer portal available for domain management.

Section 4: Registration Locks

1. Automated DS maintenance SHOULD be suspended when a registry lock is set (in particular, EPP lock serverUpdateProhibited).
2. To secure ongoing operations, automated DS maintenance SHOULD NOT be suspended based on a registrar lock alone (in particular, EPP lock clientUpdateProhibited).

Section 5: Multiple Submitting Parties

1. Registries and registrars SHOULD provide a another (e.g., manual) channel for DS maintenance in order to enable recovery when the Child has lost access to its signing key(s). This out-of-band channel is also needed when a DNS operator does not support DS automation or refuses to cooperate.
2. When DS update requests SHOULD be executed immediately, whether they are received through EPP or another interface interface.
3. Only when the entire DS record set has been removed, SHOULD DS automation be suspended, in order to prevent accidental re-initialization of the DS record set when the registrant intended to disable DNSSEC.
4. In all other cases where a non-empty DS record set is provisioned out-of-band (e.g., manually) or via EPP (including after an earlier removal), DS automation SHOULD NOT (or no longer) be suspended.
5. In the RRR model, if the registry performs DS automation, the registry SHOULD notify the registrar of all DS updates (see also Recommendation 4 under Section 3).
6. In the RRR model, registries SHOULD NOT perform automated DS maintenance if it is known that the registrar does not support DNSSEC.

Section 6: CDS vs CDNSKEY

1. DNS operators SHOULD publish both CDNSKEY records as well as CDS records, and follow best practice for the choice of hash digest type [DS-IANA].
2. Parents, independently of their preference for CDS or CDNSKEY, SHOULD require publication of both RRsets, and SHOULD NOT proceed with updating the DS RRset if one is found missing or inconsistent with the other.
3. Registries (or registrars) scanning for CDS/CDNSKEY records SHOULD verify that any published CDS and CDNSKEY records are consistent with each other, and otherwise cancel the update [I-D.ietf-dnsop-cds-consistency].

Discussion

- Which of these recommendations are most contentious?

- Good discussion on the list. (Unresolved) suggestions received so far:
  - Section 2: Should validity/acceptance checks run periodically?
  - Section 3: Are email notifications really practical for error reporting? (What is the alternative?)
    - "in accordance with the communication preferences established by the child zone operator" to avoid being opinionated?

- Adoption?