Towards an Industry Best Practice for DS Automation

Barbara Jantzen <barbara@desec.io>
Peter Thomassen <peter@desec.io>

DNS OARC 45 – 7 October 2025 – Stockholm

DNSSEC validation rate

36%

vs.

secure delegation rate

8%

- Asia 32% (+4% since 2023)
- Oceania 54% (+11%)
- Africa 46% (+15%)
- Americas 37% (+4%)
- Europe 48% (+8%)

- 18% in top-1k domains
- 50–70% in some places
- **even for signed zones:**

< 50%

Global averages; sources: deSEC, https://stats.labs.apnic.net/dnssec, https://rick.eng.br/dnssecstat/, https://ithi.research.icann.org/graph-m11.html, https://stats.dnssec-tools.org/#/?tld_tab=3, https://dl.acm.org/doi/10.1145/3131365.3131373

DNSSEC has an accessibility problem.

Closing the Accessibility Gap through Automation

- **Full automation** can make DNSSEC **more accessible – and less error-prone**
- **CDS/CDNSKEY records** in the child zone indicate desired DS records
  - **For updates**, “old signs new" (**“old signs new”**, RFC 7344)
  - **For initialization**, use provider’s existing chain of trust (RFC 9615)
  - Efficiency improvement: allow child to nudge parent (instead of scanning; RFC9859)
- Successful parent-side implementations: .ch/.cr/.cz/.li/.se/.uz/.za/…
- **Different implementation choices regarding validity checks, locks, etc.**
  - Small differences in handling of details – but works!
  - This currently **blocks deployment for gTLDs** (but some would like to)

➢ Let’s develop **guidance new deployments**: draft-ietf-dnsop-ds-automation
  - Maximize interoperability, minimize surprise
  - Based on SAC126

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

Improvements from Monday workshop

1. For certain DS updates (see analysis (Section 3.2)) and for DS deactivation, relevant points of contact known to the parent entity SHOULD be notified.
2. For error conditions, the DNS operator and domain's technical contact (if applicable) SHOULD be first notified. The registrant SHOULD NOT be notified unless the problem persists.
3. Child DNS operators SHOULD be notified using a report query [RFC9567] (see [RFC9859]). Notifications to humans (domain holder) will be performed using the communication method established in accordance with the policies of the parent-side entity (registry or registrar). The same condition SHOULD NOT be reported unnecessarily frequently to the same recipient.
4. In the RRR model, registries performing DS automation 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 SHOULD be made accessible through the customer portal available for domain management. The DS update history MAY be made available in the same way.

Section 4: Registration Locks

1. To secure ongoing operations, automated DS maintenance SHOULD NOT be suspended based on a registrar update lock alone (such as EPP status clientUpdateProhibited).
2. When performed by the registry, automated DS maintenance SHOULD NOT be suspended based on a registry update lock alone (such as EPP status serverUpdateProhibited).

deSEC

Section 5: Multiple Submitting Parties

Monday workshop: Needs rewording

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. DS update requests SHOULD be executed immediately after verification of their authenticity, regardless of whether they are received in-band or via an out-of-band channel.
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.
4. In all other cases where a non-empty DS RRset is provisioned through whichever channel, automation SHOULD NOT (or no longer) be suspended (including after an earlier removal).
5. In the RRR model, registries SHOULD NOT perform automated DS maintenance if it is known that the registrar performs this function, or does not support DNSSEC at all.

deSEC

Section 6: CDS vs CDNSKEY

Monday workshop: Needs discussion

Improvements from Monday workshop

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. ~~Parents consuming 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].~~
   <Redundant from Section 2 Recommendation 1.b>

   Proposal: This Section really is about acceptance checks → **move to Section 2**

Thank you!

This project is supported
by the ICANN Grant Program.

Peter Thomassen
peter@desec.io

Backup

Loose ends (or: Operational Considerations from SAC126)

- Should DS automation involve the registrar or the registry, or both?
- 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?
- 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?