Towards an Industry Best Practice for DS Automation

Peter Thomassen <peter@desec.io>

ICANN 84 Tech Day – October 27, 2025

DNSSEC validation rate

36%

vs.

secure delegation rate

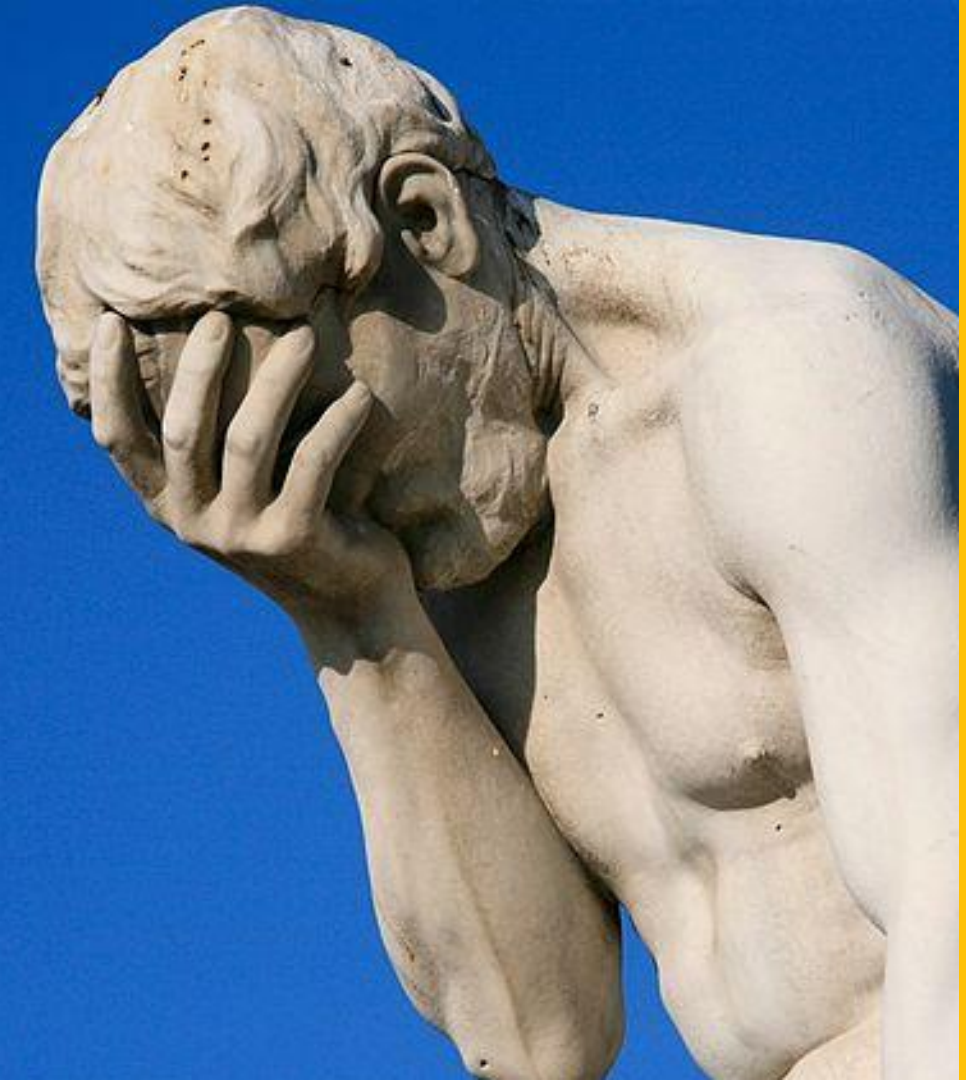
8%

- 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



deSEC

Is DNSSEC too hard?

(and scary?)

DNSSEC has an accessibility problem.

Closing the Accessibility Gap through Automation

- Initially (10 years ago): **Manual signing, manual key maintenance**
- Today: **Tooling available** for all of that
  - … including initialization of DS records
  - … and even automatic change of algorithm
- Next step: Automating of **DS provisioning**
- **Full automation** can make DNSSEC **more accessible – and less error-prone**
  - greatly **reduces overhead**
  - **enables things** like secure provider change (multi-signer transition)
- Number of **deployments increasing**, number of **incidents decreasing**

Technical Overview

- **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; RFC 9859)
- 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** (although there is interest)

➢ 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

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 will be performed in accordance with the communication preferences established with 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).

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. 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. When processing a CDS/CDNSKEY "delete" signal to remove the entire DS record set ([RFC8078]), DS automation SHOULD NOT be suspended. For all other removal requests, DS automation SHOULD be suspended, in order to prevent accidental re-initialization.
4. Whenever a non-empty DS record set is provisioned, through whichever channel, DS automation SHOULD NOT (or no longer) be suspended (including after an earlier removal).
5. In the RRR model, registries SHOULD disable automated DS maintenance if it is known that the registrar performs this function, or does not support DNSSEC at all.

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 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].
   <really an acceptance check – may move this one to Section 2>

Outlook

- Document adopted by IETF DNSOP WG
  - Draft: draft-ietf-dnsop-ds-automation
- Most issues settled, draft pretty stable
- Expect finalization over coming months

Open questions:

- Should registries suspend automation if the registrar has no DS removal interface?
- Should automating parties apply DS validity checks only when making a change, or also recheck periodically?

Questions?

This project is supported
by the ICANN Grant Program.

Peter Thomassen
peter@desec.io