

Operational Recommendations for DS Automation

[draft-ietf-dnsop-ds-automation](#)

IETF 124 – DNSOP WG
November 3, 2025

Steve Sheng, [Peter Thomassen](#)

Status

- Goal: Broad consensus on how to deploy DS provisioning automation
- Collected feedback from IETF and outside
 - ICANN Community (CPH TechOps, Tech Day, DNSSEC Workshop; to do: ASO)
 - APTLD, CENTR
 - ROW (Registry Operations Workshop)
 - DNS OARC
 - ...?
- Several issues resolved, draft converging

Changes since last IETF

- Humans should be notified according to preferences established with registry/registrar (not necessarily via email)
- Remove recommendation telling parents to require publication of both CDS and CDNSKEY
- Providing access to DS update history is now optional
- Clarify recommendation on suspension of automation after DS RRset removal and provide extra analysis

Open Questions

1. Should registries do automation if the registrar has no DS removal interface?

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.

- Pro argument: Enables DNSSEC for domains where it otherwise can't be enabled
- Con argument: Registrant cannot change or remove DS if needed (but can change registrar)
- Opt-in?

2. Should automating parties apply DS validity checks only when making a change, or also recheck periodically?

3. Should we keep Appendix C, on "Approaches not pursued"? Current content:

- Lowering TTL before an automatic DS update
- Parents requiring publication of both CDS and CDNSKEY