Towards DNSSEC Delegation Signer (DS) Record Automation

Update on SSAC DS Automation Report

ICANN 80 – DNSSEC and Security Workshop
June 10, 2024

Peter Thomassen

Motivation

- **DS record provisioning** is a crucial aspect of DNSSEC provisioning
- **Registries and registrars play critical role** in it
- **DS provisioning lacks automation**
  - Internal processes may be automated, but registrant faces idiosyncratic/disparate/ad-hoc processes
  - Especially when child uses a **third-party DNS service**
- **Important for …**
  - automatic initialization
  - provider transfer
  - multi-signer setups
- This is about facilitating efficient DS provisioning **for signed zones**
  - not: signing all zones

News

- Draft report **initially focused on CDS/CDNSKEY scanning**
- Discussions around scanning inefficiency brought **notification mechanisms** into focus
  - IETF draft on Generalized DNS Notifications being worked on (→ John Levine's talk)
- IESG has approved Authenticated DNSSEC Bootstrapping for publication
  - Addresses trust-on-first-use (TOFU) problem of CDS/CDNSKEY processing
- Taking above into account, report has pivoted towards **broader exposition of problem and solution space**

Status

- Work Party has been updating report for a higher-level perspective and in accordance with developments
- Findings and Recommendations being finalized
- Expect report before next ICANN meeting

Backup

Problem Statement

- The need for human intervention around setting up a domain name is **not aligned with registrants' expectations**, and **does not scale** sufficiently well when maintaining large domain portfolios.
- Non-automatic DS management has emerged as a major obstacle for broad deployment of DNSSEC. For example, studies have shown that **40% of registrants** who actively **requested zone signing** [...] did **not subsequently configure DS records** for their domain. As the number of domains [...] increased by a factor of three during the observation period [...], the fraction without DS records **remained stagnant at about 40%**.*

---

* See Figure 8 of https://conferences.sigcomm.org/imc/2017/papers/imc17-final53.pdf and related discussion.

DNS Provider Interface

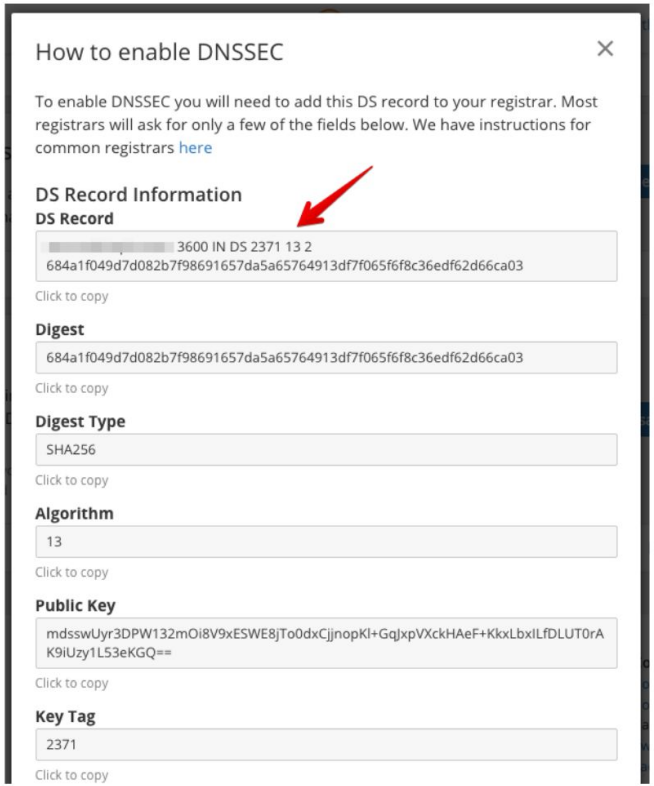

Figure 5. A DNS Operator's Interface for Registrant to Retrieve DS Record Information

Registrar Interface

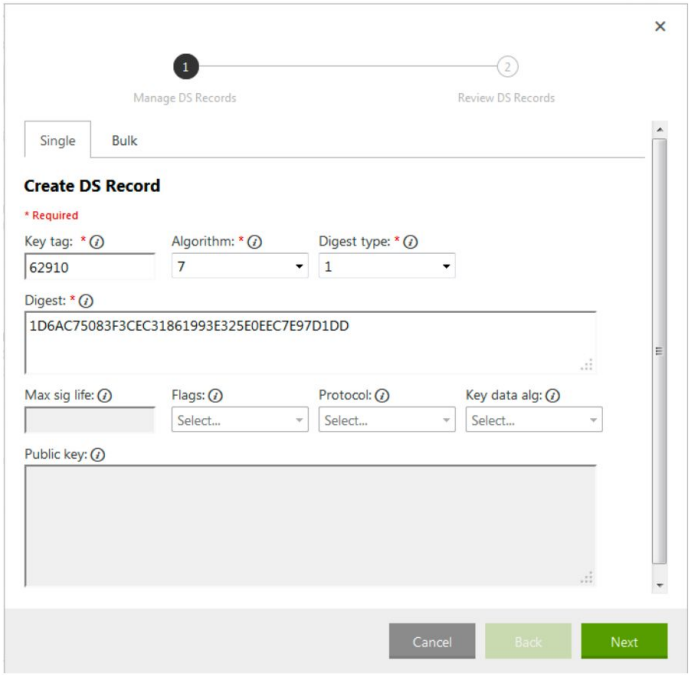

Figure 8. Another registrar's interface for registrants to create DS Record. It requires separate input of the various DS record components. Note that the numerical value of the Digest Type can be selected from a drop-down field (current selection: 1), whereas the Child DNS operator's interface used a mnemonic ("SHA256") for this field. The registrant would have to know that the correct choice in this case is 2. – The input fields in the lower half of the screenshot are all irrelevant.

DS Provisioning: Direct Interaction of Child & Parent (I)

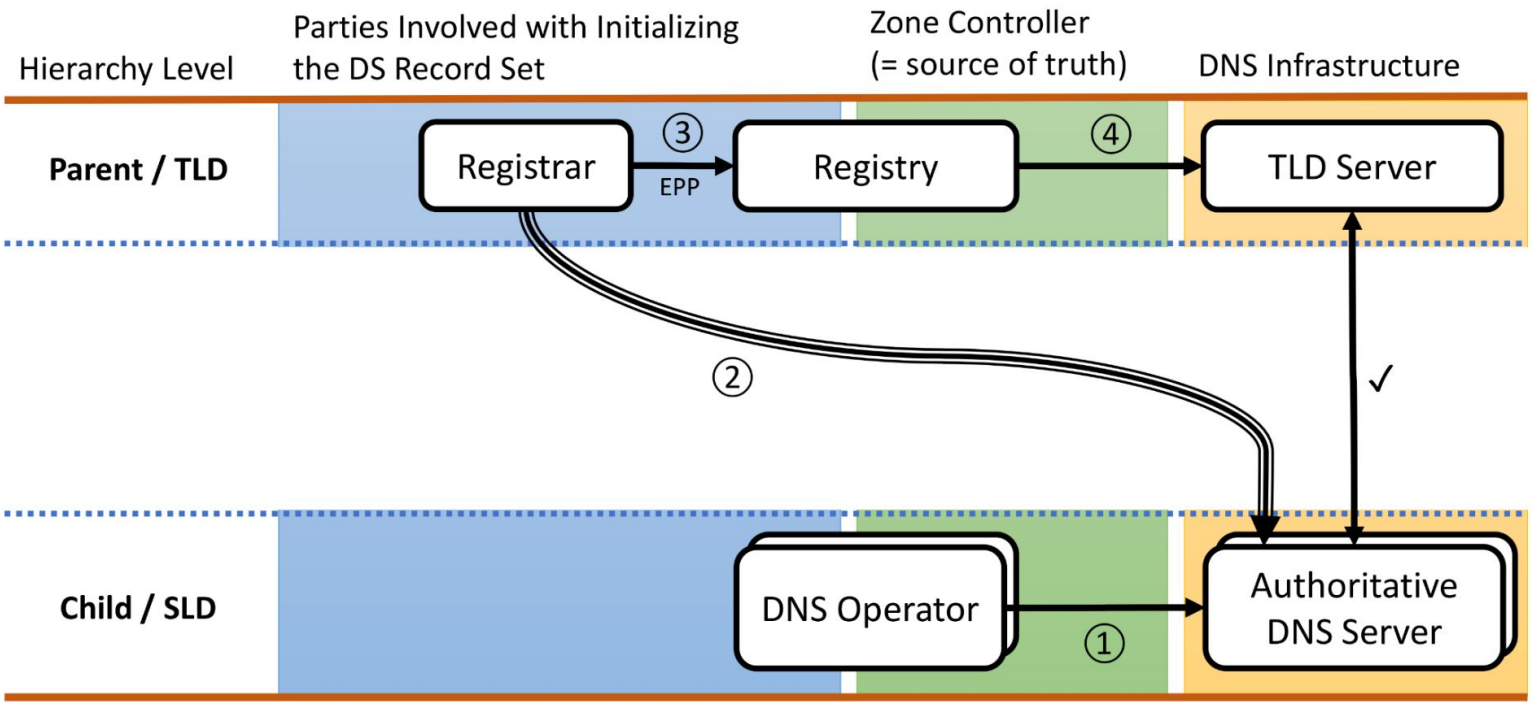

Figure 3. Simplified entity relationships during DS initialization with CDS/CDNSKEY

DS Provisioning: Direct Interaction of Child & Parent (II)

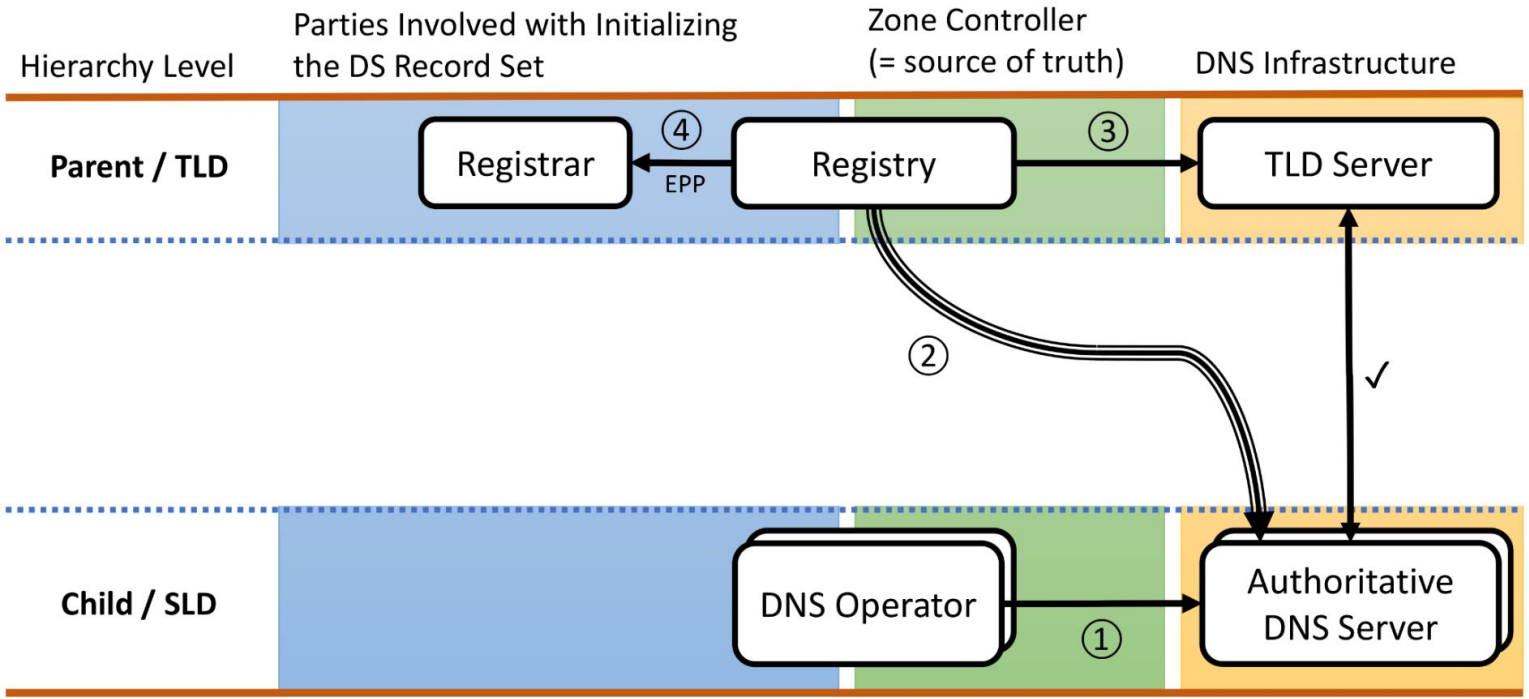

Figure 4. Simplified entity relationships during DS initialization with CDS/CDNSKEY

Operational Considerations

- For automation to work smoothly, several aspects need to be considered:
  - Scalability (Are parent-side scans impractical? Can notifications from the child improve it?)
  - Safety measures (e.g., acceptance checks, DS TTL policies)
  - Resolving submissions by multiple parties (e.g., CDS/CDNSKEY vs. manual submission)
  - Automation in the presence of locks?
  - Reporting of significant changes and errors
  - Consistency (e.g., CDS vs. CDNSKEY)
- These should be addressed, and ideally be handled consistently across TLDs
  - Above issues starting to get addressed by IETF (e.g., draft-ietf-dnsop-generalized-notify)