Towards an Industry Best Practice for DNSSEC DS Automation

Update on SSAC DS Automation Report

ICANN 78 – TechDay
October 25, 2023

Peter Thomassen

Motivation

- **Registries and registrars play a critical role in the DNSSEC ecosystem**
  - Their internal DNSSEC operations are mostly automated today
- However: **not much progress for automation of DS record provisioning**
  - **Especially** when the child uses a **third-party DNS service**
  - **Critical functionality** for glitch-free provider transfer + multi-signer setups → **missing piece**
- About 10 ccTLDs / 2 registrars / 1 RIR maintain DS records automatically
  - Also, authenticated bootstrapping (child: 3 DNS operators; parent: 2 ccTLDs, 1 registrar)
- There is a **gap in the gTLD space: no automation**
  - Lack of automation leaves only idiosyncratic / disparate / ad hoc processes
- **Note:** This is about facilitating efficient DS provisioning **for signed zones**
  - not: signing all zones

Key Findings (draft)

- In the registry-registrar-registrant (RRR) model, **when DNS service is provided by the registrar, the key change and subsequent DS update can be administered “internally”**, such as in direct interaction by the registrar with the registry via EPP.
- [... Otherwise], **DS records are typically deployed using the manual deployment method**, i.e., *Registrant Pull & Push*. This particularly applies to cases where the RRR model is in use, and **DNS service is not provided by the Registrar**.
- The manual method usually involves registrants submitting key information to their registrar, who in turn submits it to the registry. This first part of this process can be **onerous and error-prone**, and is often perceived as **frustrating and difficult**.

DS Provisioning: Registrant Pull & Push Method

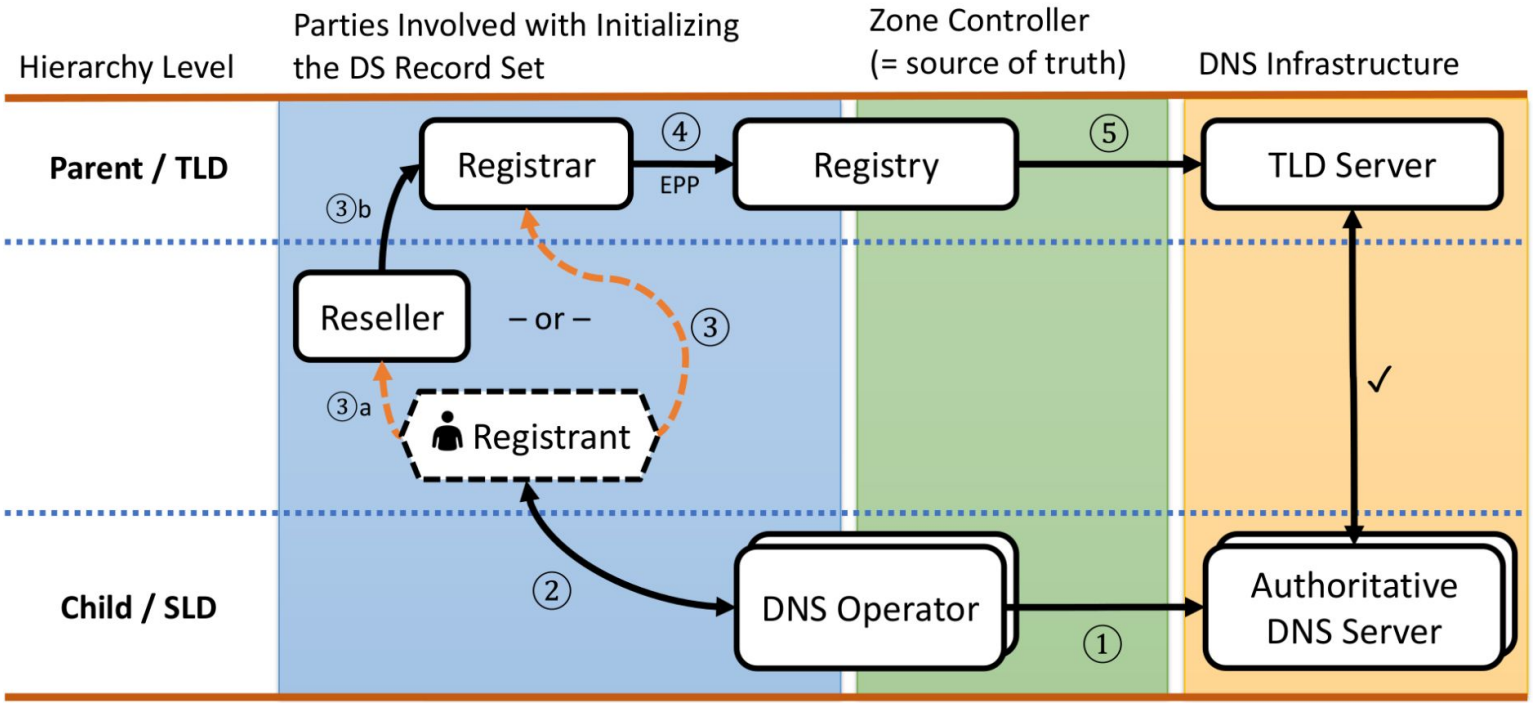

Figure 2. Entities and their relationships during DS provisioning.

DNS Provider Interface

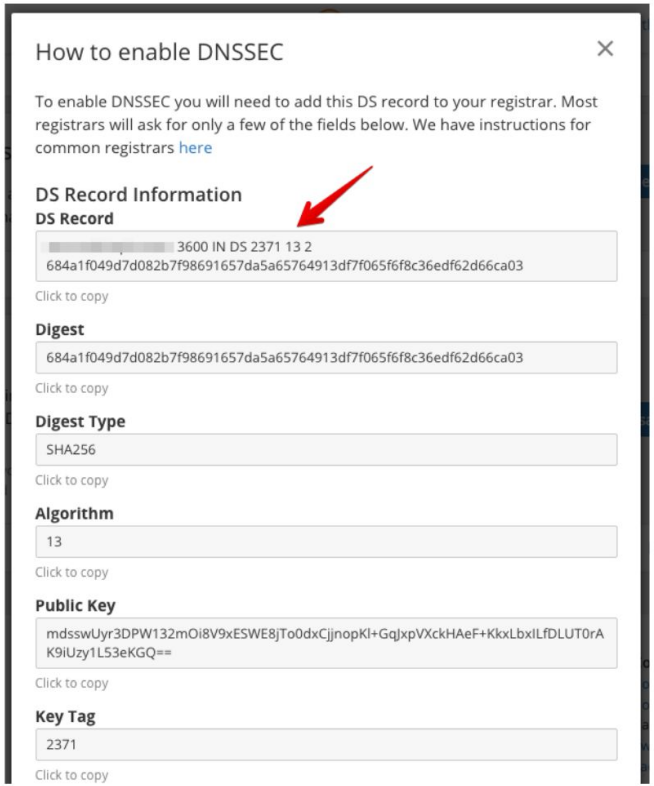

Figure 5. A DNS Operator's Interface for Registrant to Retrieve DS Record Information

Registrar Interface

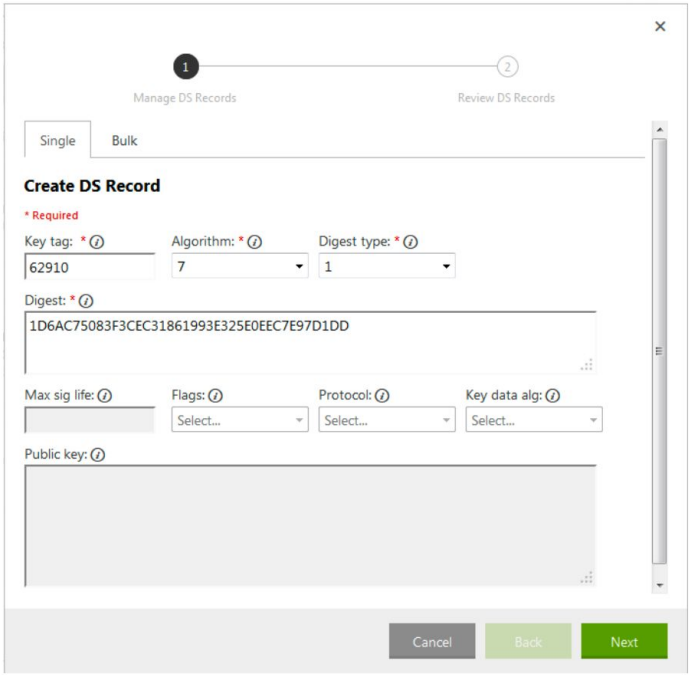

Figure 8. Another registrar's interface for registrants to create DS Record. It requires separate input of the various DS record components. Note that the numerical value of the Digest Type can be selected from a drop-down field (current selection: 1), whereas the Child DNS operator's interface used 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.

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.

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

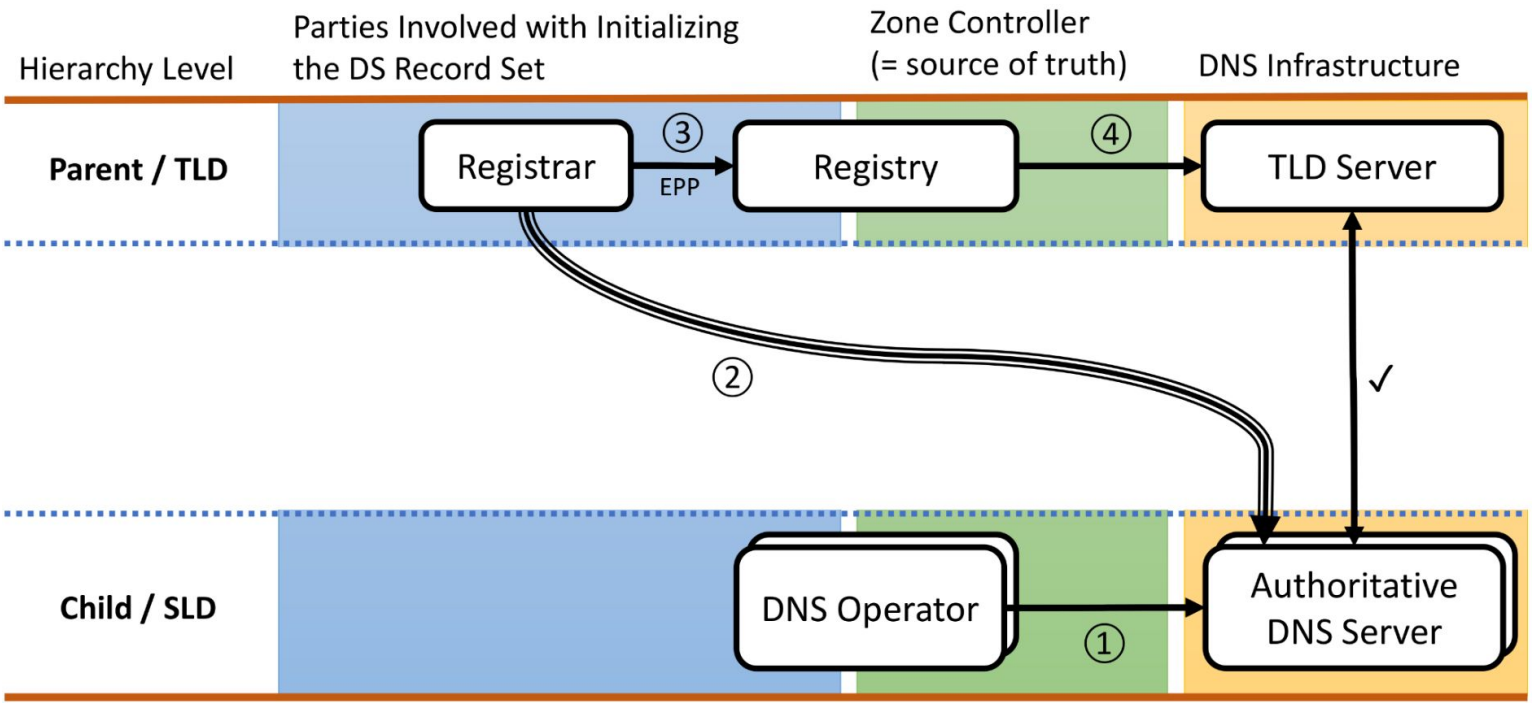

Figure 3. Simplified entity relationships during DS initialization with CDS/CDNSKEY

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

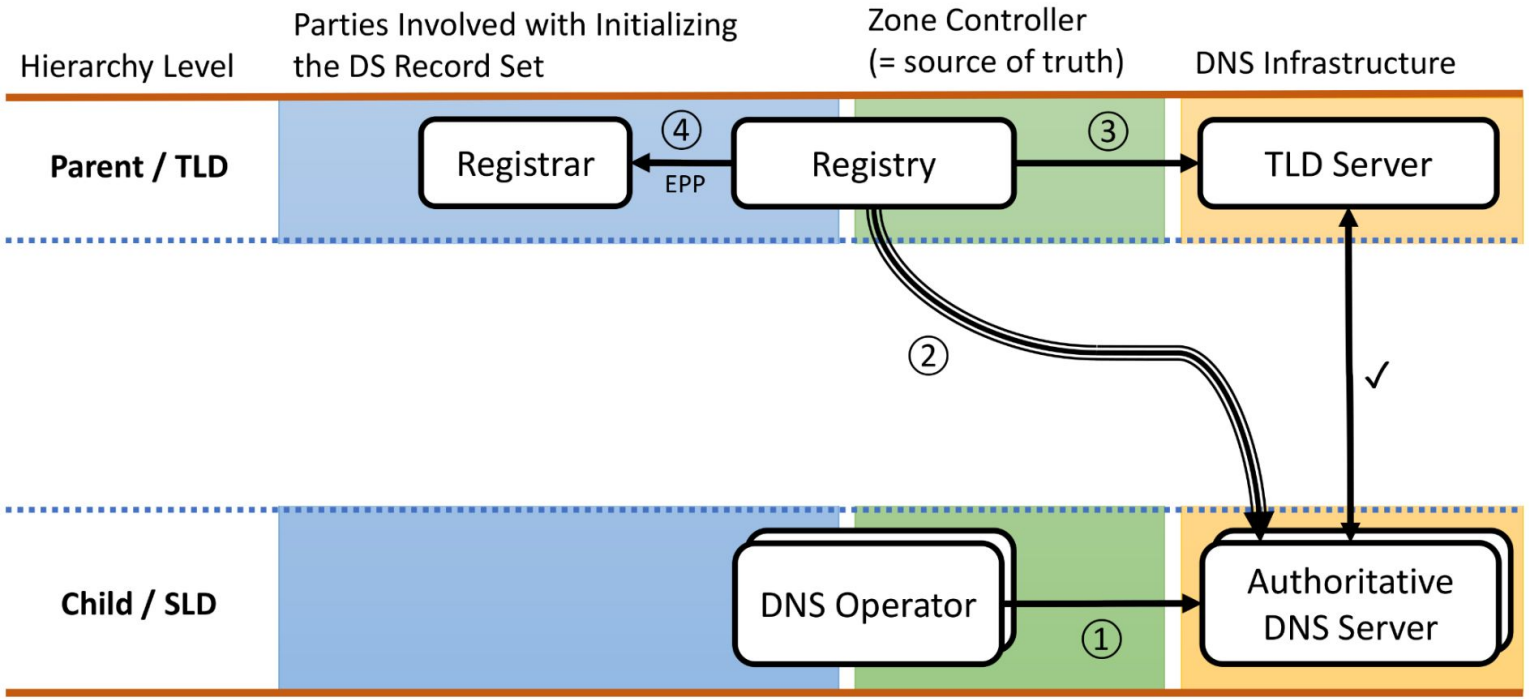

Figure 4. Simplified entity relationships during DS initialization with CDS/CDNSKEY

Current Thinking

- ICANN Org and thought leaders in the gTLD Ry/Rr community should **begin studying how to support DS automation**
- 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)