SSAC Report on DS Automation

SAC126

ICANN 81 – DNSSEC and Security Workshop
November 13, 2024

Peter Thomassen

Motivation: Registrant-centric Approach

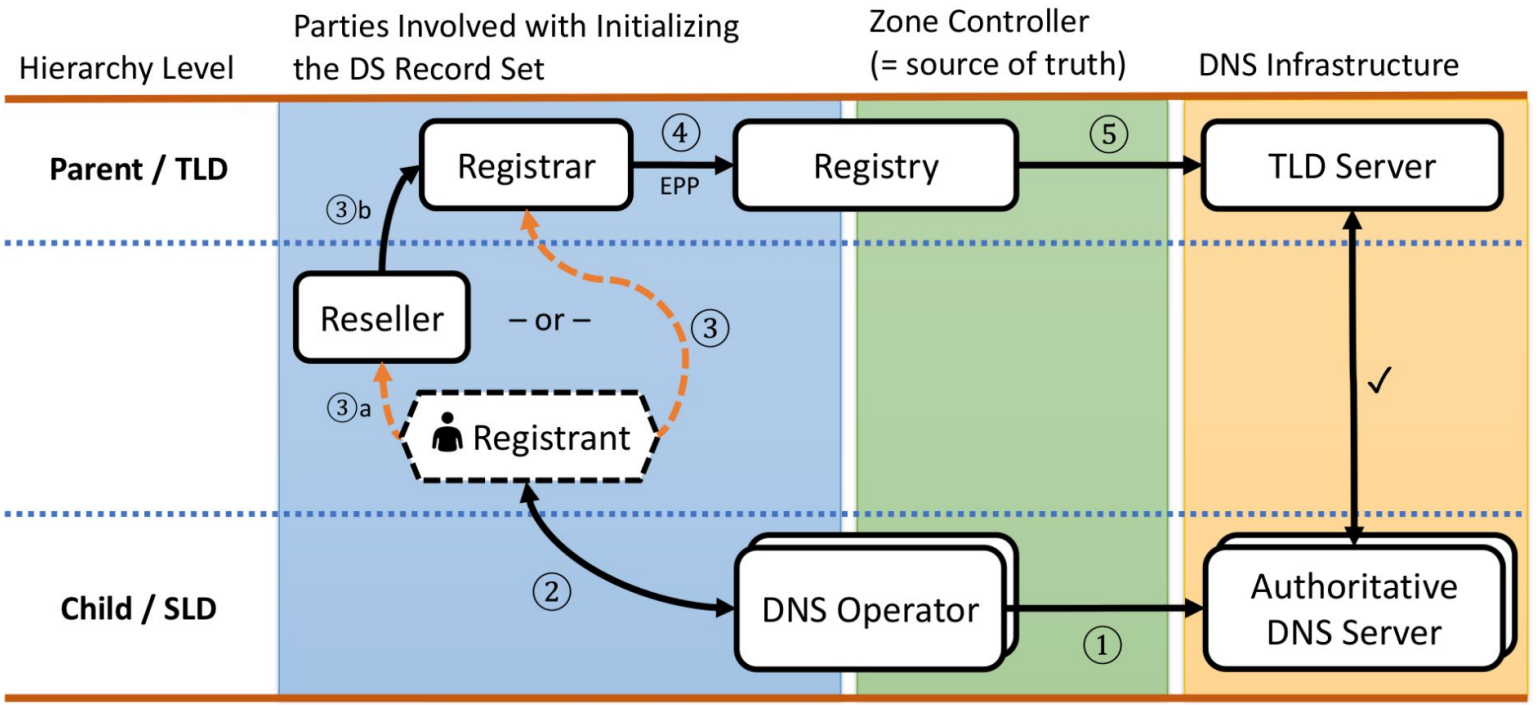

Figure 2. Entities and their relationships during DS provisioning.

Motivation

- **Registries and registrars play a critical role in the DNSSEC ecosystem**
  - Their internal DNSSEC operations are mostly automated today
- However, **users desiring DNSSEC are mostly left with manual DS record provisioning and management**
  - Especially when the child uses a third-party DNS service

- **Current Registrant-centric approach to DS management introduces significant complexity, idiosyncratic interfaces, and chance for error.**

- **The management of DS record sets should occur in a smooth, efficient, and faultless fashion.**
  - DS management automation can contribute to this goal.

Automated DS Management: Pull-based Approach (1)

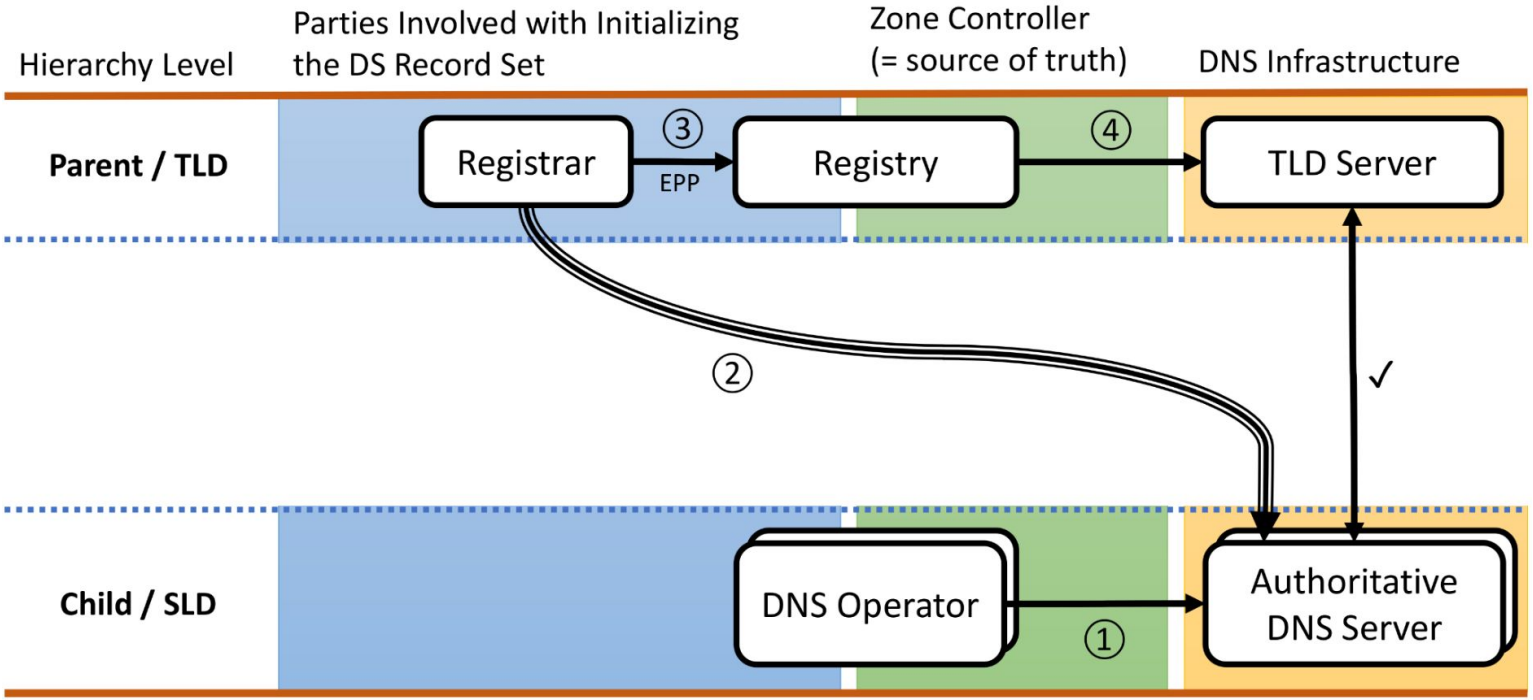

Figure 3. Simplified entity relationships during DS initialization with CDS/CDNSKEY

Automated DS Management: Pull-based Approach (2)

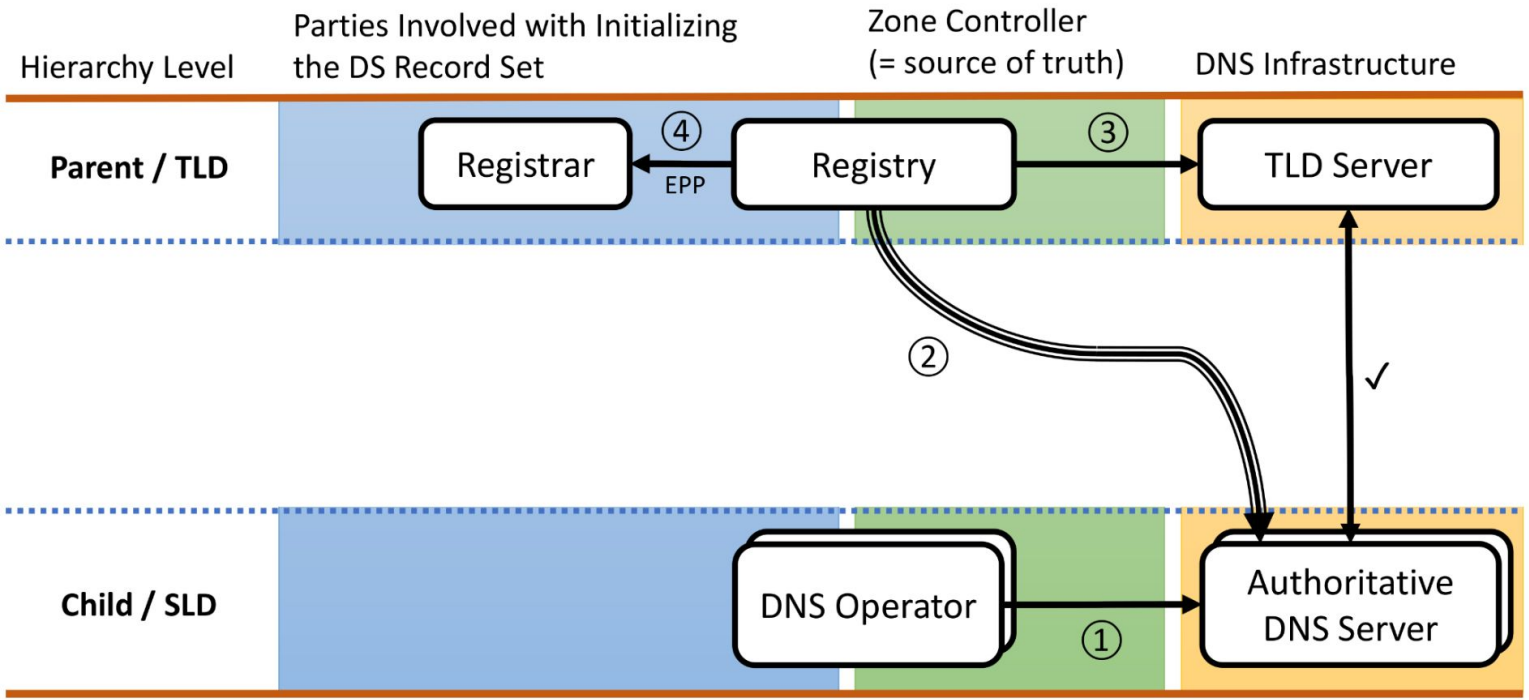

Figure 4. Simplified entity relationships during DS initialization with CDS/CDNSKEY

Automated DS Management: Overview

- **Pull-based Approach** (see previous slides)
  - IETF standards available (RFC 7344, 8078, 9615)
- **Pushed-based Approach:** The Child DNS operator would contact the registrar or registry and push the desired DS update directly into the parent-side system
  - needs credential provisioning
  - IETF standards not available
- **Hybrid Approach:** The Child DNS operator indicates that a new DS values are desired (push). The registrar/registry then retrieves them using pull-based method (e.g., by querying CDS/CDNSKEY records)
  - IETF standardization under way

Analysis of Solutions

Approach	Status	Pros	Cons
Registrant-centric	most commonly used		○ puts registrant in the coordinating role ○ complex and error prone
Pull-based Automation	RFC 7344, 9615; adopted by several ccTLDs	Internet standard and deployment experience	○ suffers from some inefficiency and delays related to scanning
Push-based Automation		Optimal efficiency (after trust is established)	○ requires credential provisioning ○ needs standards proposals ○ needs deployment
Hybrid Automation	standardization under way	Combines best of pull- and push-based automation	○ standardization not yet finished ○ needs deployment

Operational Considerations

- **For DS automation to work smoothly, several aspects need to be considered:**
  - Should DS automation involve the registrar or the registry, or both?
  - What kind of validity checks should be performed 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 DS update timing?
  - How are conflicts resolved when DS parameters are accepted through multiple channels (e.g. via a conventional channel and via automation)? In case both the registry and the registrar are automating DS updates, how to resolve potential collisions?
  - What is the relationship with other registration parameters, like registry/registrar locks?
  - Should a successful or rejected DS update trigger a notification to anyone?

- **These should be addressed, and ideally be handled consistently across TLDs**

Automated DS Management: Recommendations from SAC126

1. If a registry or a registrar wishes to implement DS automation for third-party DNSSEC operations, the current recommended interoperable mechanism is CDS/CDNSKEY (RFCs 7344, 9615). This mechanism has limitations as described in this document but has been deployed and there is operational experience in using it.

2. ICANN Org should support registries and registrars who want to implement DS automation using the mechanisms from Recommendation 1, such as by facilitating a Fast-Track RSEP.

3. ICANN org should facilitate the development of operational guidance for registries and registrars around the implementation of DS automation, in particular the operational aspects outlined in the report.