81 ANNUAL GENERAL MEETING

Insights from the SSAC:

An interactive session with the ICANN Community with updates from SSAC members on current projects and future priorities

Agenda

- Opening (Ram Mohan)
- A Year of Progress and Openness (Tara Whalen)
- Insights from SAC125: SSAC Report on Registrar Nameserver Management (Duane Wessels)
- Insights from SAC126: SSAC Report on DNSSEC Delegation Signer Automation (Peter Thomassen)
- Community Discussion (Ram Mohan)

A Year of Progress and Openness

Tara Whalen, SSAC Vice Chair

A Year of Progress and Openness at the SSAC

- **3 impactful reports in 2024**: DNS Security Extensions (DNSSEC) Automation, Name Collision Analysis, and Registrar Nameserver Management.
- **9 new SSAC members** with diverse backgrounds
- **Open SSAC meetings at ICANN**
- **SSAC workshop opened to community** on AI and DNS abuse, quantum computing, DNS and blockchain

SSAC: Nov 2024

Six Strategic Goals for SSAC 2024-2026

1. Enhance Quality and Relevance of SSAC Advice
2. Boost Engagement of Existing Members
3. Streamline Work Process and Timely Report Generation
4. Strengthen SSAC's Voice on Crucial Topics
5. Support Members' Expertise Expansion and Amplification
6. Enhance Diversity of SSAC Membership

5 Topics: The SSAC As An Authority

Intent

SSAC as an authority on key topics in ICANN

1	DNS Abuse	The most significant security issue facing our community.
2	New gTLDs	One of the largest strategic and tactical priorities for our community.
3	DNSSEC	A significant technology that improves DNS security. Still evolving.
4	Alternative Namespaces	New namespaces should want to integrate with the existing one. What are the issues?
5	Internet Governance & SSR	Add technical heft and provide meaningful advice for policy makers worldwide.

Insights from SAC125: SSAC Report on Registrar Nameserver (NS) Management

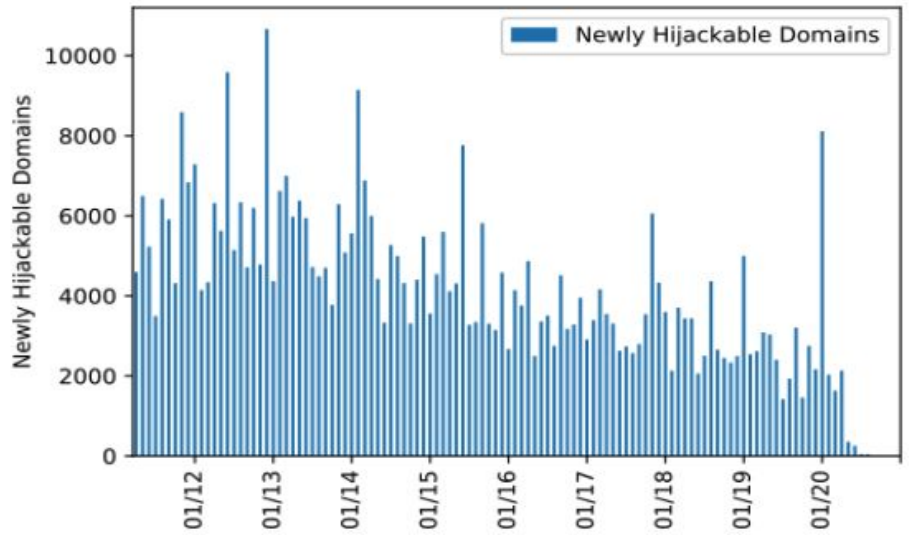
KC Claffy, Gautam Akiwate, Duane Wessels

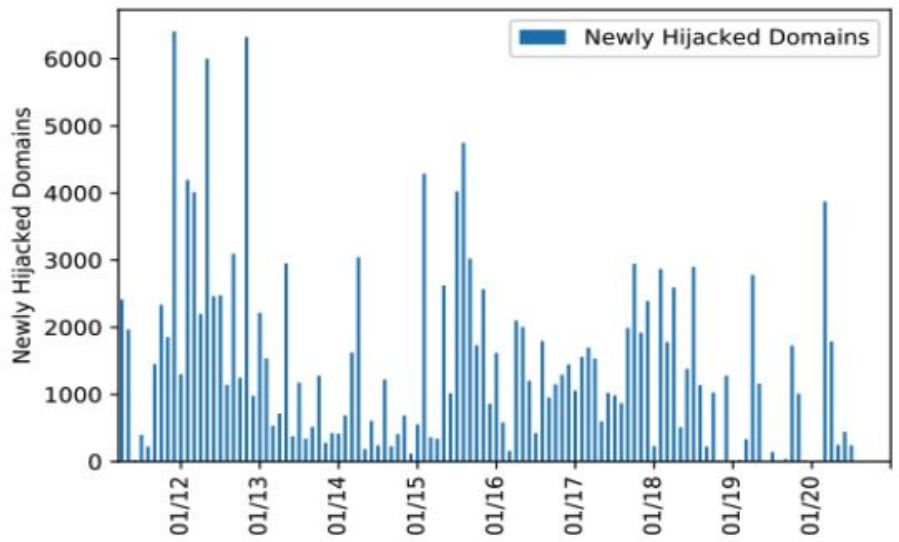
SAC125 - Problem Statement

- When a domain name registration expires, the domain cannot be deleted if other domains depend on it.
- A combination of Extensible Provisioning Protocol (EPP) advice and registry policies often prevents the simple deletion of a domain with subordinate host objects referenced by other domains **in the same registry**.
- Some registrars have been bypassing these restrictions by **renaming** subordinate host objects (outside of the registry), thus allowing removal of the expired domain.
- Renaming host objects can create **unsafe sacrificial name servers**.
- Malicious actors can register sacrificial name servers and take control of dependent domains.

SAC125 - Scale of the Issue

- SAC125 built on the risks identified in the paper ***Risky BIZness: Risks Derived from Registrar Name Management.***
- Between 2011 and 2020, nearly half a million domains were made vulnerable due to unsafe sacrificial name servers.
- Of these domains, nearly a third were resolution-hijacked.





SAC125: SSAC Report on Registar Nameserver Management

- Explored the risks that emerge from the expiration of domains that other domains rely on for authoritative name service.
- Investigated options for detection, remediation for domains that are currently exposed, and operational practices that will prevent new exposures.
- For each options to mitigate current exposures and prevent new exposures the SSAC reviewed.
  - ***Benefits*** of each option to registrars, registries, and registrants.
  - ***Burdens*** to registrars, registries, and registrants.
  - ***Residual risk*** if the option is implemented.

SAC125 - Parties That Could Remediate Exposed Domains

Acting Party	Benefits	Burdens	Residual Risks
Registrants	Maximum incentive alignment.	Registrants generally are not DNS experts and lack technical understanding of the need for remediation.	Low success rate
Registrars	Empowered to take action on behalf of registrant customers	Misplaced incentive	Reliance on third parties to identify exposed domains. Liability if mistakes occur
Registries	Could have biggest remediation impact	Misplaced incentive; don't normally initiate changes	Reliance on third parties; undesirable precedent
Third-Party Defensive Registrations	Minimal policy impact	Misplaced incentive, i.e., unclear who would maintain. Uncertain up-front and ongoing costs	No exit strategy

SAC125 - Options Explored to Prevent New Exposure

Delete Host Object:

- Relax registry requirements to allow host object deletion and the registrar would issue an EPP request to delete the host object.
- Drafting underway in IETF REGEXT.

Delete Host Object with Notification:

- Come up with a new cross-registry notification protocol and system.
- Notify dependent registrants of changes and avoid dangerous database inconsistencies.

Use empty.as112.arpa as shared sacrificial namespace:

- Rename hosts to unique values under empty.as112.arpa.
- Doesn't necessitate coordination among registries.
- Ensures that specific name server domains won't be registered by others.

Per-Registrar Non-registerable Sacrificial Namespace:

- Registrars create sinkhole domains for hosting a sacrificial name server.

Global / Community Non-registerable Sacrificial Namespace:

- Registrars utilize a third-party service provider for a global sinkhole name server to cut costs and potentially reduce risks.
- ICANN Org may select an entity or itself manage this name server.

Use Reserved TLDs or Special-Use Domain names:

- Utilize a reserved TLD, such as .invalid, for naming sacrificial name servers.
- ICANN might create a dedicated TLD like .sacrificial for this use.

SAC125 - Recommendations

1. The ICANN registry and registrar communities collaborate to develop and implement a comprehensive code of conduct to mitigate the risks associated with registrable (unsafe) sacrificial nameservers.

2. ICANN Org should design, develop, and regularly publish aggregated statistics specifically focused on the prevalence of unsafe sacrificial nameservers and the effectiveness of different mitigation measures.

3. ICANN Org should directly engage with registries and registrars to assist in mitigation and prevention efforts based on the insights gleaned as a result of implementing Recommendation 2.

Insights from SAC126: SSAC Report on DNSSEC Delegation Signer (DS) Automation

Peter Thomassen

Motivation: Registrant-centric Approach

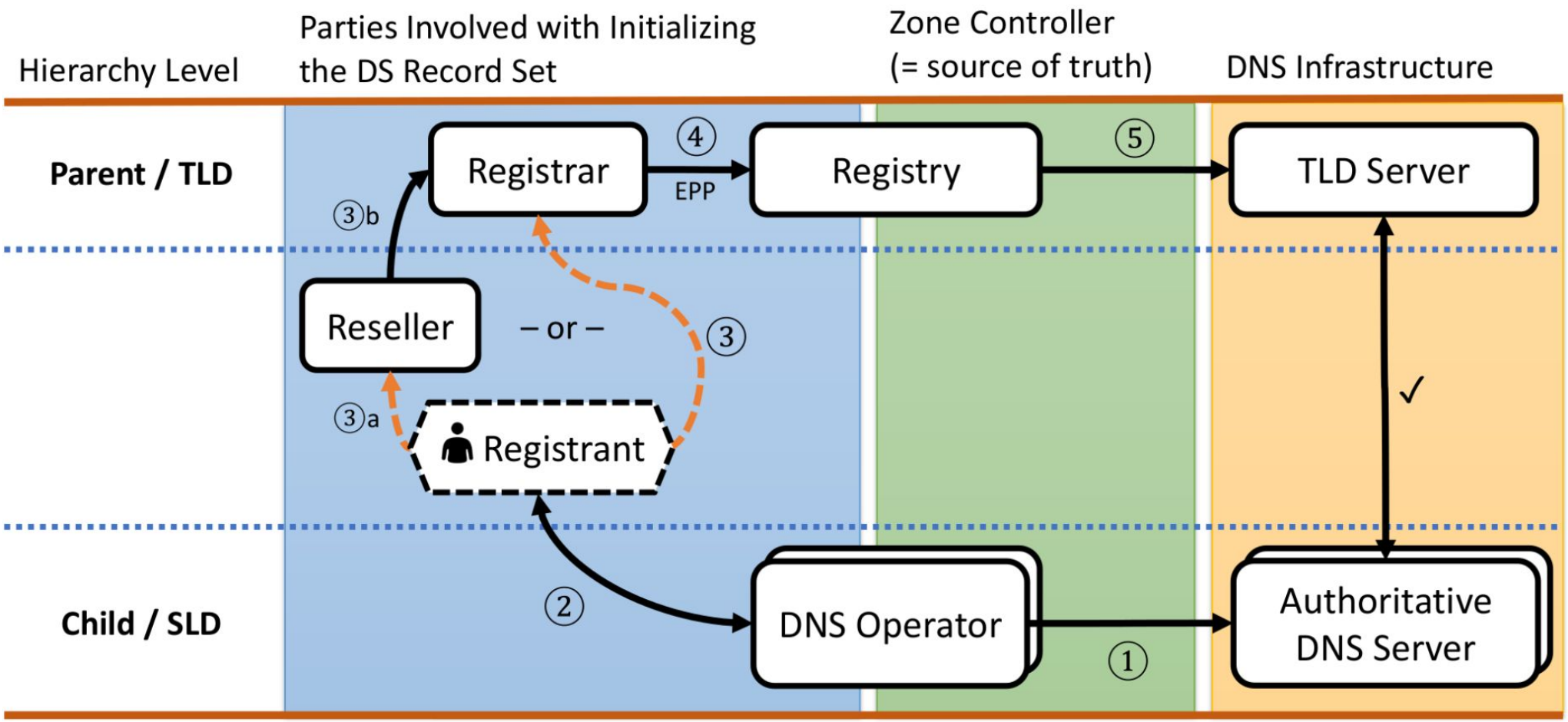


Figure 2. Entities and their relationships during DS provisioning.

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**
- **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)

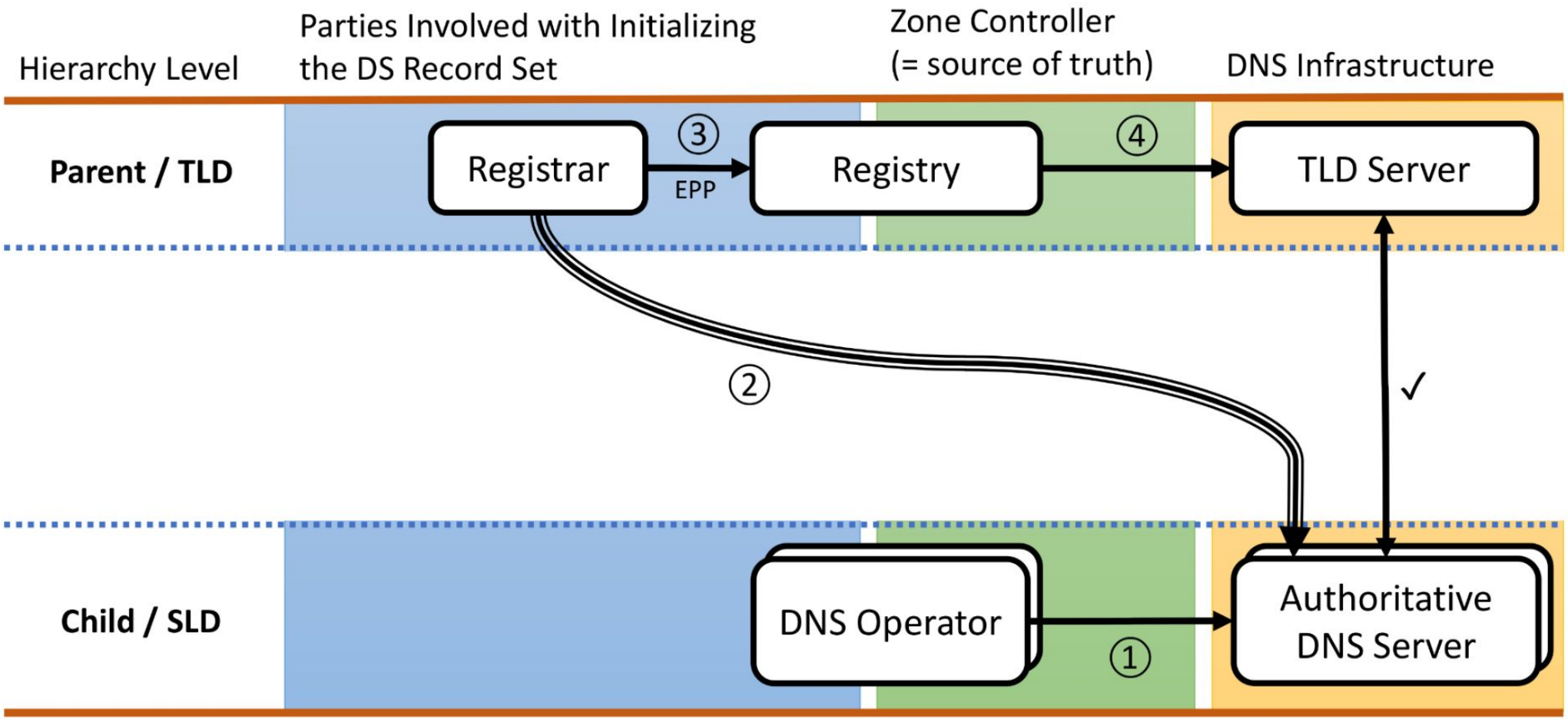


Figure 3. Simplified entity relationships during DS initialization with CDS/CDNSKEY

Automated DS Management: Pull-based Approach (2)

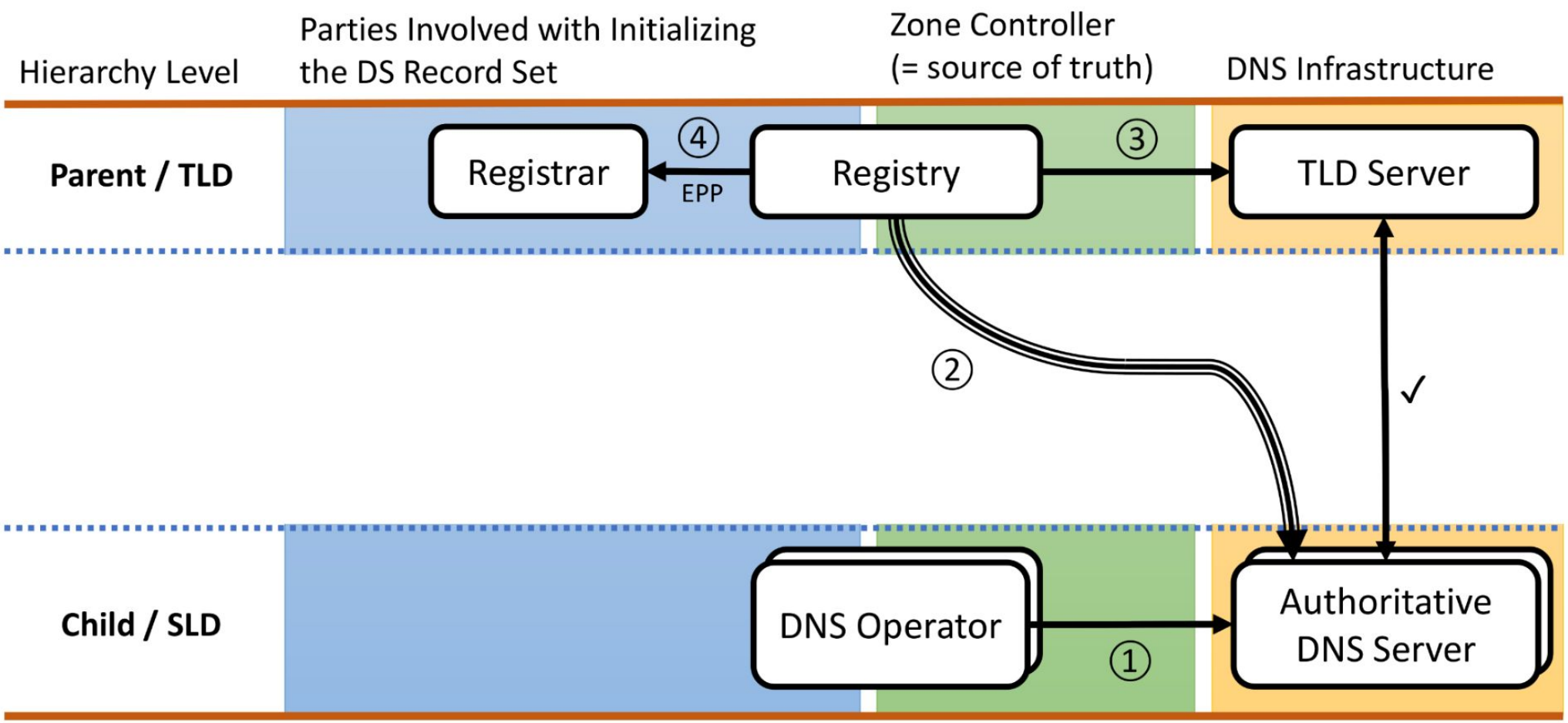


Figure 4. Simplified entity relationships during DS initialization with CDS/CDNSKEY

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

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.

Summary

Ram Mohan

Summary

Openness and Progress → Always a work in progress!

SAC126: DNSSEC DS Automation → Automation could help streamline DNSSEC management

SAC125: Registrar NS Management → Closing the info gap on security risks in managing expired domains.

Questions for the SSAC?