Automation of DS Management: Status and Developments

ICANN 75 – DNSSEC Workshop
September 21, 2022

Peter Thomassen
peter.thomassen@securesystems.de

SSE

DNSSEC validation rate

31 %

- globally
- 50–95% in some places

vs.

secure delegation rate

6 %

- globally
- 50–70% in some places
- **even for signed zones:**

< 50%

Sources: deSEC, https://stats.labs.apnic.net/dnssec, https://rick.eng.br/dnssecstat/, https://www.sidn.nl/en/news-and-blogs/dnssec-adoption-heavily-dependent-on-incentives-and-active-promotion

Why are so few Delegations Secure?

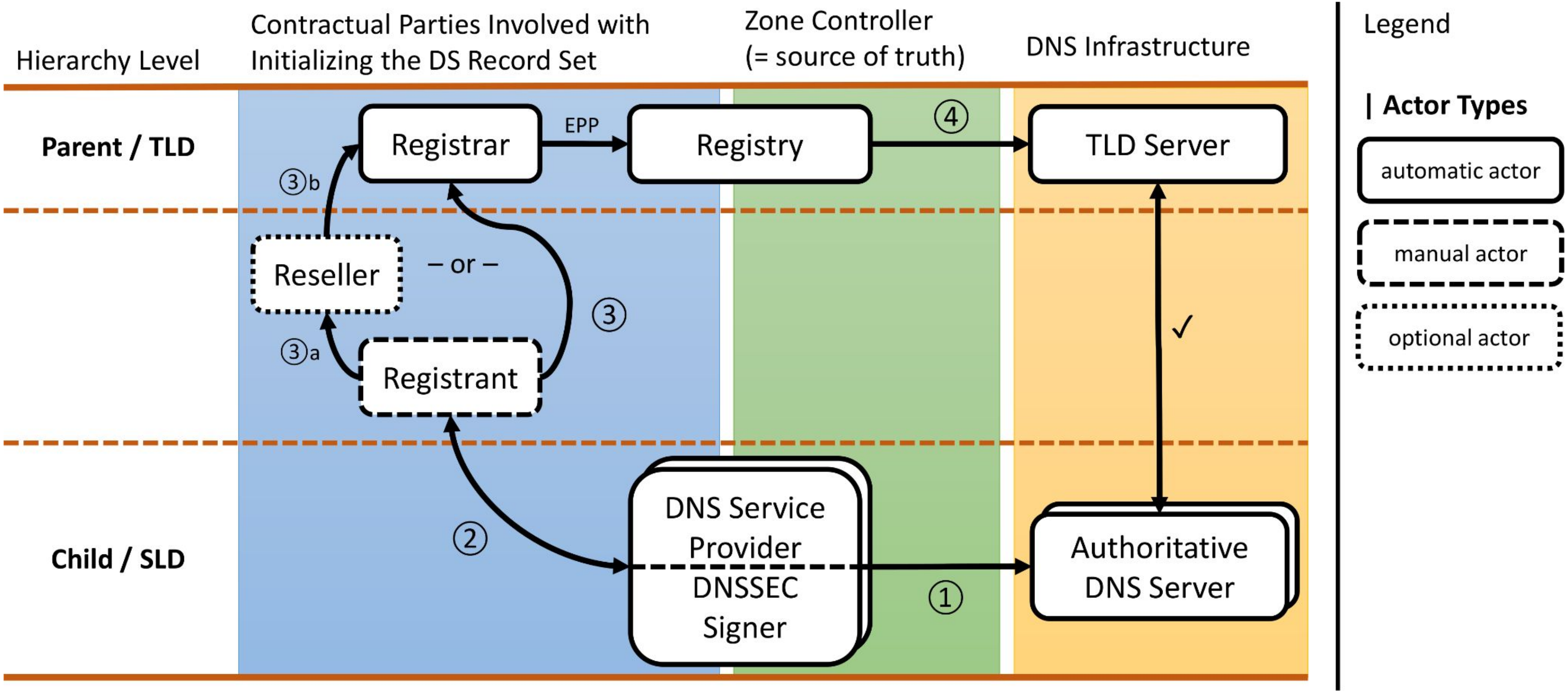
- Deploying DS records is a **multi-party problem**
  - involving the DNSSEC signer (origin) and the parent Registry (recipient)
  - … and often the Registrar as the messenger,
  - … typically facilitated through the Registrant

- Error-prone, (too) many parties, slow, out of band, not properly authenticated
  → **needs automation!**

- Any **automation must involve the source of truth**
  - typically the DNS operator

  → **facilitate independent participation of DNS operators**

Traditional DS Deployment



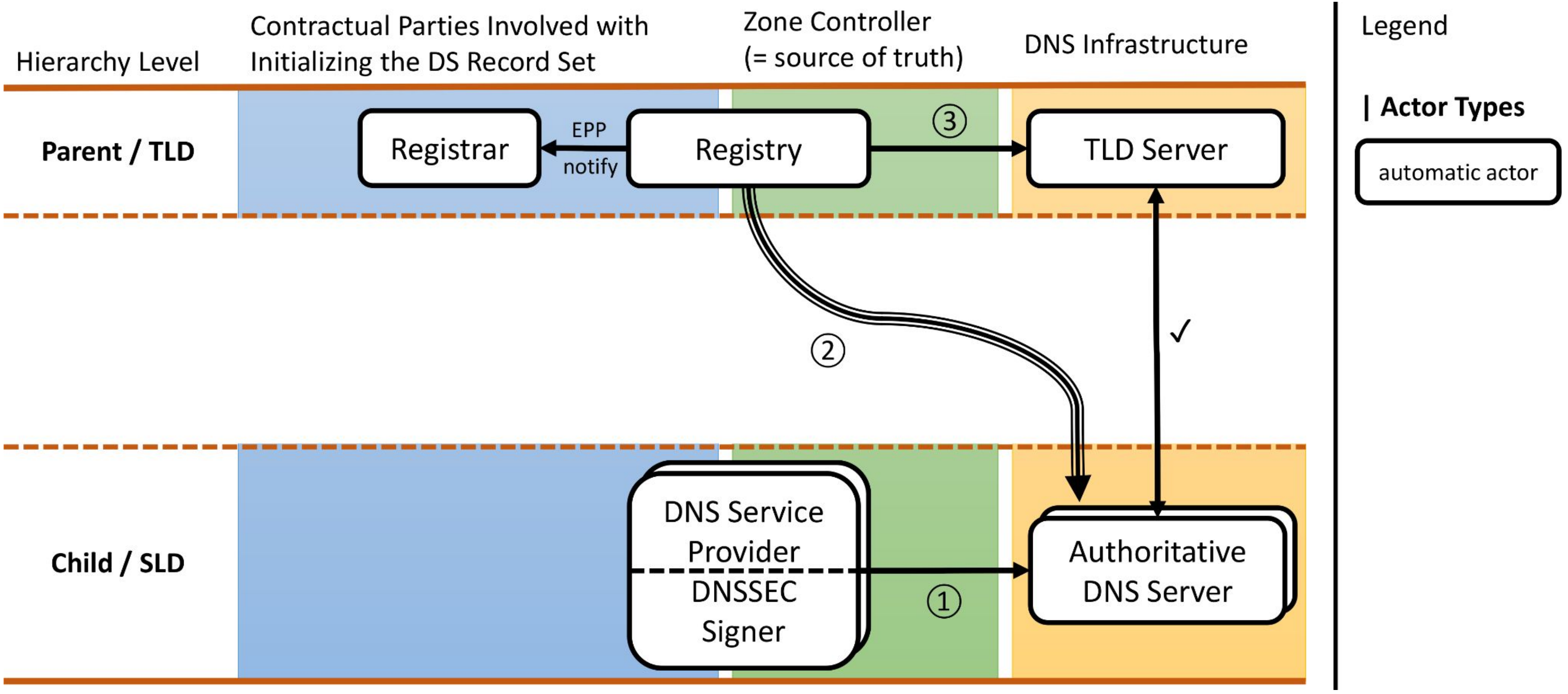
□ CDS/CDNSKEY to the Rescue!

- Idea: **CDS/CDNSKEY records** at Child zone apex (next to SOA record)
  - can be proactively discovered by parent
  - needs consistency across nameservers to avoid harm (draft-thomassen-dnsop-cds-consistency)

- **Authentication during bootstrapping:** draft-ietf-dnsop-dnssec-bootstrapping
  - operator **co-publishes CDS/CDNSKEY records** at subdomains **under NS hostnames**
  - uses pre-existing DNSSEC chain of trust of these “proxy domains” for validation
  - (RFC 8078 in 2017 allowed consuming CDS/CDNSKEY without cryptographic authentication)

- **Authentication for rollovers:** RFC 7344 (published in 2014)
  - authentication via child's existing chain of trust
  - just validate CDS/CDNSKEY records like any other record

CDS/CDNSKEY-based Deployment



Current State of DS Automation

Child-side (= publication of CDS/CDNSKEY records):

- Supported by **4 DNS operators**, covering **significant fraction of zones**
  - insecure bootstrapping (child apex only): *DNSimple*, *GoDaddy* (+ some I don't know?)
  - authenticated bootstrapping (= co-publication under NS hostname): *Cloudflare*, *deSEC*

Parent-side (= CDS/CDNSKEY scanning):

- supported by **7 ccTLD registries**
  - insecure bootstrapping (5): Costa Rica (.cr), Czechia (.cz), Niue (.nu), Sweden (.se), Slovakia (.sk)
  - authenticated bootstrapping (2): Switzerland (.ch), Liechtenstein (.li)
- GoDaddy planning to perform **CDS/CDNSKEY scanning as a Registrar**

Source: https://github.com/oskar456/cds-updates

SSAC DS Automation Work Party

- Reminder: **“facilitate independent participation of DNS operators”**

- SSAC established the “DS Automation Work Party” to tackle this problem
  - targeted at **registries, registrars, and DNS service provider** industry
  - **survey methods** used for DS record management and related tasks
  - **explain** issues, ways of managing DS (with upsides/downsides) and current state of things
  - **provide recommendations** to facilitate automatic initialization/updating of DS records

- Status:
  - developed survey, data collection under way
  - preparing advisory document (early stage)

Thank you!

Questions?