The State of DS Automation

Deployments and Current Work

ICANN 76 – DNSSEC Workshop
March 15, 2023

Peter Thomassen
peter.thomassen@securesystems.de

SSE

DNSSEC validation rate

32 %

- globally
- 50–95% in some places

vs.

secure delegation rate

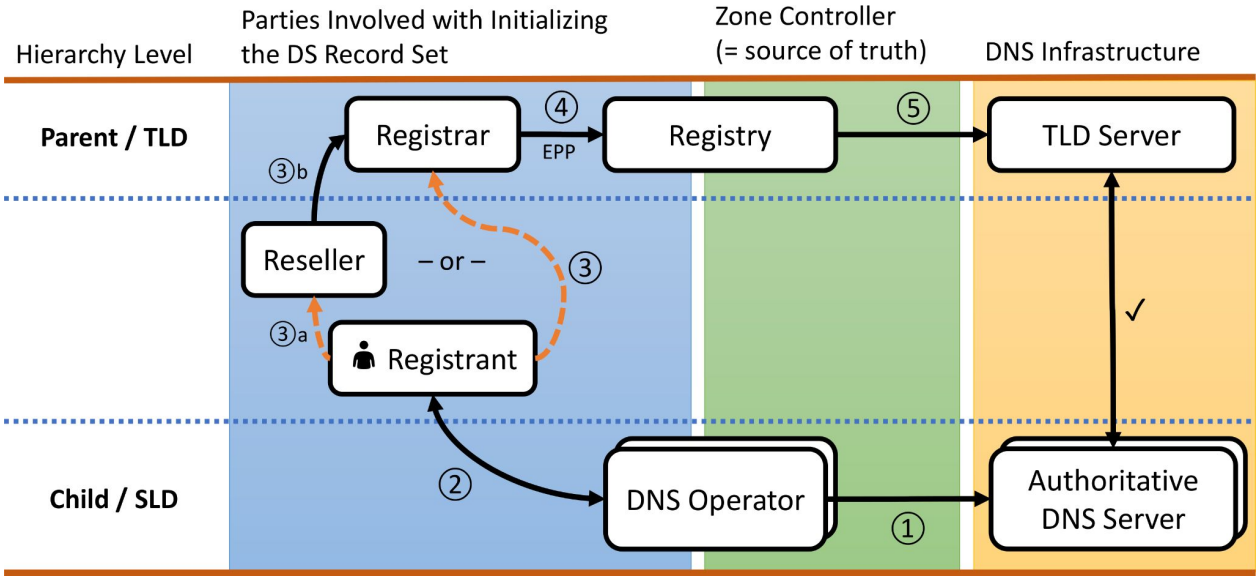
7 %

- SLDs 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

Traditional DS Deployment is a Multi-Party Problem

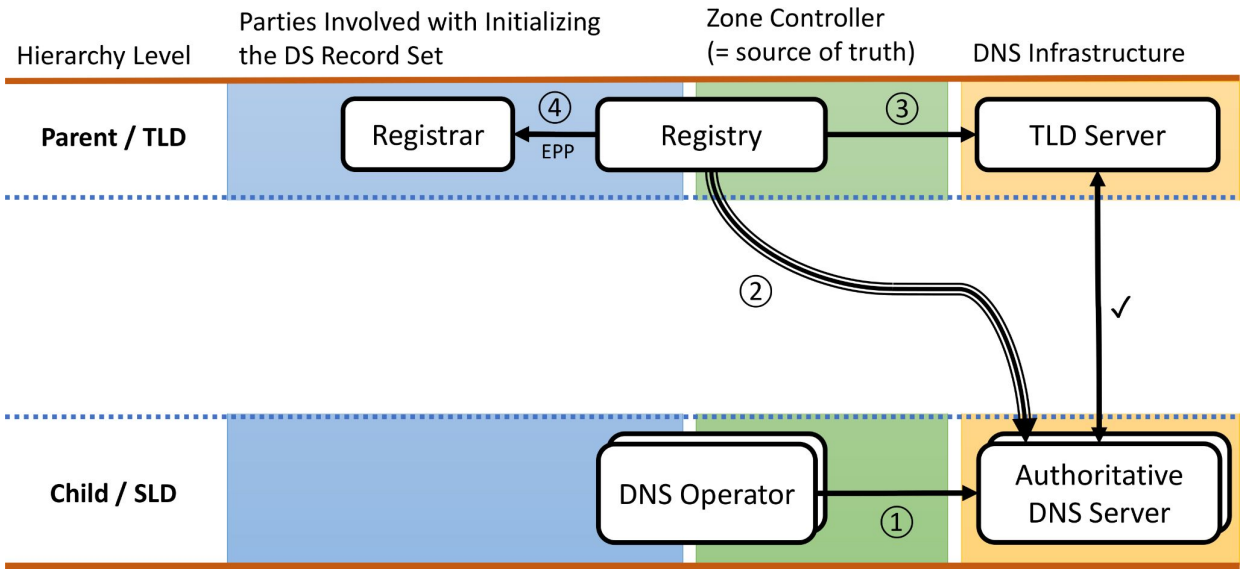


- Slow
- Error-prone
- Out of band
- Not properly authenticated

- Involves the Child DNS Operator (origin) and Parent Registry (recipient)
  - … typically with the Registrar as the messenger
  - … typically facilitated through the Registrant

CDS/CDNSKEY to the Rescue

- Let's take a shortcut!
- Authorized via signal from Registrant
  - No manual dealing with cryptographic params
- Known timing
- Authenticated



Current State of Deployment: Child Side

- Supported by **5 DNS operators**
  - insecure bootstrapping (2): *DNSimple*, *GoDaddy* (+ some I don't know?)
  - authenticated bootstrapping (3): *Cloudflare*, *deSEC*, *Glauca HexDNS*
  - … all of them support rollovers

- Authoritative Nameservers
  - rollovers, insecure bootstrapping: PowerDNS, Knot DNS, BIND, …
  - authenticated bootstrapping:
    - LUA extension available for *PowerDNS*
    - Extension for *Knot DNS* under development (NLnet Foundation)

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

Current State of Deployment: Parent Side

- Supported by **7 ccTLD registries**
  - insecure bootstrapping (7): Costa Rica (.cr), Czechia (.cz), Faroe Islands (.fo), Niue (.nu), Sweden (.se), Slovakia (.sk), {.alt,.edu}.za
  - authenticated bootstrapping (2): Switzerland (.ch), Liechtenstein (.li); Chile (.cl) planning
- Supported by **2 gTLD registries**
  - authenticated bootstrapping (2): .swiss, .whoswho
- Supported by **CentralNic**
  - insecure bootstrapping for SLDs like .de.com, .uk.net
- Support by **2 registrars**
  - insecure bootstrapping (2): Domainnameshop, Glauca (both plan to add authentication)
  - GoDaddy planning implementation

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

DS Automation: Considerations

- When a zone is signed, the Registrant apparently wants DNSSEC
  - Even more so when an “intent for DS update” is signaled

DS Automation: Considerations

- When a zone is signed, the Registrant apparently wants DNSSEC
  - Even more so when an “intent for DS update” is signaled

Relevant Specifications:

- **Bootstrapping:** draft-ietf-dnsop-dnssec-bootstrapping (updates RFC 8078)
- **DS rollovers:** RFC 7344
- Ongoing developments
  - Better consistent than sorry: draft-thomassen-dnsop-cds-consistency
  - Optimize timing/cost trade-off: draft-thomassen-dnsop-generalized-dns-notify

DS Automation: Considerations

– – –

- When a zone is signed, the Registrant apparently wants DNSSEC
  - Even more so when an “intent for DS update” is signaled

Relevant Specifications:

- **Bootstrapping:** draft-ietf-dnsop-dnssec-bootstrapping (updates RFC 8078)
- **DS rollovers:** RFC 7344
- Ongoing developments
  - Better consistent than sorry: draft-thomassen-dnsop-cds-consistency
  - Optimize timing/cost trade-off: draft-thomassen-dnsop-generalized-dns-notify

Issues: EPP contention, locks interaction, error reporting, …

❗ **Consistent treatment** across Registries → **Avoid registrant confusion** ❗

SSAC DS Automation Work Party

SSAC's "DS Automation Work Party" studying the problem space

- **Collected data** on current DS automation practices
- **Investigating related issues**, such as EPP/CDS contention, locks interaction, error reporting
- **Preparing** advisory document

Considerations:

1. When the DNS Operator is not the same entity as the Registrar, the customary DS provisioning method is onerous and error-prone. It is perceived as frustrating and difficult, and not completed by 40% of Registrants.[1] This has become one of the choke points for DNSSEC adoption.

[1] Source: https://conferences.sigcomm.org/imc/2017/papers/imc17-final53.pdf

SSAC DS Automation Work Party: Considerations (cont.)

2. For many TLDs, DNSSEC operation is not automated from the Registrant's point of view, even though pieces of the infrastructure are. This is contrary to Registrants' expectations.

3. Recent protocol developments[2] created new mechanisms for automating the DS provisioning multi-party process, using signaling records published by the DNS Operator and consumed by the parent. The mechanism has working production implementations by several ccTLDs and Registrars.[3]

4. Enabling support for automatic acceptance of DS parameters directly from the Child DNS Operator requires the Registry/Registrar to make a number of technical decisions.

[2] RFC 7344, RFC 8078, draft-ietf-dnsop-dnssec-bootstrapping
[3] https://github.com/oskar456/cds-updates

Thank you!

Questions?