Automatic DNSSEC Bootstrapping with Authentication

ICANN 75 – Tech Day
September 19, 2022

Peter Thomassen <peter@desec.io>
Nils Wisiol <nils@desec.io>

draft-ietf-dnsop-dnssec-bootstrapping

DNSSEC validation rate

32%

- 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

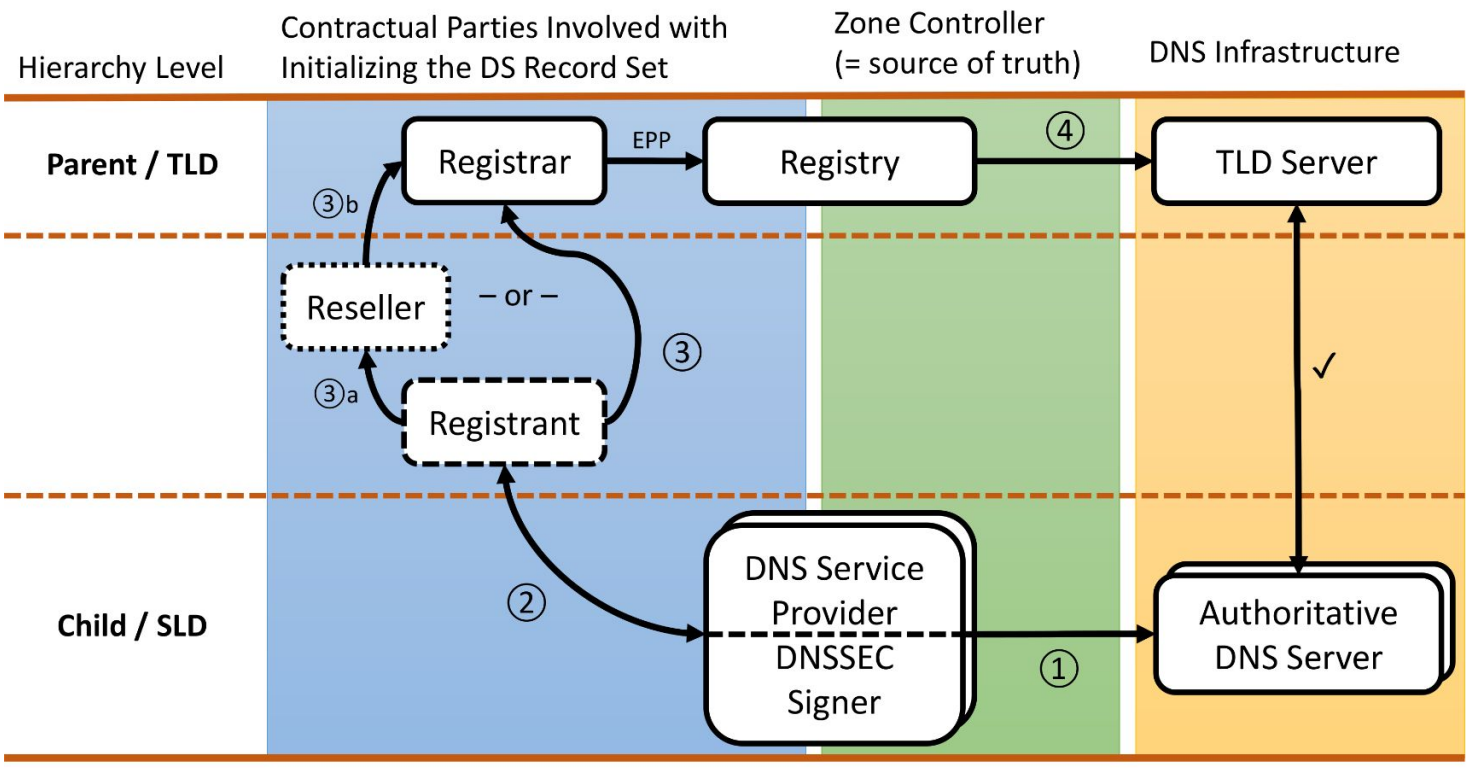
- Error-prone, (too) many parties, slow, out of band, not properly authenticated
  → **needs automation!**

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

  → **needs independent participation of DNS operators**

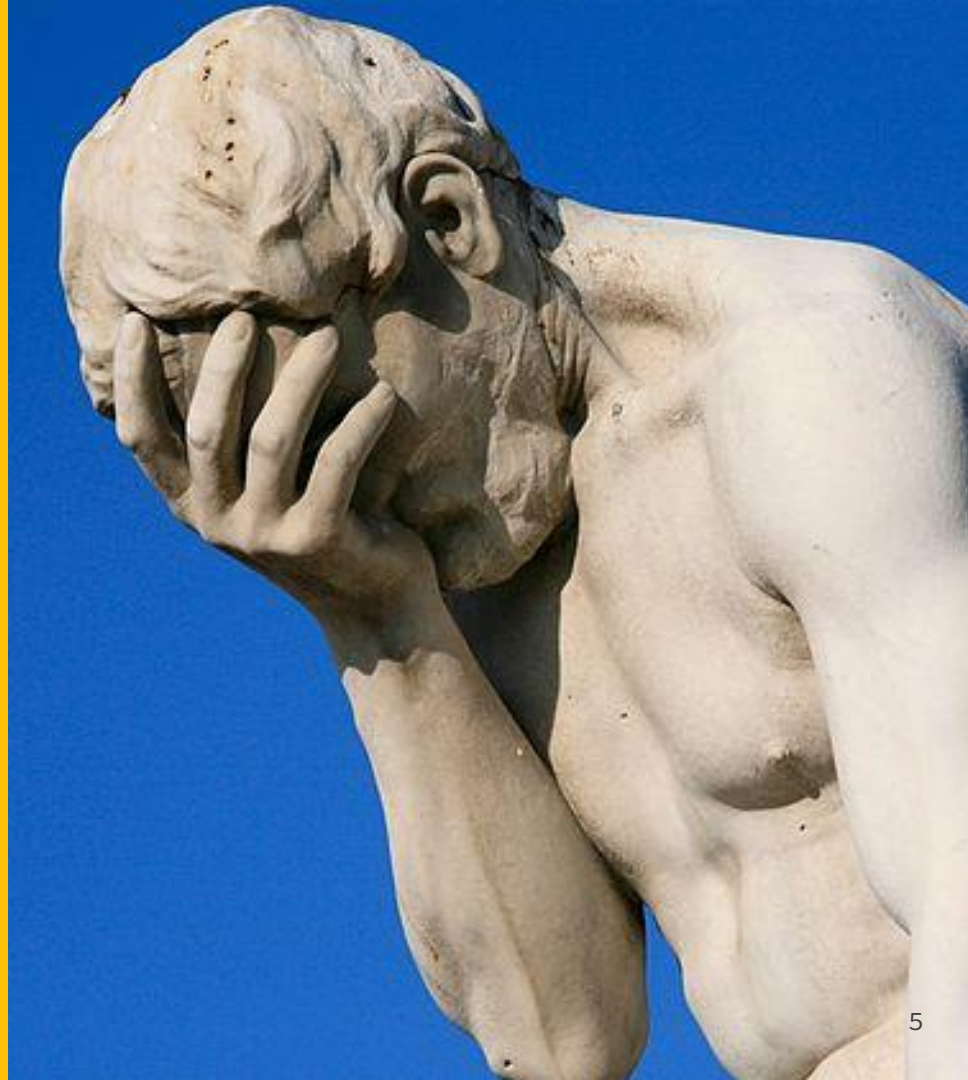
deSEC

Traditional DS Deployment



DNSSEC is too hard

and we know it



Solution: Transfer Trust from DNS Operator

Internet Draft: draft-ietf-dnsop-dnssec-bootstrapping

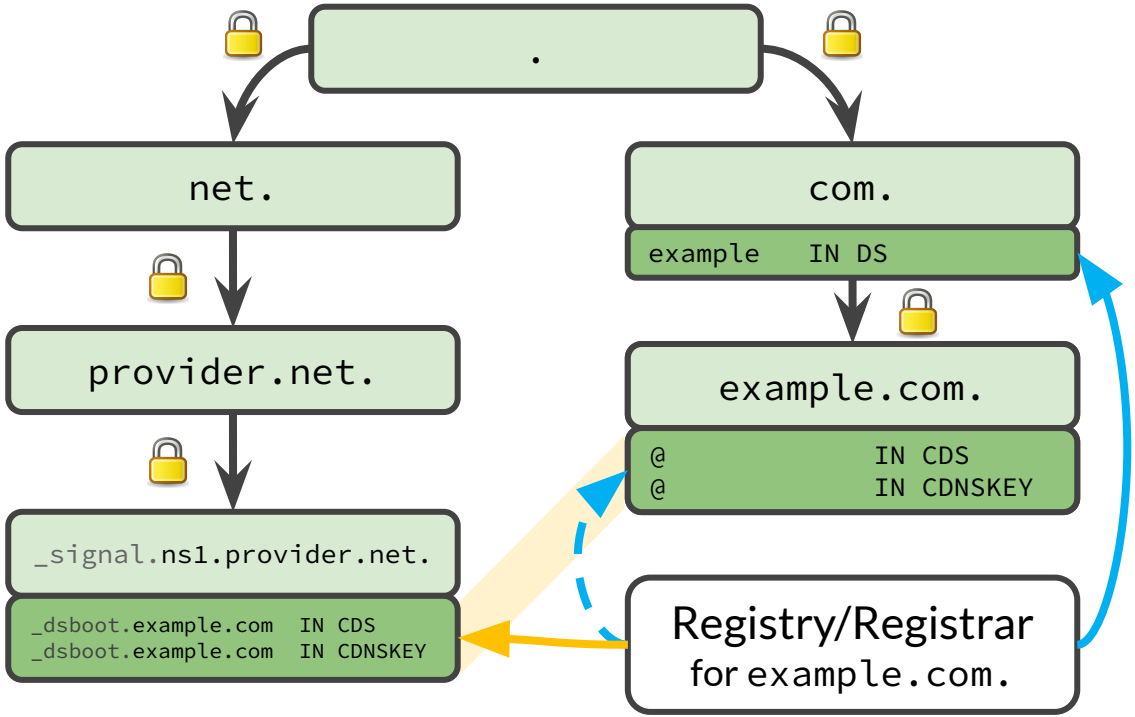
How does it work?

1. Define a **signaling mechanism for DNS operators**
   - allow **publishing arbitrary information** about the zones under management, **on a per-zone basis**
   - do so using namespace **under each nameserver hostname** with **zone-specific subdomains**
   - **require DNSSEC for authentication** (requires nameserver domains to be secure)

2. Ask DNS Operators to **publish authentication signal** for CDS/CDNSKEY
   - start with conventional **CDS/CDNSKEY records** at the apex of the target zone (RFC 8078)
   - **co-publish** these records **via signaling mechanism** (signed with NS zone's keys)

3. **Validate** target domain's CDS/CDNSKEY records **against this signal**
   - if successful: **"transfer trust to the target domain"**
     → **provision DS records** at parent

CDS/CDNSKEY Authentication via Nameserver Signaling



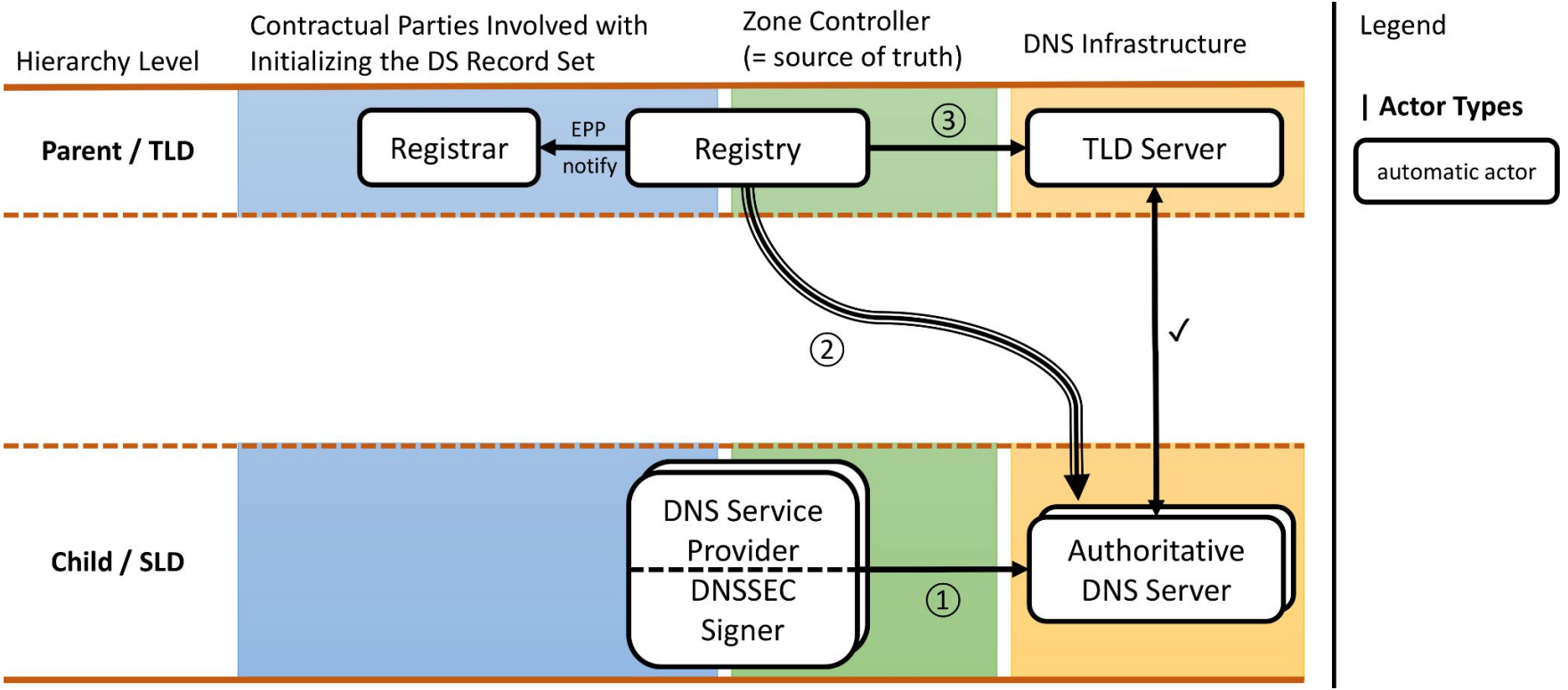
💡 Use an **established chain of trust** (left) to take a detour

- identically co-published
- authenticated, immediate
- no active on-wire attacker

Extends RFC 8078 to add authentication for initial DS

deSEC

CDS/CDNSKEY-based Deployment



It's already in Production

– – –

Child:

- **2 DNS operators**, for all DNSSEC-enabled domains
  - deSEC
  - Cloudflare (manages **23% of Top 1M domains**)

Parent:

- **2 ccTLDs:** .ch/.li
  - .cl close to roll-out
- Insecure bootstrapping supported by 5 ccTLDs (.cr, .cz, .nu, .se, .sk)
- GoDaddy to introduce automatic **DNSSEC bootstrapping as a Registrar**

Sources: Cloudflare coverage measurement: Nils Wisol via Tranco (06/2022); https://github.com/oskar456/cds-updates

You are invited!

– – –

- DNSSEC bootstrapping specification on the way to IETF DNSOP Last Call
  - https://datatracker.ietf.org/doc/draft-ietf-dnsop-dnssec-bootstrapping/
- Client-side **implementations deployed for significant number of registrations**
- **Now:** need parent-side implementations
  - **add authentication to existing** CDS/CDNSKEY scanning implementations (~5 ccTLDs)
  - **start scanning** for CDS/CDNSKEY **under more TLDs**
    - ➢ code examples available, please approach me: peter@desec.io
  - Registrars / ccTLD registries → **Implementations!** 🤩
- **Let's make DNSSEC easy.**

Thank you!

… also to our sponsor:

Questions?

Backup

Protocol Details

Algorithm

- **Co-publish CDS/CDNSKEY records** under a subdomain of the NS hostnames:
  → `CDS/CDNSKEY IN _dsboot.example.com._signal.ns1.provider.net`
- Use **DNSSEC to validate** these records, under **each NS hostname**

Technical Considerations

- Naming scheme with `_signal` label allows delegating to separate zone
  - removes risk of accidentally modifying the nameserver's A/AAAA records
  - reduces churn on nameserver zone
  - allows splitting off DNS operations (e.g. online-signing with different key; delegate by parent)
- prefix allows different types of signals (e.g. for multi-signer p2p key exchange)

Security Model

- We use an established chain of trust to take a detour
  - authenticated, immediate
  - no active on-wire attacker
- Actors in the chain of trust can undermine the protocol
  - can also undermine CDS / CDNSKEY from insecure
- Mitigations exist, e.g:
  - monitor delegation
  - diversify NS TLDs
  - multiple vantage points

deSEC

	Bootstrapping Method		
	Manual	CDS/CDNSKEY	Proposed
Bootstrapping Involves			
zone operator Z	✓[1]	✓	✓
domain owner	✓	✗	✗
registrar	✓	✗	✗
registry	✓	✓	✓
Actors who can initialize keys			
Required parties (trusted)			
registrar	✓	✓[2]	✓[2]
NS zone operator	✗	(✓)	(✓)[3]
NS zone ancestors	✗	(✓)	(✓)
NS zone owner	✗	(✓)	(✓)
Others parties (untrusted)			
active on-wire attacker	depends	✓[4]	✗
social engineering attacker [1]	✓	✗	✗
Properties			
Prerequisites	out-of-band channel	MITM attack mitigation	suitable NS zone configuration
Authentication	bad in practice [1]	none	cryptographically
Duration	varies	days	minutes

Table 1: Comparison of methods for establishing a new secure delegation, dispaying a) entities involved in the bootstrapping of an individual insecure zone, b) attack surface towards trusted and untrusted third parties, and c) prerequisites, key material authentication, and bootstrapping duration. Key initialization within parentheses (✓) requires collusion across all NS zones. [1] For offline signing, only the signing key holder is involved. [2] Registry could refuse deployment through registrar. [3] Requires knowledge of private key. [4] Several vantage points and long time must be covered.