Automatic DNSSEC Bootstrapping with Authentication

CENTR Jamboree 2023
June 1, 2023

Peter Thomassen <peter@desec.io>

draft-ietf-dnsop-dnssec-bootstrapping

DNSSEC validation rate

31%

vs.

secure delegation rate

7%

- Germany 70%
- Scandinavia 90%
- Russia 63%
- Saudi Arabia 99%

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

< 50%

Global averages; 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

Problem Statement

Securing a delegation = Ry creates DS record with child's DNSSEC parameters.

Problems:

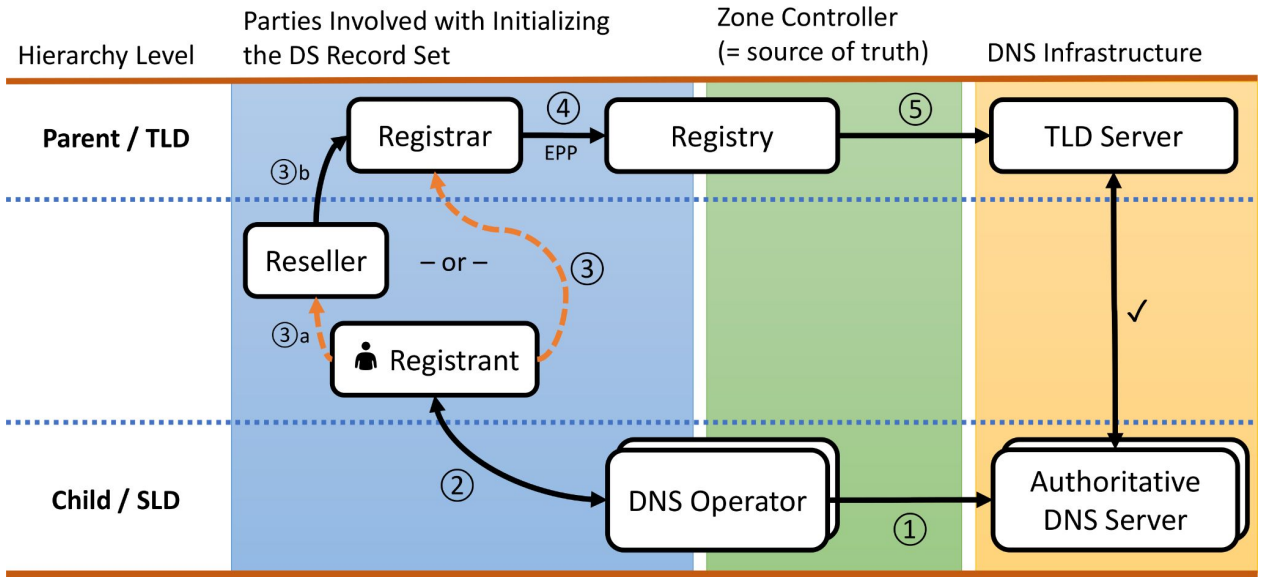
1. **How does the Registry get these parameters?**
   - Largely the same problem as "DS Automation" for rollovers
2. **How are those parameters authenticated?**
   - NB: for key *rollovers*, existing chain of trust can be used. Not here!
3. **What else is there to consider?**

Approaches to DNSSEC Bootstrapping

1. **manual submission**
    - Generally supported, but cumbersome

deSEC

Approaches: Manual Submission



- 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

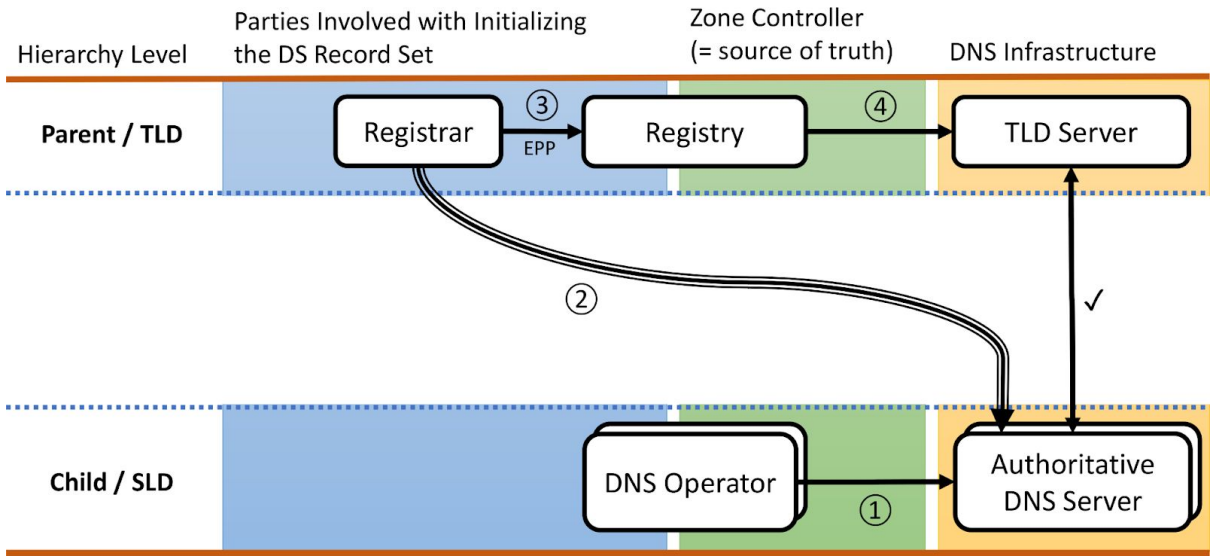
deSEC

Approaches to DNSSEC Bootstrapping

1. **manual submission**
   - Generally supported, but cumbersome
2. **trust on first use** (TOFU): query DNSKEY, compute DS, and hope for the best
   - Used by notable Registrar in Germany

Approaches: Trust on First Use (various interfaces)

- No manual dealing with cryptographic parameters
- Known timing
- No authentication!



Approaches to DNSSEC Bootstrapping

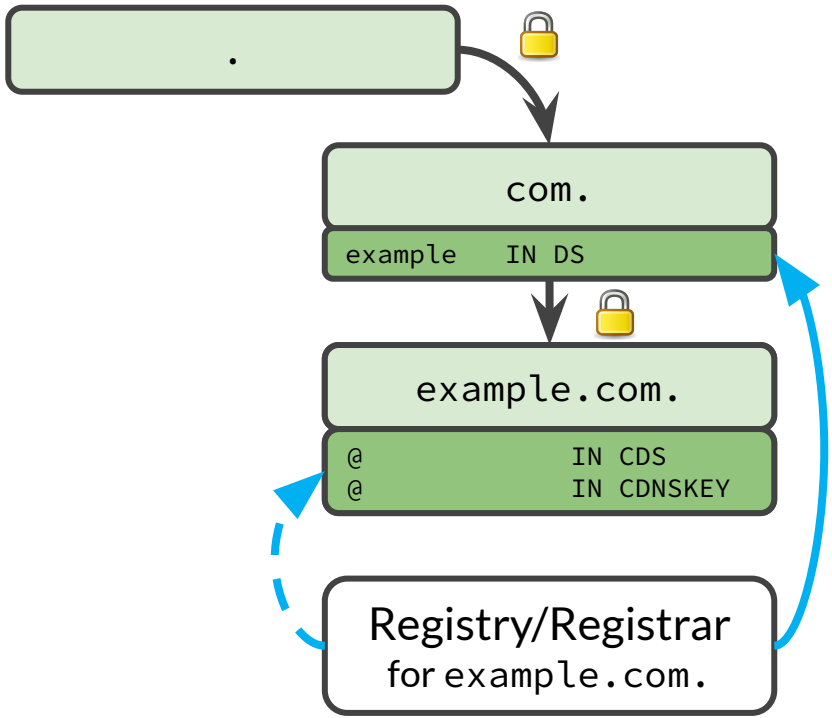
1. **manual submission**
   - Generally supported, but cumbersome
2. **trust on first use** (TOFU): query DNSKEY, compute DS, and hope for the best
   - Used by notable Registrar in Germany
3. Several attempts on **REST interfaces** or REST-DNS hybrids, driven by CIRA
   - ICANN 53, 54 (2015), draft-ietf-regext-dnsoperator-to-rrr-protocol (2018)
   - No known deployments

> *"Need to redesign around the DNS Operator"*
>
> — Jacques Latour, Tech Day at ICANN 53

Approaches to DNSSEC Bootstrapping

1. **manual submission**
   - Generally supported, but cumbersome
2. **trust on first use** (TOFU): query DNSKEY, compute DS, and hope for the best
   - Used by notable Registrar in Germany
3. Several attempts on **REST interfaces** or REST-DNS hybrids, driven by CIRA
   - ICANN 53, 54 (2015), draft-ietf-regext-dnsoperator-to-rrr-protocol (2018)
   - No known deployments
4. CDS/CDNSKEY from **insecure child** (RFC 8078)
   - Requires stateful monitoring
   - Used by **.ch/.cr/.cz/.fo/.li/.nu/.se/.sk/.alt.za/.edu.za** (parent) and various DNS operators (child)

Approaches: CDS/CDNSKEY from Insecure Child



Approaches to DNSSEC Bootstrapping

1. **manual submission**
   - Generally supported, but cumbersome
2. **trust on first use** (TOFU): query DNSKEY, compute DS, and hope for the best
   - Used by notable Registrar in Germany
3. Several attempts on **REST interfaces** or REST-DNS hybrids, driven by CIRA
   - ICANN 53, 54 (2015), draft-ietf-regext-dnsoperator-to-rrr-protocol (2018)
   - No known deployments
4. CDS/CDNSKEY from **insecure child** (RFC 8078)
   - Requires stateful monitoring
   - Used by **.ch/.cr/.cz/.fo/.li/.nu/.se/.sk/.alt.za/.edu.za** (parent) and various DNS operators (child)
5. **CDS/CDNSKEY with authentication** by child operator (IETF DNSOP draft)
   - Used by **.ch/.li** (parent) and **Cloudflare/deSEC/Glauca HexDNS** (child)
   - Implementations exist for PowerDNS Auth and Knot DNS (upstream PRs coming up)

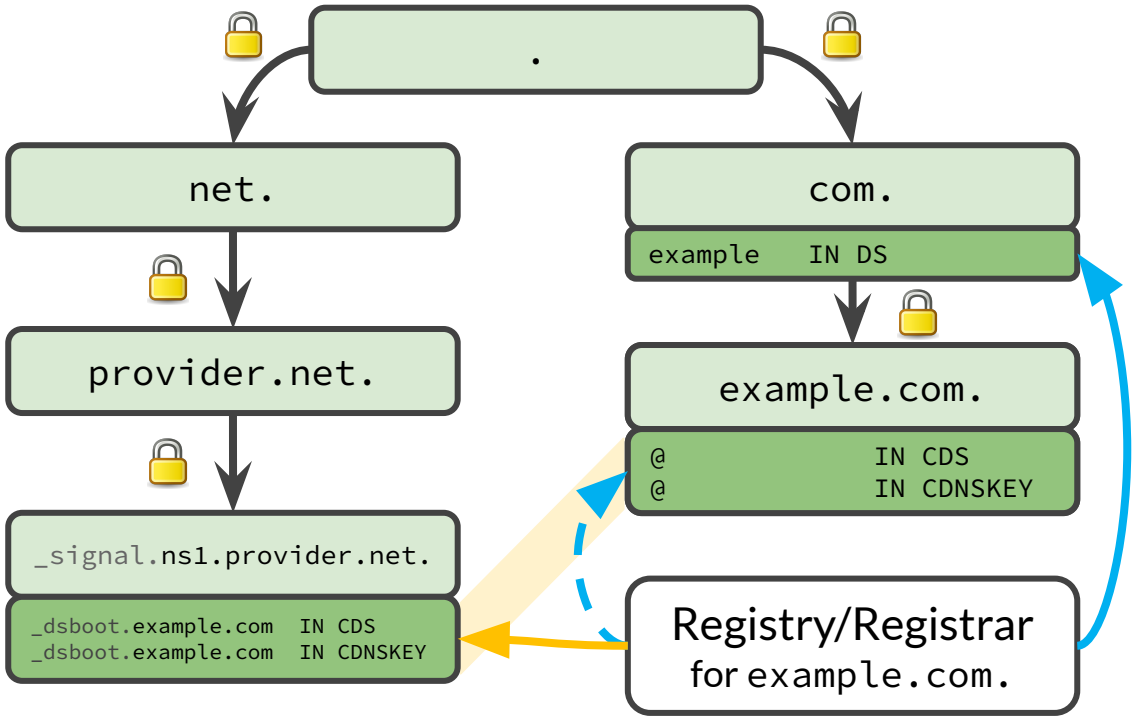
Approaches: CDS/CDNSKEY with Authentication

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

Approaches: CDS/CDNSKEY with Authentication



💡 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

It's already in Production

– – –

Child:

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

Parent:

- **2 ccTLDs:** .ch/.li (+ .cl testing)
- gTLDs in ICANN process to ensure consistent behavior
- 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

CDS & CDNSKEY (and CSYNC): Things to Think about …

– – –

- Who's in charge of scanning? Registry vs. Registrar
  - What if not done?
- CDS/CDNSKEY dichotomy: which to publish in the child?
- Acceptance checks: validation breakage? CDS ~ CDNSKEY?
  - draft-thomassen-dnsop-cds-consistency
- Registry lock: suspend scanning during EPP locks?
- Error reporting: to whom? How? How frequently?
- Competing submissions: e.g. by the registrar or via GUI
- Efficiency improvements: notification trigger instead of scanning
  - draft-thomassen-dnsop-generalized-dns-notify
- …

You are invited!

– – –

- draft-ietf-dnsop-dnssec-bootstrapping on the way to IETF DNSOP Last Call
  - Vocal support on the mailing list always helps (dnsop@ietf.org)
- Child-side **implementations**
  - **deployed** at DNS operators
  - being developed for open source auth nameservers (close to done for **PowerDNS & Knot DNS**)
- **Now:** need parent-side implementations 🤩
  - **add authentication to existing** CDS/CDNSKEY scanning implementations (~6 ccTLDs)
  - **others: start scanning** for CDS/CDNSKEY **under more TLDs**
- **Let's make DNSSEC easy.**

Thank you!

… also to our supporters:

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)

Who's in Charge of Polling?

	Registar	Registry
DS Flow	DNS Operator → Registrar → Registry (no EPP backchannel needed)	DNS Operator → Registry → Registrar (requires EPP backchannel, RFC 9167)
Deployment (today)	- 1 (Domainnameshop) - 1 planned (GoDaddy, since 2020)	- 10 (9 ccTLDs + RIPE) - Several gTLDs ready (CentralNIC, CORE)
Scope	- Covers gTLD and ccTLD names	- Covers only gTLD names
Pros	- Preserves customary flow	- Adoption appears easier in Ry space - Fewer steps to DS (EPP notify is async)
Cons	- TLD query and/or EPP rate limit - Adoption difficult, many Registrars - Some even lack DS interface today - Some charge for setting DS - NOTIFY target discovery unclear	- No ccTLD coverage in Ry agreements, potentially limiting recommendation scope

Locks

	impact on ...				
Lock	**Update**	**Delete**	**Transfer**	**Renew**	**DS automation**
Registry					
Transfer Lock			prohibited		allowed
serverUpdateProhibited	prohibited				allowed
serverDeleteProhibited		prohibited			allowed
serverTransferProhibited			prohibited		allowed
serverRenewProhibited				prohibited	allowed
URS Lock	prohibited	prohibited	prohibited		?
ccTLD-specific Lock	prohibited	prohibited	prohibited		out of scope
Registrar					
clientUpdateProhibited	prohibited				allowed
clientDeleteProhibited		prohibited			allowed
clientTransferProhibited			prohibited		allowed
clientRenewProhibited				prohibited	allowed

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.