Status Update
on Authenticated Bootstrapping of DNSSEC Delegations

OARC 36
November 30, 2021

draft-thomassen-dnsop-dnssec-bootstrapping

Peter Thomassen (deSEC, Secure Systems Engineering)
Nils Wisiol (deSEC, Technische Universität Berlin)

Overview

- Enabling DNSSEC requires **conveying DS information** to the parent
- The draft provides **in-band authentication for bootstrapping**
- Based on **CDS/CDNSKEY at the child apex** (RFC 8078)
- Verification happens through a **chain of trust to the DNS operator**
  - Chain of trust established via DNSSEC on **operator's nameserver domains**
- IETF DNSOP WG has expressed interest in adopting

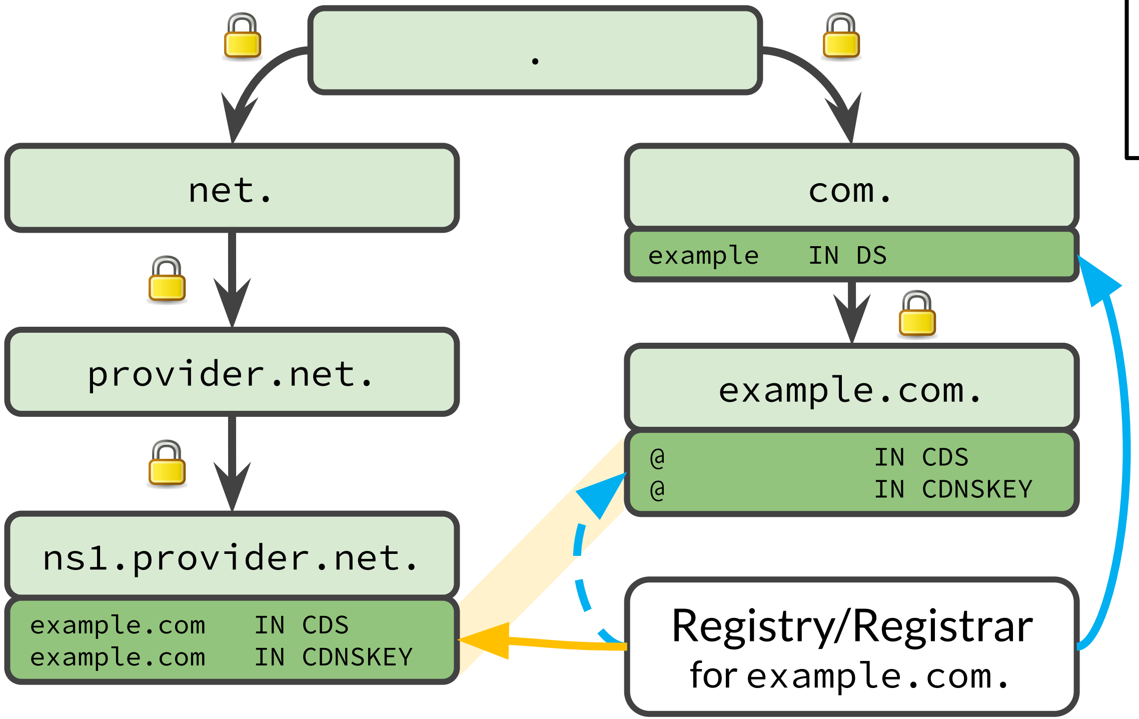
How does it work?

1. Create a **signaling mechanism for DNS operators**
   - **What?**
     - allow **publishing arbitrary information** about the zones they are authoritative for
     - in an **authenticated** fashion, **on a per-zone basis**
   - **How?**
     - use namespace **under each nameserver hostname**, e.g. `_dsauth.ns1.desec.io`
     - **require DNSSEC** under this namespace (requires nameserver domains to be secure)
     - under this namespace, **announcements** are made **using zone-specific owner names**

2. Use this mechanism to **publish an authentication signal**
   - start with **CDS/CDNSKEY records at the apex** of the target zone (RFC 8078)
   - **co-publish these records using the signaling mechanism** (signed with NS zone's keys)

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

CDS Authentication: Co-Publish under Trusted Hostname



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

- authenticated, immediate
- no active on-wire attacker

Technical Considerations

- No collision with original use of CDS/CDNSKEY (those are apex-only)
- Add extra label: `example.com.`**`_dsauth`**`.ns1.provider.net`
  - to enable delegation of signaling data to separate zone
- Name scheme features:
  - 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)
  - allows parent to discover bootstrappable domains under `parent._dsauth` (XFR, NSEC walk)
- Requires use of DNSSEC at nameserver domains (`ns1.provider.net`)

Bootstrappability in Tranco Top 1M

```
Measurement failure rate..............................:   2.30%
Remaining sample size.................................:  977007

Proportion of secure zones............................:   5.43%
Proportion of signed zones............................:   6.84%

Proportion of zones with all nameserver targets secure:  24.63%
Proportion of zones with ≥ 1 nameserver targets secure:  25.97%
```

bootstrappable:
domain is not secure *and* NS targets have validation path → signaling possible

```
Proportion of bootstrappable zones (all NS) ..........:  22.11%
Proportion of bootstrappable zones (≥ 1 NS) ..........:  23.07%
```

as of 22 October 2021

Limitations

Some edge cases cannot be accommodated by design:

- doesn't work with certain special setups
  - semantic collision when there is a delegation at an intermediate name: foo.bar.net._dsauth.[...]
- doesn't work when target domain name is too long or has too many labels
  - Constrained by the fact that the _dsauth.[...] suffix needs to be added
- doesn't work in bailiwick (< 0.33% for .com, < 0.72% for .net)

Status & Outlook

- Presented at IETF 112 → valuable feedback
  - Simplify protocol (remove hashing from signaling names)
  - Settle on a better intermediate label than `_boot` (chose `_dsauth` for now)
  - Clarify importance of cleaning up bootstrapping records
  - Point out in-bailiwick limitations etc.

  → New draft version: -03
- Awaiting adoption call by IETF DNSOP WG
- **Looking for DNS operators and registries/registrars** who are interested in deploying the protocol (as an experiment?)

Thank you!

… also to our sponsors:

SSE

PCH
Packet Clearing House

Questions?

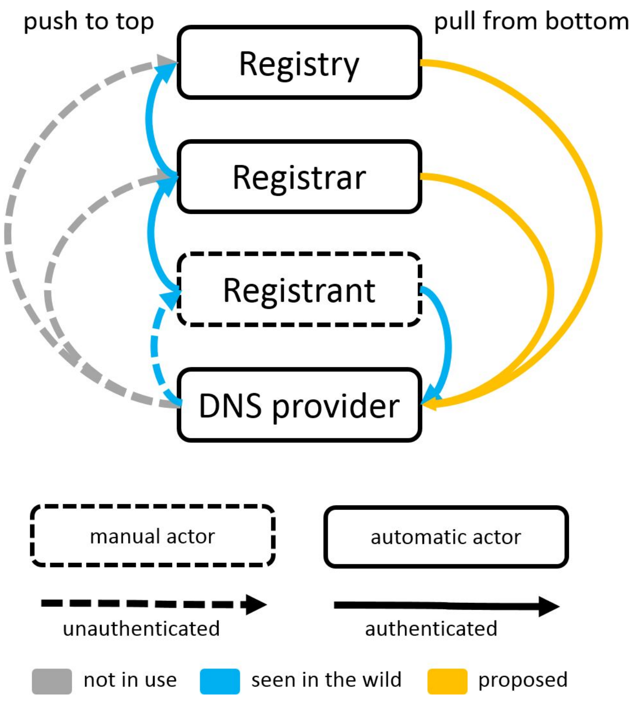
Backup

Approaches to DS Bootstrapping

- Various methods have emerged
  - TOFU, manual submission, REST interfaces*, CDS/CDNSKEY from insecure (RFC 8078)

- Each suffers from one or more downsides
  - unauthenticated || out of band || slow || stateful || error-prone || too many parties || no automation
  - **Authenticated workflow involves too many steps**

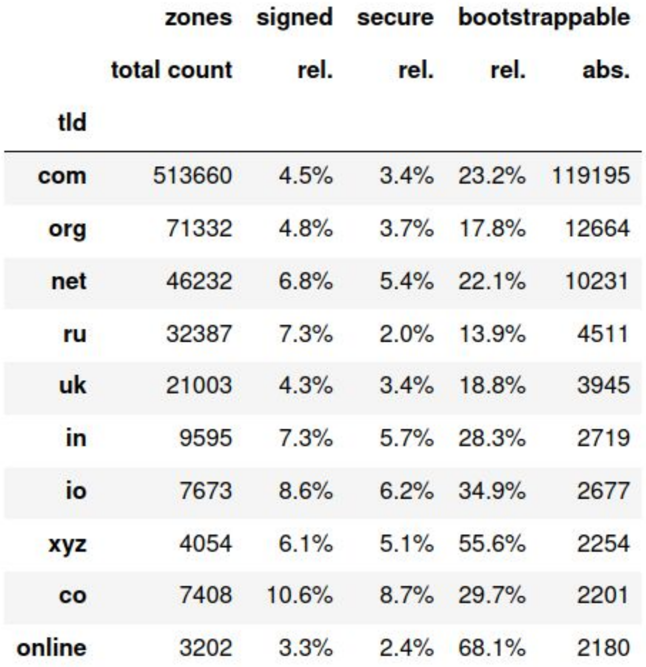
- **Goal: add authentication to direct pull** from DNS operator
  - **automatable, immediate, no state required**



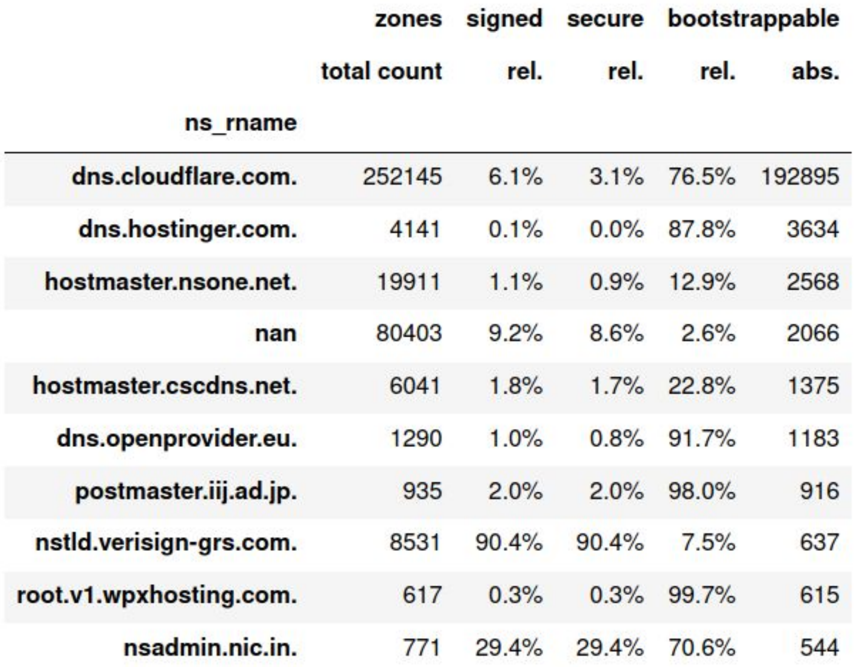
* ICANN 54 (2015), draft-ietf-regext-dnsoperator-to-rrr-protocol (2018)

deSEC

Survey on Deployment Requirements: by TLD, by Provider



	zones	signed	secure	bootstrappable	
	total count	rel.	rel.	rel.	abs.
tld					
com	513660	4.5%	3.4%	23.2%	119195
org	71332	4.8%	3.7%	17.8%	12664
net	46232	6.8%	5.4%	22.1%	10231
ru	32387	7.3%	2.0%	13.9%	4511
uk	21003	4.3%	3.4%	18.8%	3945
in	9595	7.3%	5.7%	28.3%	2719
io	7673	8.6%	6.2%	34.9%	2677
xyz	4054	6.1%	5.1%	55.6%	2254
co	7408	10.6%	8.7%	29.7%	2201
online	3202	3.3%	2.4%	68.1%	2180



	zones	signed	secure	bootstrappable	
	total count	rel.	rel.	rel.	abs.
ns_rname					
dns.cloudflare.com.	252145	6.1%	3.1%	76.5%	192895
dns.hostinger.com.	4141	0.1%	0.0%	87.8%	3634
hostmaster.nsone.net.	19911	1.1%	0.9%	12.9%	2568
nan	80403	9.2%	8.6%	2.6%	2066
hostmaster.cscdns.net.	6041	1.8%	1.7%	22.8%	1375
dns.openprovider.eu.	1290	1.0%	0.8%	91.7%	1183
postmaster.iij.ad.jp.	935	2.0%	2.0%	98.0%	916
nstld.verisign-grs.com.	8531	90.4%	90.4%	7.5%	637
root.v1.wpxhosting.com.	617	0.3%	0.3%	99.7%	615
nsadmin.nic.in.	771	29.4%	29.4%	70.6%	544

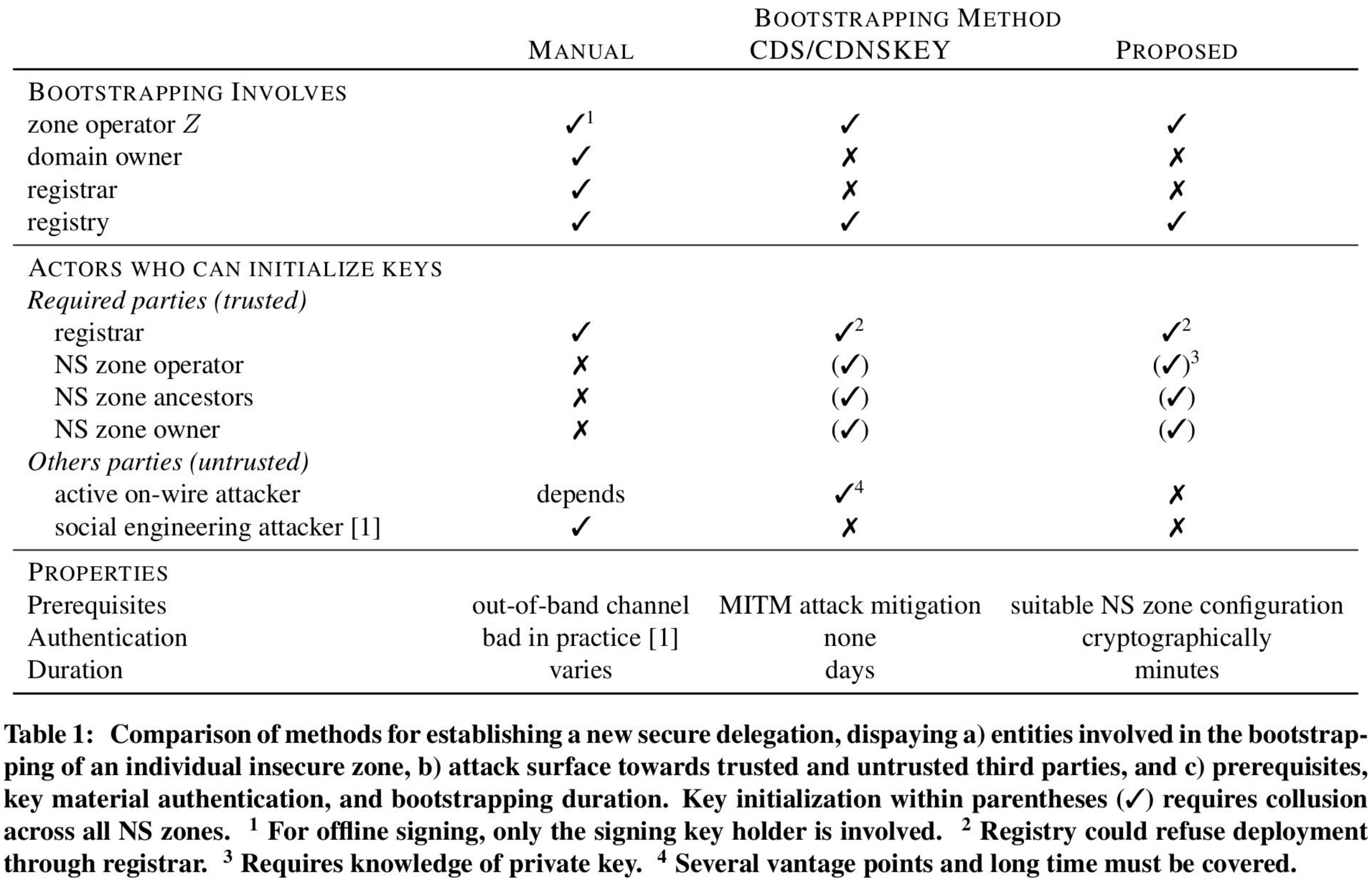
as of 22 October 2021, “nan” ns_rname means that referenced NS zones have more than one rname in their SOAs

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
    - but: known point in time / window of opportunity much smaller

- Further mitigations exist, e.g:
    - monitor delegation
    - diversify NS TLDs
    - multiple vantage points



		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.