Automatic DNSSEC Bootstrapping

using Authenticated Signals from the Zone's Operator

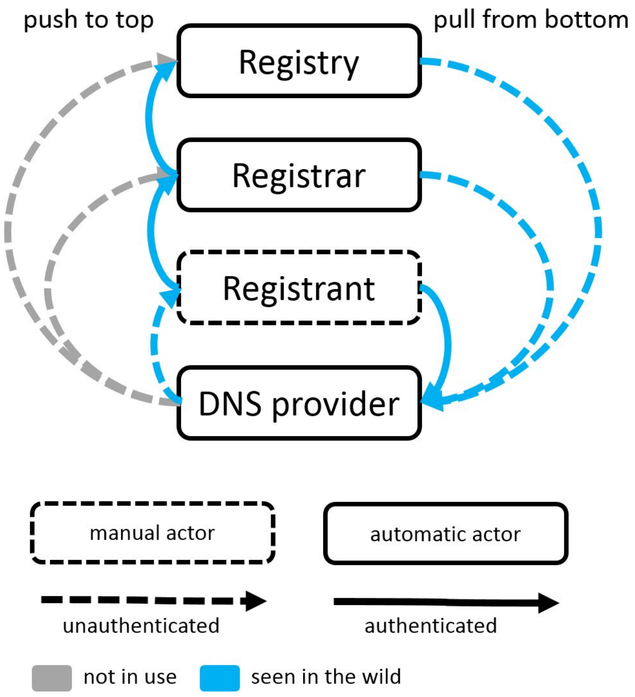
ICANN 74 – DNSSEC Workshop
June 13, 2022

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

draft-ietf-dnsop-dnssec-bootstrapping

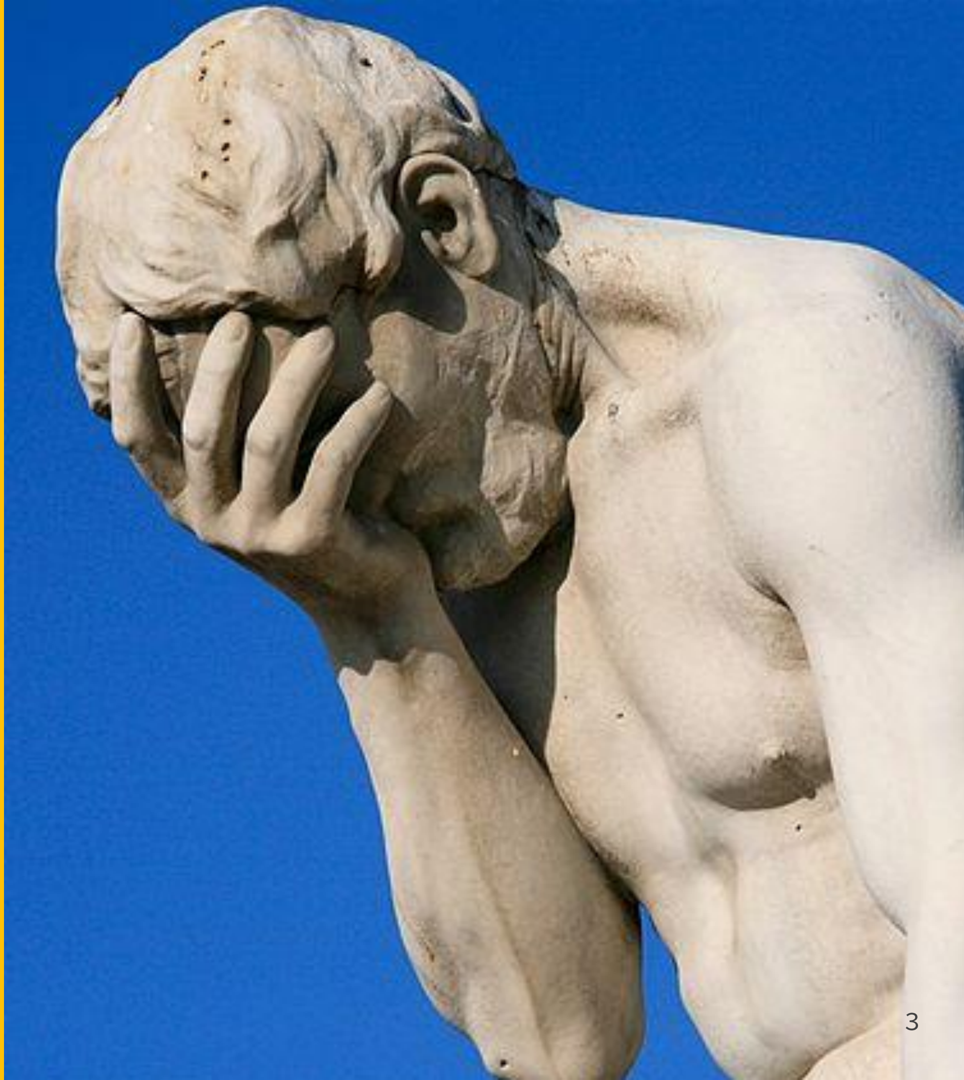
The State of DS Initialization

- **Secure** transfer needs many steps
- RFC 8078 brought parent pulling
  - via CDS/CDNSKEY records
  - **not secure for bootstrapping**



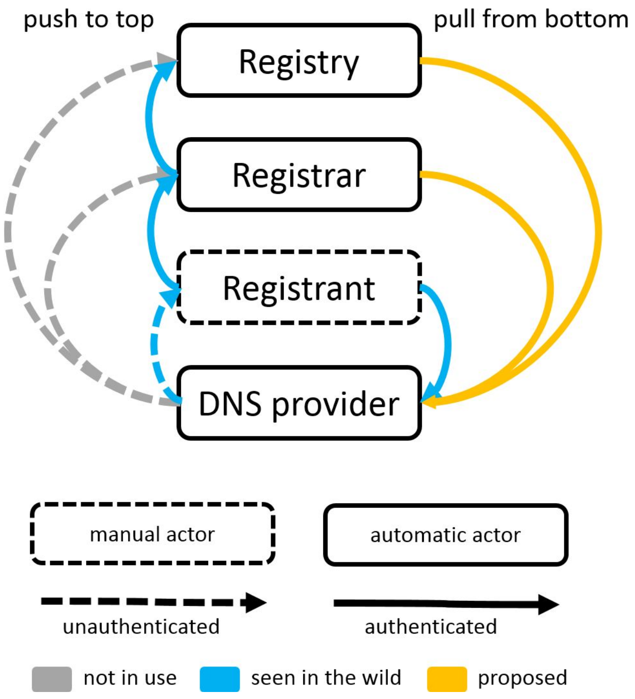
DNSSEC is too hard

and we know it

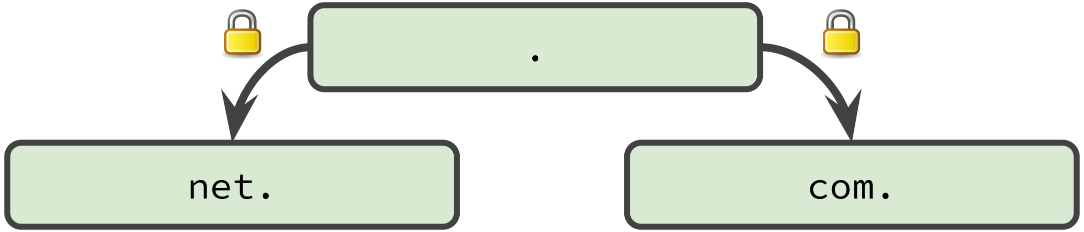


Authenticated Pull from the DNS Provider

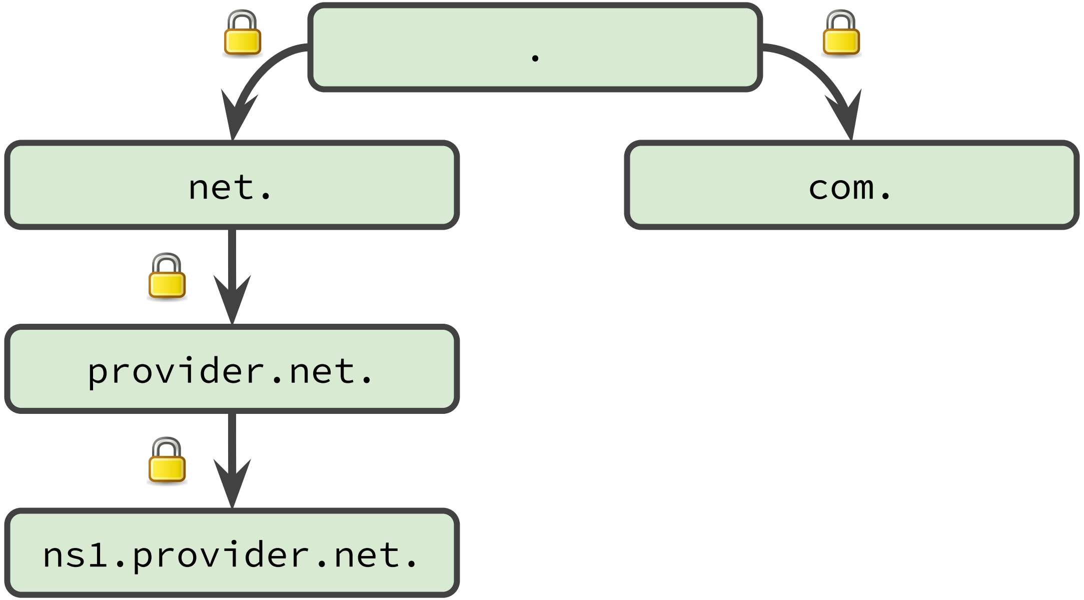
- authenticate CDS/CDNSKEY records
- automated, in-band, immediate, stateless



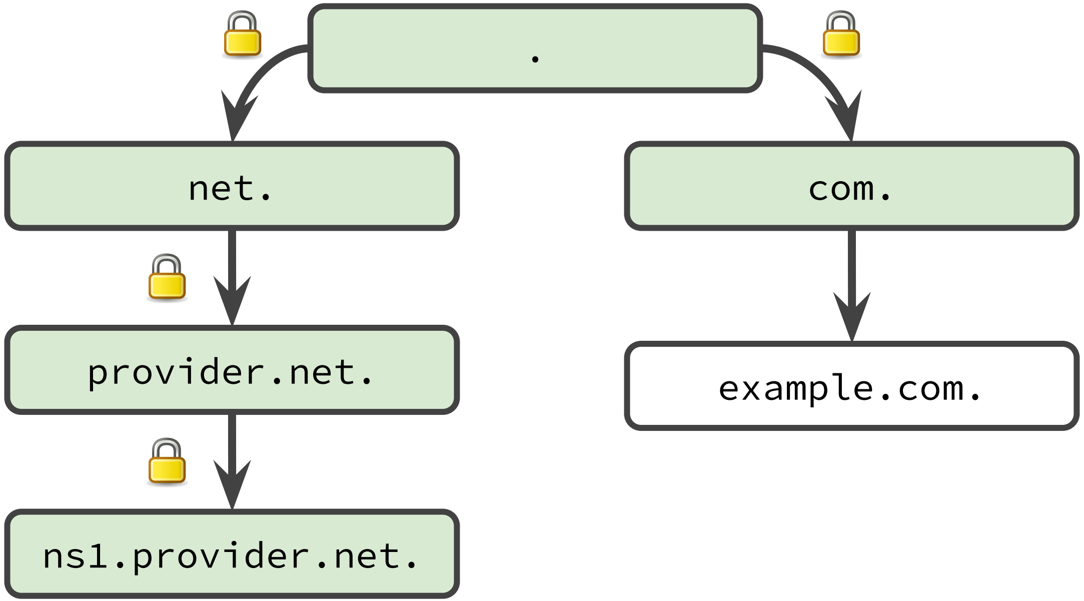
Reminder: CDS Authentication via Trusted Nameserver



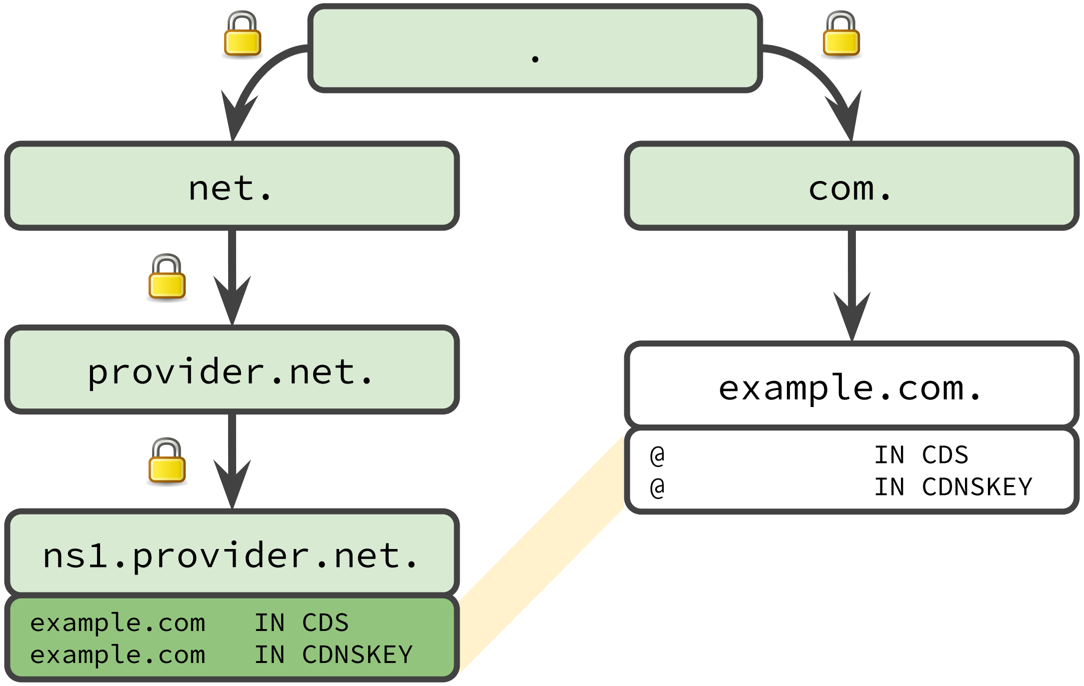
Reminder: CDS Authentication via Trusted Nameserver



Reminder: CDS Authentication via Trusted Nameserver



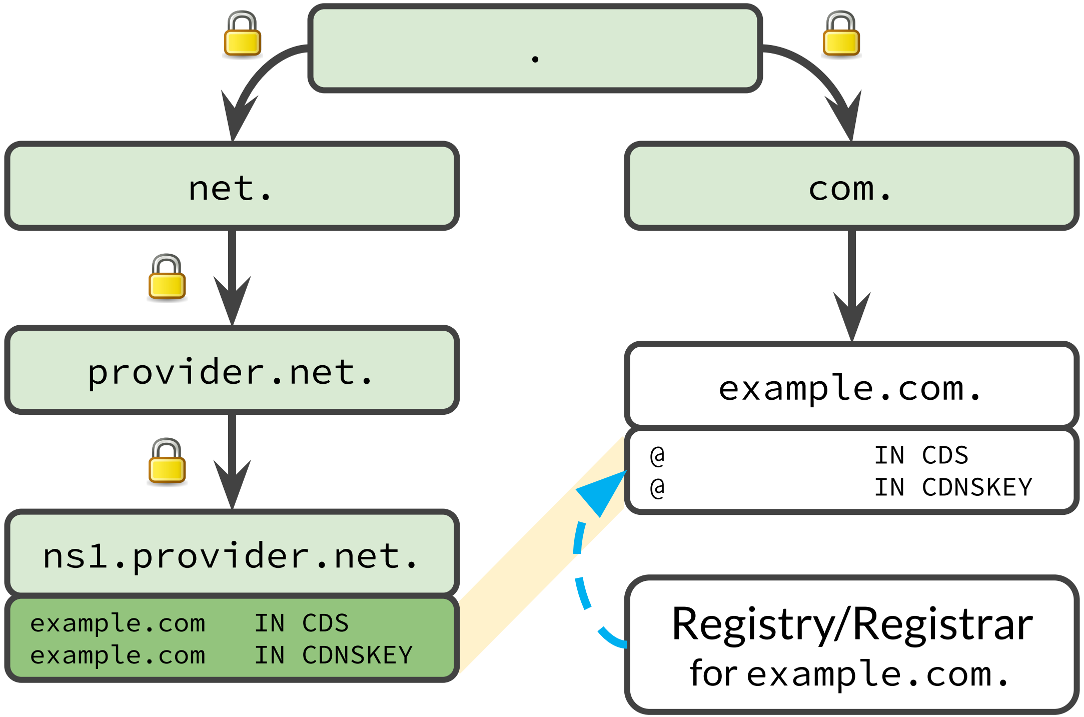
Reminder: CDS Authentication via Trusted Nameserver



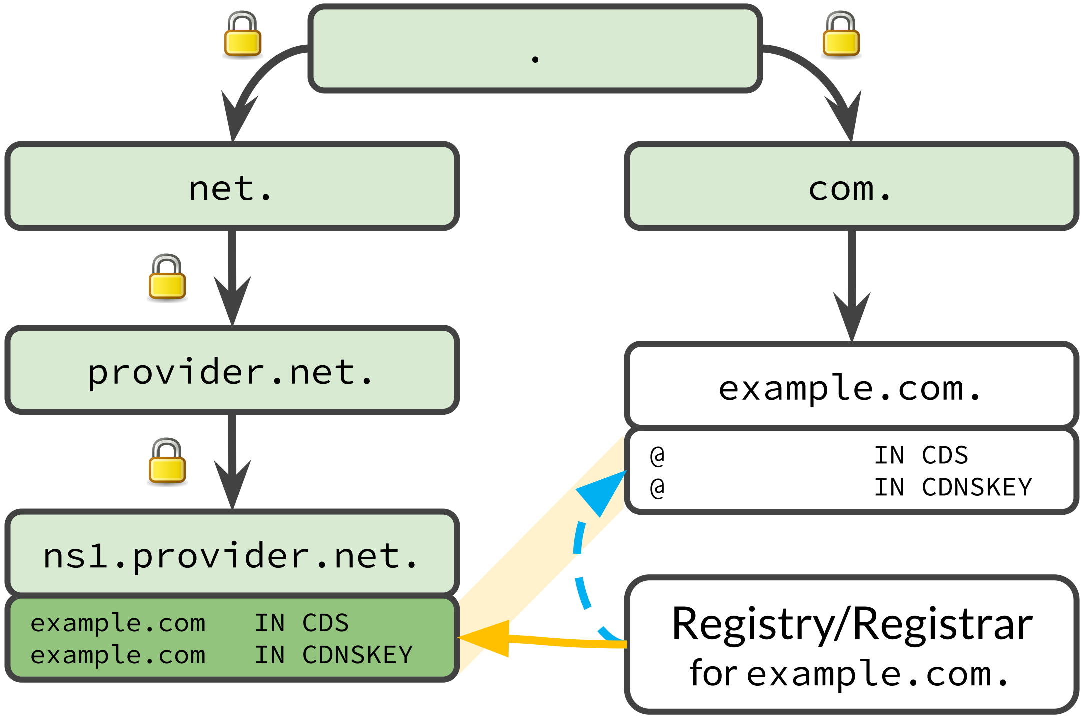
```
example.com    IN CDS
example.com    IN CDNSKEY
```

```
@                  IN CDS
@                  IN CDNSKEY
```

Reminder: CDS Authentication via Trusted Nameserver



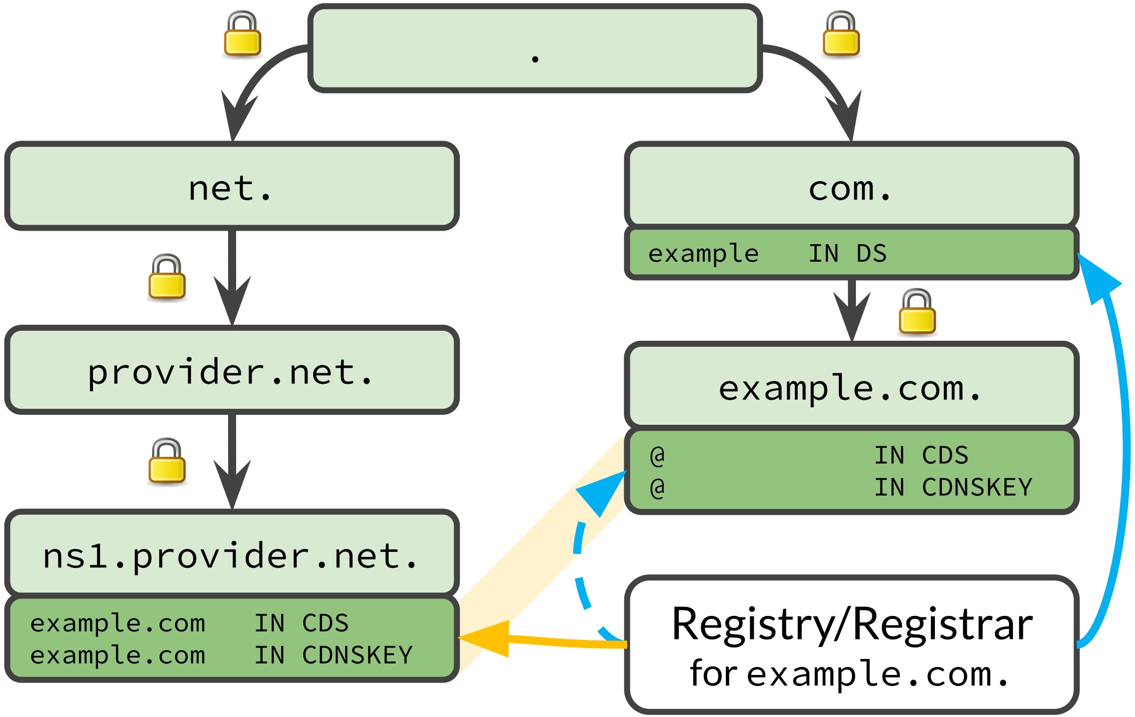
Reminder: CDS Authentication via Trusted Nameserver



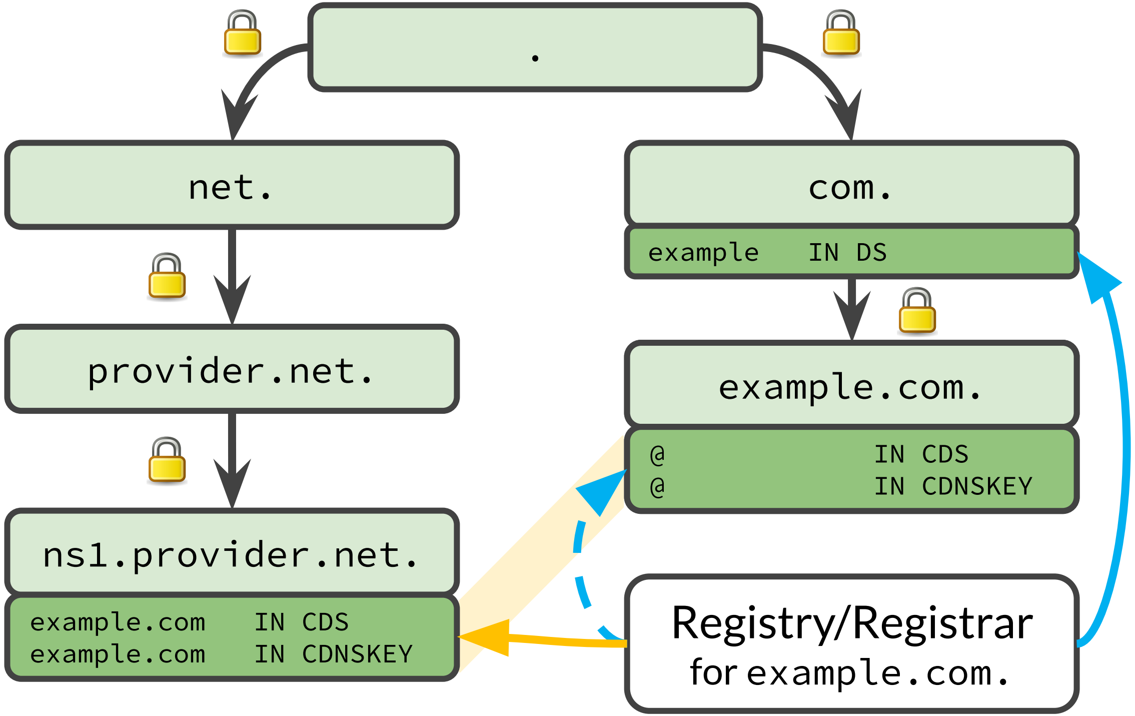
```
example.com   IN CDS
example.com   IN CDNSKEY
```

```
@                   IN CDS
@                   IN CDNSKEY
```

Reminder: CDS Authentication via Trusted Nameserver



Reminder: CDS Authentication via Trusted Nameserver



💡 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

Status

- Adopted by IETF DNSOP WG in April 2022

- Wrote post for APNIC Blog to get the word out
  - https://blog.apnic.net/2022/03/08/authenticated-bootstrapping-of-dnssec-delegations/

- Implementations:
  - Prototype implementation: https://github.com/desec-io/dsbootstrap
  - CoCCA: implementation under way for 59 ccTLDs
  - GoDaddy: implementation planned after CDS scanning
  - .cl: implementation finished, waiting for internal approval
  - implementations by other registries and DNS operators under way

Protocol Changes since Last Presentation @ ICANN 72

Some details have changed since 10/2021. **Current definition:**

- **Co-publish CDS/CDNSKEY records** under a subdomain of the NS hostnames
  - Example: `CDS/CDNSKEY IN _dsboot.example.com._signal.ns1.provider.net`
  - Zone containing the NS hostnames **required to be signed**
    → **enables validation**

How's that different from before?

- A new naming scheme was necessary to solve an edge case ambiguity
  - Previously, target domain was hashed, and there was only one underscore label (in the middle)
- Side effect: Signaling mechanism is now more general
  - Can signal other things under different prefix

Outlook

Document Status

- Authors consider protocol rather mature
- Document polishing needed; then: ask for WG Last Call

What's needed?

- Document review / suggestions for improvement
  - https://datatracker.ietf.org/doc/draft-ietf-dnsop-dnssec-bootstrapping/
- Registrars / ccTLD registries → **Implementations!**
- **Let's make DNSSEC easy.**

Thank you!

… also to our sponsor:

SSE

Questions?

Backup

Survey on Deployment Requirements: General Results

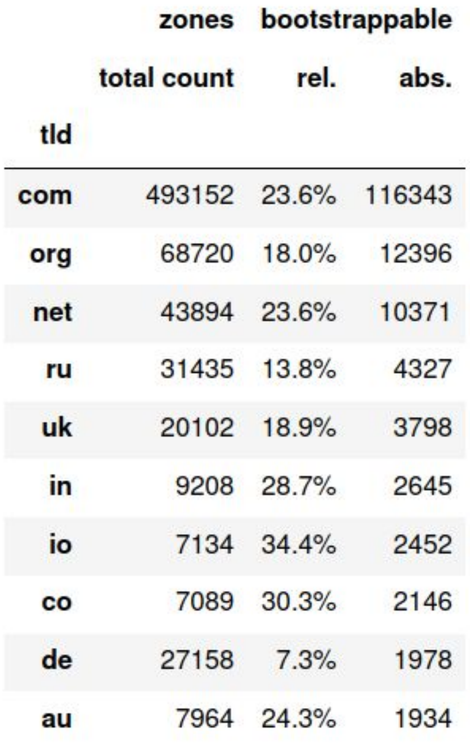
```
Failure rate ..................................:   3.80%
Remaining sample size .........................:  962012

Proportion of secure zones ....................:   4.47%
Proportion of signed zones ....................:   5.87%

Proportion of zones with all nameserver targets secure:  24.14%
Proportion of zones with ≥ 1 nameserver targets secure:  25.36%
```

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

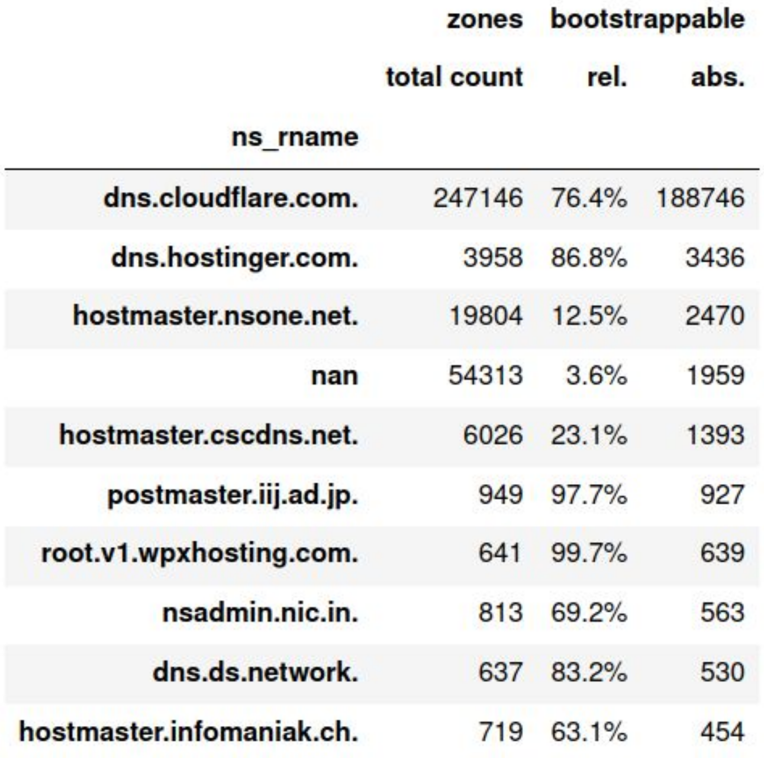
```
Proportion of bootstrappable zones (all NS) ..........:  21.77%
Proportion of bootstrappable zones (≥ 1 NS) ..........:  22.66%
```

as of 09/2021

Survey on Deployment Requirements: by TLD and Provider



	zones	bootstrappable	
	total count	rel.	abs.
tld			
com	493152	23.6%	116343
org	68720	18.0%	12396
net	43894	23.6%	10371
ru	31435	13.8%	4327
uk	20102	18.9%	3798
in	9208	28.7%	2645
io	7134	34.4%	2452
co	7089	30.3%	2146
de	27158	7.3%	1978
au	7964	24.3%	1934



	zones	bootstrappable	
	total count	rel.	abs.
ns_rname			
dns.cloudflare.com.	247146	76.4%	188746
dns.hostinger.com.	3958	86.8%	3436
hostmaster.nsone.net.	19804	12.5%	2470
nan	54313	3.6%	1959
hostmaster.cscdns.net.	6026	23.1%	1393
postmaster.iij.ad.jp.	949	97.7%	927
root.v1.wpxhosting.com.	641	99.7%	639
nsadmin.nic.in.	813	69.2%	563
dns.ds.network.	637	83.2%	530
hostmaster.infomaniak.ch.	719	63.1%	454

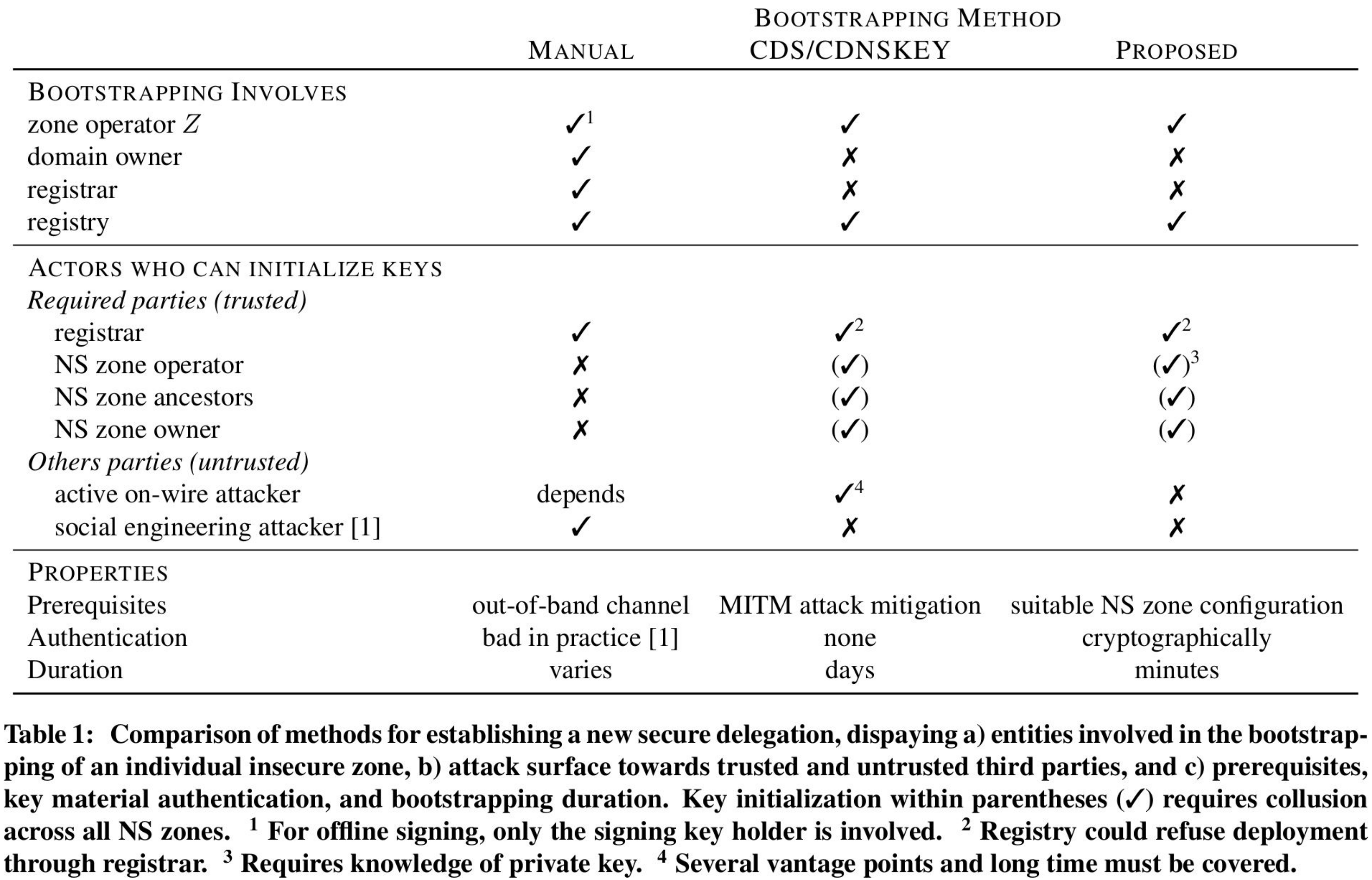
as of 09/2021

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.