

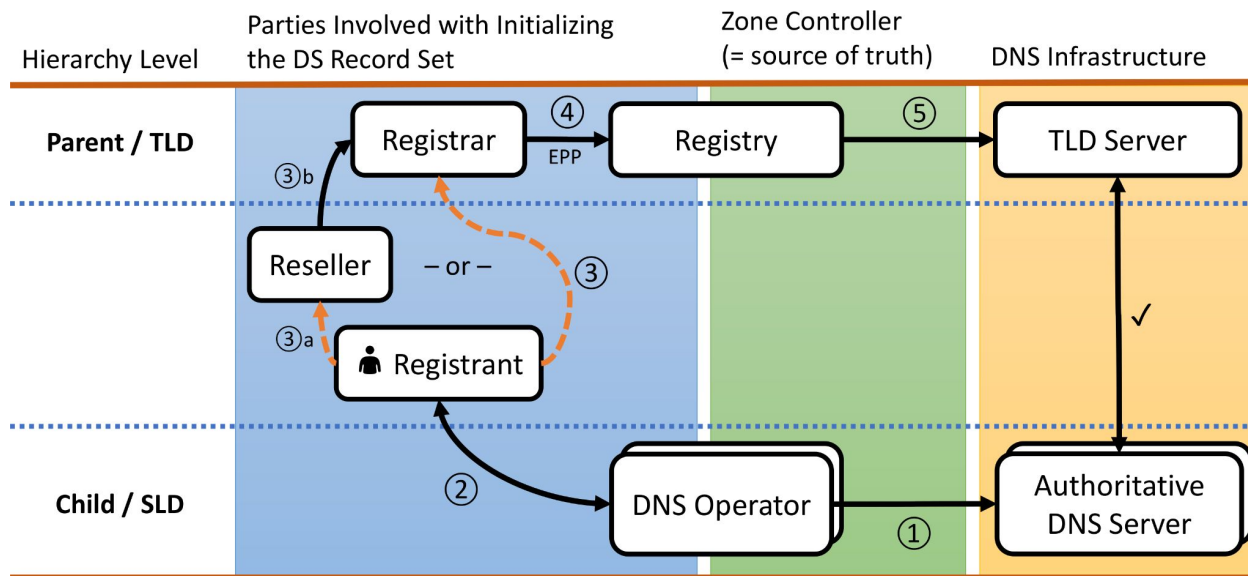
Implementation Status of DNSSEC Bootstrapping

[draft-ietf-dnsop-dnssec-bootstrapping](#)

Peter Thomassen <peter@desec.io>

ICANN79 – DNSSEC and Security Workshop
March 6, 2024

Registrant-centric DS Provisioning

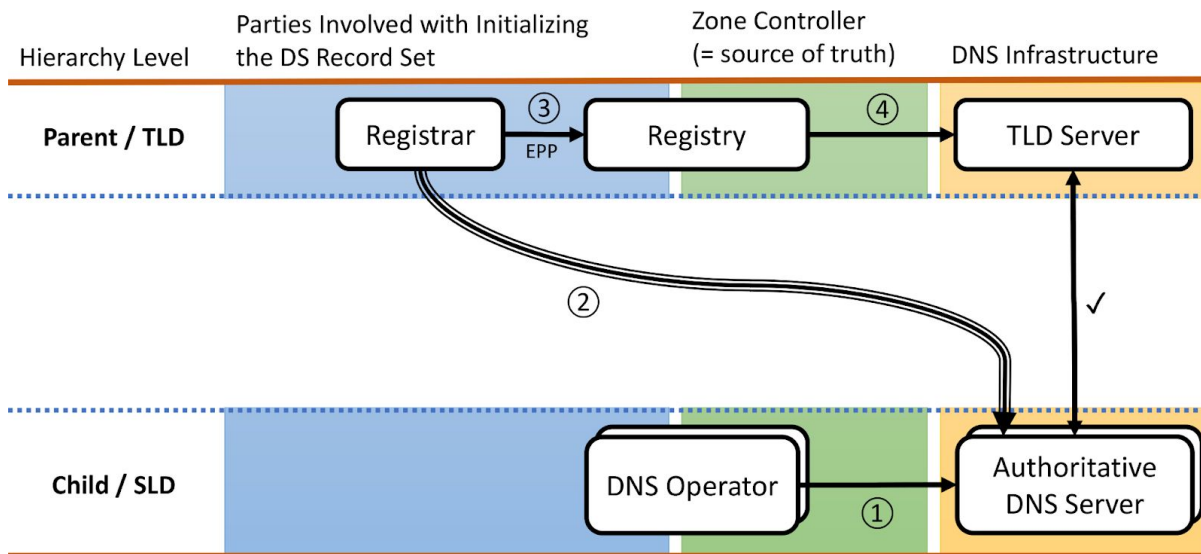


- Slow
- Error-prone
- Out of band
- Not properly authenticated

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

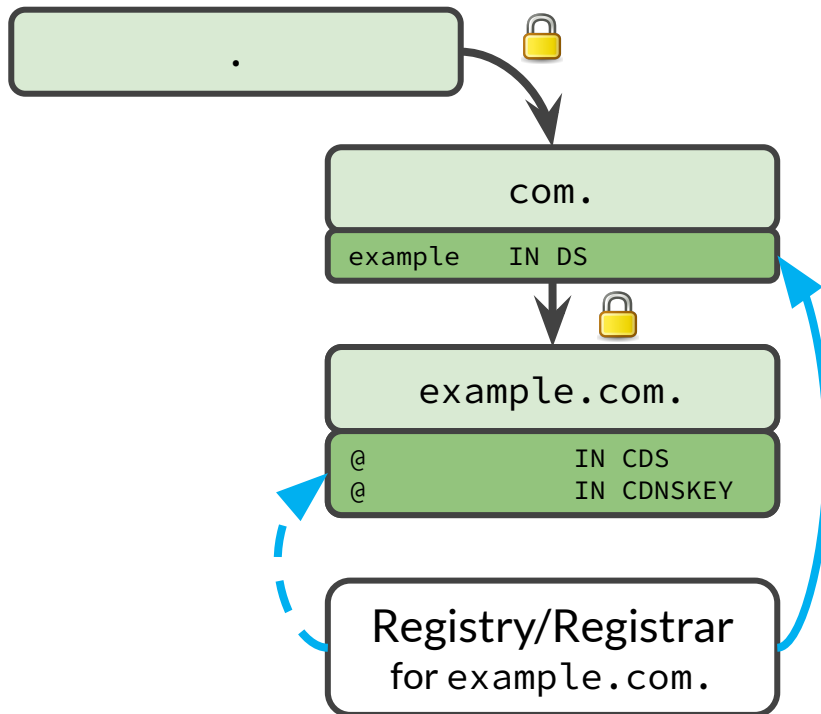
Automatic DS Provisioning

- No manual dealing with cryptographic parameters
- Authentication?



CDS/CDNSKEY Processing from Insecure Child

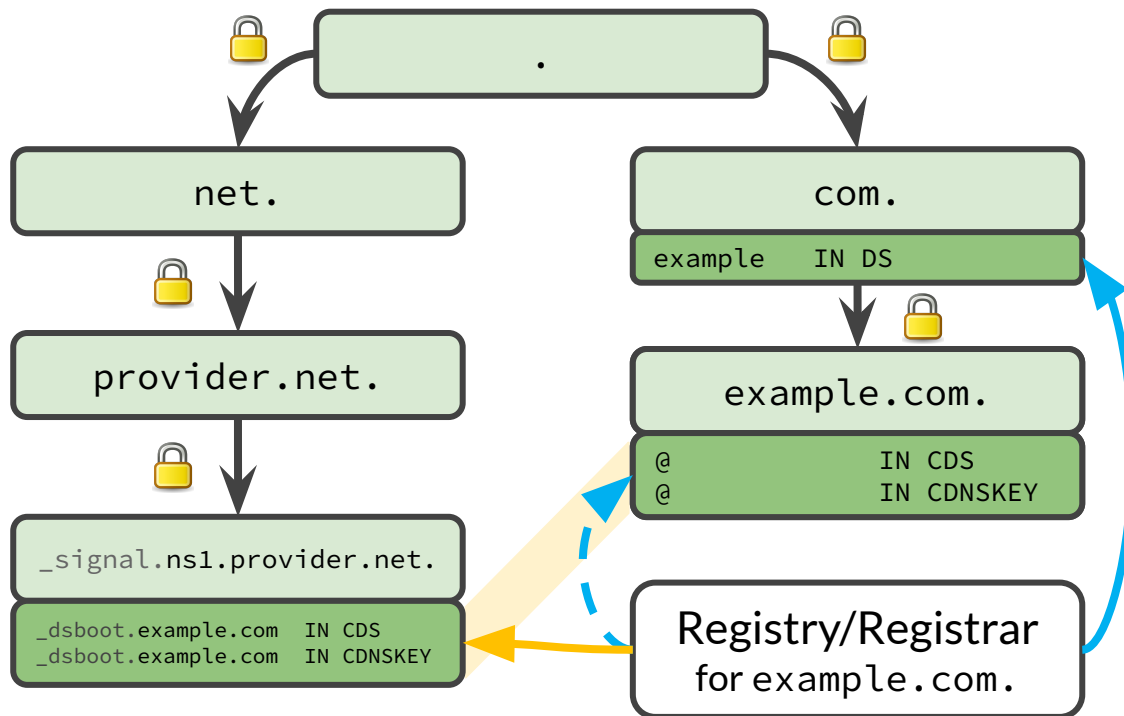
— — —



- Accept after delay (RFC 8078 Section 3.3)
- Trust on first use (“TOFU”)

CDS/CDNSKEY Processing 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

Protocol Status

— — —

- Passed IETF DNSOP WG Last Call in February
- Parent side (processing signaling records):
 - implementations at .ch/.li
 - some gTLDs working towards deployment
- Child side (publishing signaling records)
 - Operators: Cloudflare, Glauca HexDNS, deSEC
 - Authoritative servers: **Knot DNS 3.3.5** (~next week) and **PowerDNS 4.9.0-beta2**

Knot DNS Implementation: authsignal module

zone:

- domain: example.com
 dnssec-signing: on
- domain: ...
- domain: ...

Knot DNS Implementation: authsignal module

mod-onlinesign:

- id: *authsignal*
- nsec-bitmap: [CDS, CDNSKEY]

zone:

- domain: **_signal.ns1.provider.net**
module: [mod-authsignal,
mod-onlinesign/*authsignal*]
- domain: *example.com*
dnssec-signing: on
- domain: ...
- domain: ...

PowerDNS Implementation via LUA Interface

— — —

1. Enable LUA in config: `enable-lua-records=yes`

2. Download synthesis script:

```
curl https://raw.githubusercontent.com/desec-io/desec-ns/f3b561d43213d9e2b5c82dc7c2a8ed1fe7ea198d/ns/lua/signaling.lua \  
> /usr/share/lua/5.1/authsignal.lua
```

3. Hook up to signaling zone:

```
ZONE=_signal.ns1.provider.net # assuming zone already exists  
pdnsutil replace-rrset $ZONE * LUA 1 \  
CDS      ";require('authsignal') return signal('$ZONE', 'CDS')" \  
CDNSKEY  ";require('authsignal') return signal('$ZONE', 'CDNSKEY')"
```

Thank you!

... also to our sponsors:



Questions?