

IETF Hackathon

IETF 114

23-24 July 2022

Philadelphia, Pennsylvania

Hackathon Plan

- Draft: [draft-ietf-dnsop-dnssec-bootstrapping](#)
- Requires co-publishing the target zone's CDS/CDNSKEY records at a subdomain of the nameserver's hostname
- Example: Bootstrapping `example.co.uk` via `ns1.desec.io` requires:

`_dsboot.example.co.uk._signal.ns1.desec.io. IN CDS ...`

No automation so far.

- Hackathon plan: Automatically generate these records, either via
 - period cronjob, or
 - dynamic synthesis (by nameserver when queried)

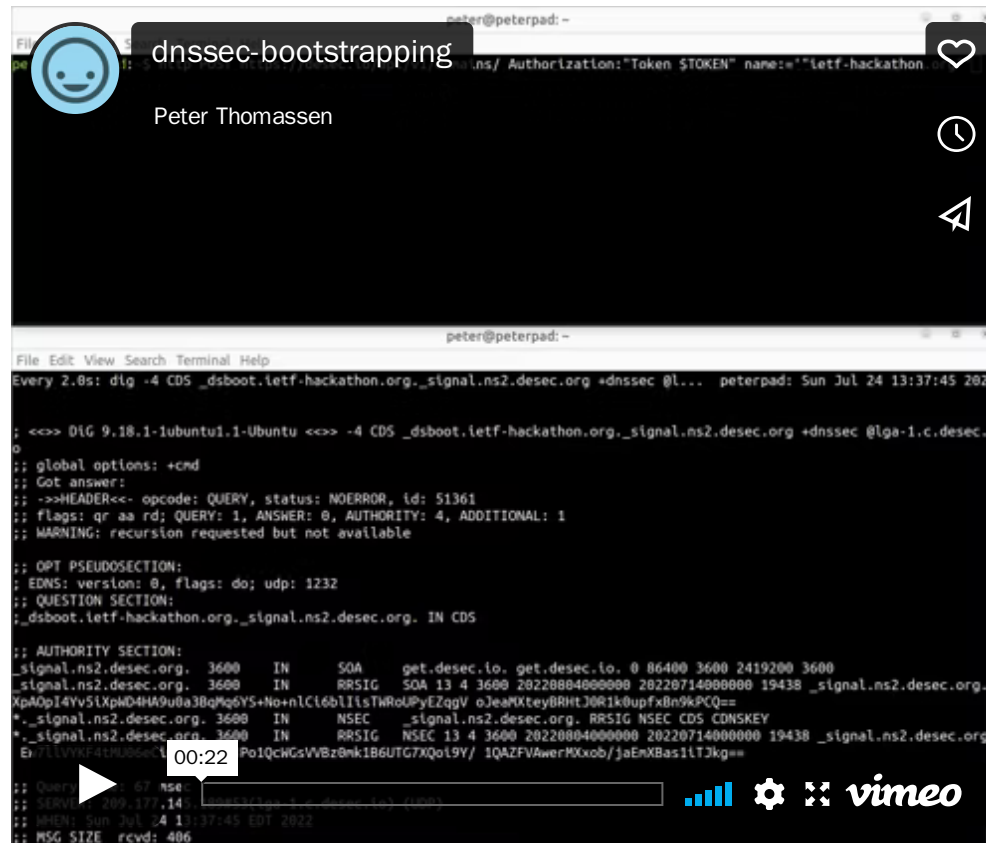
What got done

- Agreement: Expose only minimal configuration to admin
 - Tagging a zone as "bootstrapping zone" enables synthesis for all managed zones
- Code (deployed):
 - deployed:
 - saltant.net: cronjob (catalog zone → bootstrap zone) ([Gitlab repo](#))
 - at deSEC: PowerDNS record synthesis ([deSEC PR #46](#))
 - in the works:
 - Knot DNS module
- Techniques:
 - cronjob: Python script
 - PowerDNS: LUA records
 - Knot DNS: native C module

What we learned

- Pretty straightforward, plan worked overall
- Learned some things about LUA – good to have an expert at the table :-)
- Unexpected insight: bootstrap zones also have 2 NS records
→ need to have them on two secondaries
 - e.g. `_signal.ns1.desec.io` is hosted on ns1 *and* ns2
- Protocol seems workable in practice

Video demo



The screenshot shows a video player interface. At the top, there is a header bar with a blue circular profile icon on the left, the text "dnssec-bootstrapping" in the center, and a heart icon on the right. Below the header, the name "Peter Thomassen" is displayed. The main area of the video player shows a terminal window with the following content:

```
peter@peterpad: -  
File Edit View Search Terminal Help  
Every 2.8s: dig -4 CDS _dsboot.ietf-hackathon.org._signal.ns2.desec.org +dnssec @l... peterpad: Sun Jul 24 13:37:45 2022  
  
; <=> Dig 9.18.1-ubuntu1.1-Ubuntu <=> -4 CDS _dsboot.ietf-hackathon.org._signal.ns2.desec.org +dnssec @lga-1.c.desec.l  
o  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<-- opcode: QUERY, status: NOERROR, id: 51361  
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1  
;; WARNING: recursion requested but not available  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags: do; udp: 1232  
;; QUESTION SECTION:  
; _dsboot.ietf-hackathon.org._signal.ns2.desec.org. IN CDS  
  
;; AUTHORITY SECTION:  
_signal.ns2.desec.org. 3600 IN SOA get.desec.lo. get.desec.lo. 0 86400 3600 2419200 3600  
_signal.ns2.desec.org. 3600 IN RRSIG SOA 13 4 3600 20220804000000 20220714000000 19438 _signal.ns2.desec.org.  
XpAOpI4Yv5lXpM4HA9u0a3BoMq6Y5+No+nLC16b1IisTWRoUPyEZqgV oJeaMXteyBRHtJ0R1k0upfx8n9%PCQ==  
*_signal.ns2.desec.org. 3600 IN NSEC _signal.ns2.desec.org. RRSIG NSEC CDS CDSKEY  
*_signal.ns2.desec.org. 3600 IN RRSIG NSEC 13 4 3600 20220804000000 20220714000000 19438 _signal.ns2.desec.org.  
En7llvKf4tU066C1 Po1QchGsVVBz0nk1B6UTGXQol9Y/ 1QAZFVAwerMXxob/jaEnXBasi1tJkg==  
  
;; Query time: 67 msec  
;; SERVER: 209.177.14. (209.177.14.1) (UDP)  
;; WHEN: Sun Jul 24 13:37:45 EDT 2022  
;; MSG SIZE rcvd: 406
```

At the bottom of the terminal window, there is a play button icon, a progress bar with the time "00:22", and a Vimeo logo.

Wrap up

Team members:

Cronjob:

- John O'Brien

PowerDNS synthesis:

- Jerry Lundström
- Nils Wisiol

Knot DNS synthesis:

- Peter Thomassen

First timers @ IETF/Hackathon:

- John O'Brien
- Nils Wisiol