Safer DNSSEC

Viktor Dukhovni

Google Public DNS

Presented at OARC39 Workshop
[Based on ICANN75 talk]

Agenda

DNSSEC Today

Critical zones

Safer DNSSEC

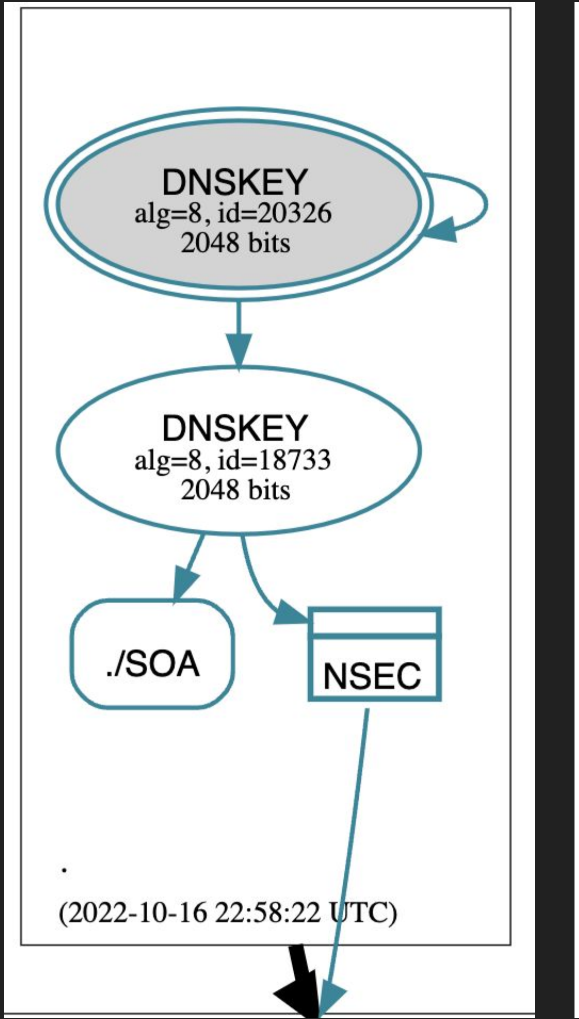
Next steps: plea for feedback from Registry Operators (and others)

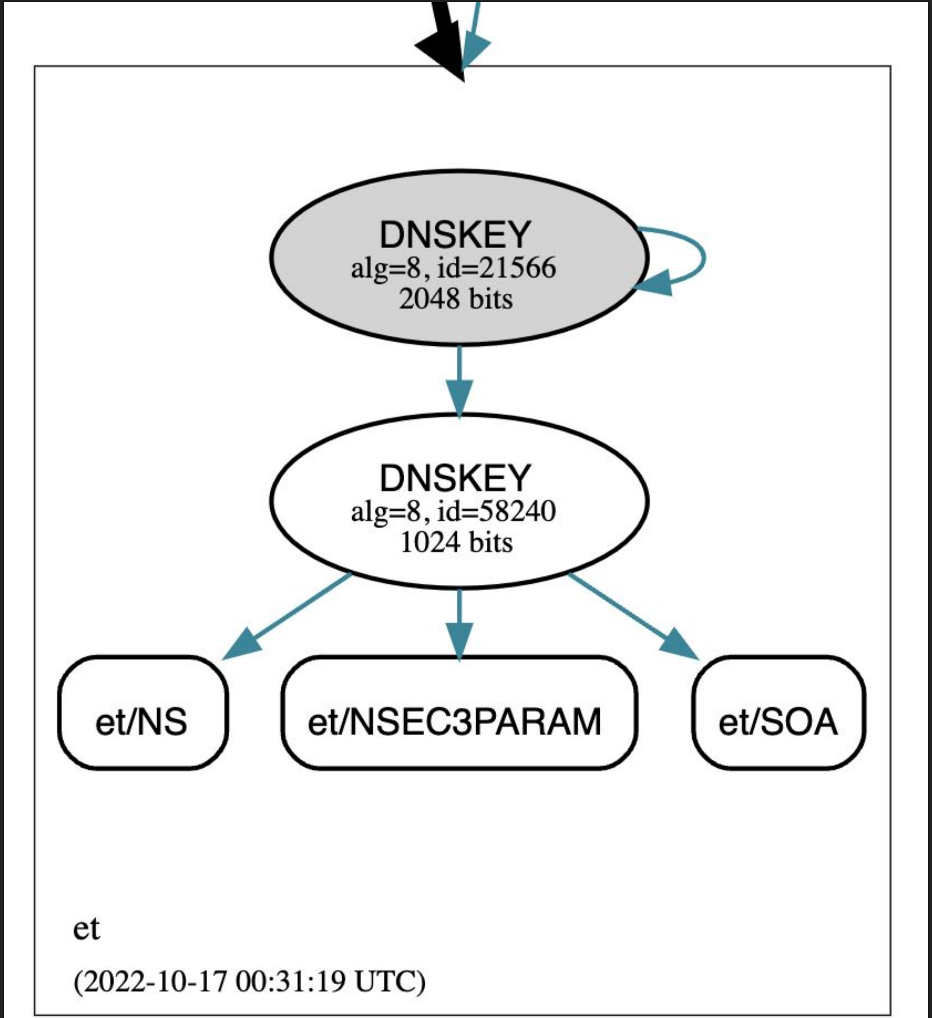
DNSSEC Enrollment Today

- **Child zone DNS operator signs the zone**
  - Low risk, increasingly well automated, including ZSK rollovers
  - Some operators sign most customer zones by default
  - May also partly automate KSK rollovers by publishing CDS and waiting for matching DS
- Registrant communicates associated DS or DNSKEY records to Registrar
  - Can be tedious and error prone
  - Often neglected when DNS operator != Registrar
- Registrar submits DS (or DNSKEY) records to registry
  - Long DS TTLs leave little slack for errors:
    - High risk of sustained down time
    - Poorly executed backout also risky
  - Often no validation by either the registry or registrar

Sign and Pray

- Upload **DS** records into parent zone via registrar, often clunky web form
  - Hope DS records are entered correctly
  - Hope zone is correctly signed
  - Hope no unexpected authoritative nameserver bugs
  - Hope no critical applications or users adversely affected (latent bug)
- No possibility of timely rollback
  - Parent-side DS records often have one or two day TTLs
  - How quickly can bad records be removed or updated?
- No parent-side DS validation
  - gTLD registries ***obliged*** to publish DS records that ***brick*** your zone
- **Critical production zones reluctant to deploy DNSSEC**


DNSKEY
alg=8, id=20326
2048 bits
DNSKEY
alg=8, id=18733
2048 bits
./SOA
NSEC
.
(2022-10-16 22:58:22 UTC)


DNSKEY
alg=8, id=21566
2048 bits
DNSKEY
alg=8, id=58240
1024 bits
et/NS
et/NSEC3PARAM
et/SOA
et
(2022-10-17 00:31:19 UTC)

Critical zones

- Users and customers rely on and expect ***always on*** service
- Each minute of downtime carries substantial costs
- Disdain changes that can’t be rolled out regionally and progressively
- Instill a “*roll back first, debug later*” culture
- **Critical production zones reluctant to deploy DNSSEC**

Safer DNSSEC

- Short initial **DS** RRset TTLs
- Prompt **DS** rollback and update
- Pre-publication **DS** validation

Short initial DS TTLs (Registry)

- **DS** RRsets get a short initial TTL after ***any*** change
  - Not just when zone is first delegated signed
- Initial TTL as low as **~60s**!
- TTL can grow (incrementally or just once) when resigned unchanged
  - Resigning could be expedited (hours rather than days) while the TTL is low
- Opt-in or default for all delegations?
- Is there a role for signalling from the child zone?
  - Via TTL of CDS or DNSKEY RRsets?

Prompt rollback (Registry and Registrar)

- At most minutes to remove **DS** or update to prior working state
- Presumes short TTL to be effective
- Naturally implies prompt signing of
  - new NSEC/NSEC3 record if DS is removed, or
  - new DS RRSIG if DS updated (note, subject to validation!)
  - *Not compatible with Infrequent whole zone signing*
- Is timeliness adequately covered under existing registry SLAs?
  - e.g. ICANN gTLD requirements?

Pre-publication DS validation

- Reject **DS** changes that invalidate child zone
  - Via any of its (active) servers
  - With respect to any of the signalled algorithms
- Should registrar staple validated CDS in-lieu of registry probing?
- Should validation be opt-in for some or default for all child zones?
- Should matching CDS be required to confirm DS changes?
  - Too strict as default, would require prior opt-in
  - Should NS and glue changes also be pre-validated?
- How does this relate to registry lock?
  - [A precedent for limited direct Registry to Registrant relationship]

Next Steps and request for feedback

- What else would be a **practical** means to reduce deployment risk?
- Looking for assistance and feedback
  - Primarily Registry Operators (gTLD and ccTLD)
  - ICANN
  - Auth zone operators
  - Critical zone registrants
  - The DNS community

Thank You. Q&A

Related effort:

- https://datatracker.ietf.org/meeting/114/materials/slides-114-dnsop-slides-114-dnsop-dry-run-dnnsec-00

DNSSEC (and DANE SMTP) deployment statistics:

- https://stats.dnssec-tools.org

DANE DNSSEC running commentary:

- https://twitter.com/VDukhovni/with_replies