



rm -rf SHA-1: Algorithm Rolls En Masse

Howard Eland

2021-05-27

Background

- Over 50 million resource records pre-DNSSEC
- Started DNSSEC operations in 2008
- NSEC3 with Opt Out, Algorithm 7 (RSASHA1-NSEC3-SHA1)
- Type 1 and 2 DS records
- Hash Iterations = 1, static salt, next KSK pre-publish



Driving Factors

Scope

While removing risk of using SHA-1 was the impetus behind this project, we took this opportunity to also:

- **Examine original DNSSEC implementation choices**
- **Reassess: does what made sense then still make sense now?**
- **Evaluate signer capabilities with newer algorithms**

Zones In Scope

- **209 TLDs**
- **208 nic.\$TLD zones, second level and sub-zones**
- **417 zones total**

Bonus Challenges

- **Many TLDs were *also* mid-KSK roll**
- **Many Customers are the IANA Administrative contact**
- **ICANN knocking on our door**
- **Tools starting to warn about SHA-1 (DNSViz, etc.)**

Research

Learned from others' strife

With **MANY** thanks to all:

- [DNSSEC Algorithm Roll-over | RIPE Labs](#)
- [Keep 'm rolling: monitoring .se's DNSSEC algorithm rollover](#)

Lab Testing

- **Algorithm tests**
 - SHA-256 ran without issues
 - ECDSA took too long for production signing
- **Other testing:**
 - Hash iteration increase to 100
 - Stop KSK pre-publish
 - Dropping DS type 1
 - RFC 6781, Section 4.1.4, conservative
 - Signer operations at each stage

Approach

Focus on Education and Notification

- Account Managers: KSK & algorithm roll processes, timelines
- Customers: what we're doing, and why
- IANA: Flood Warning
- **Tracking in Notion!**
 - Zones in table, with current status
 - Kanban and Gantt chart views

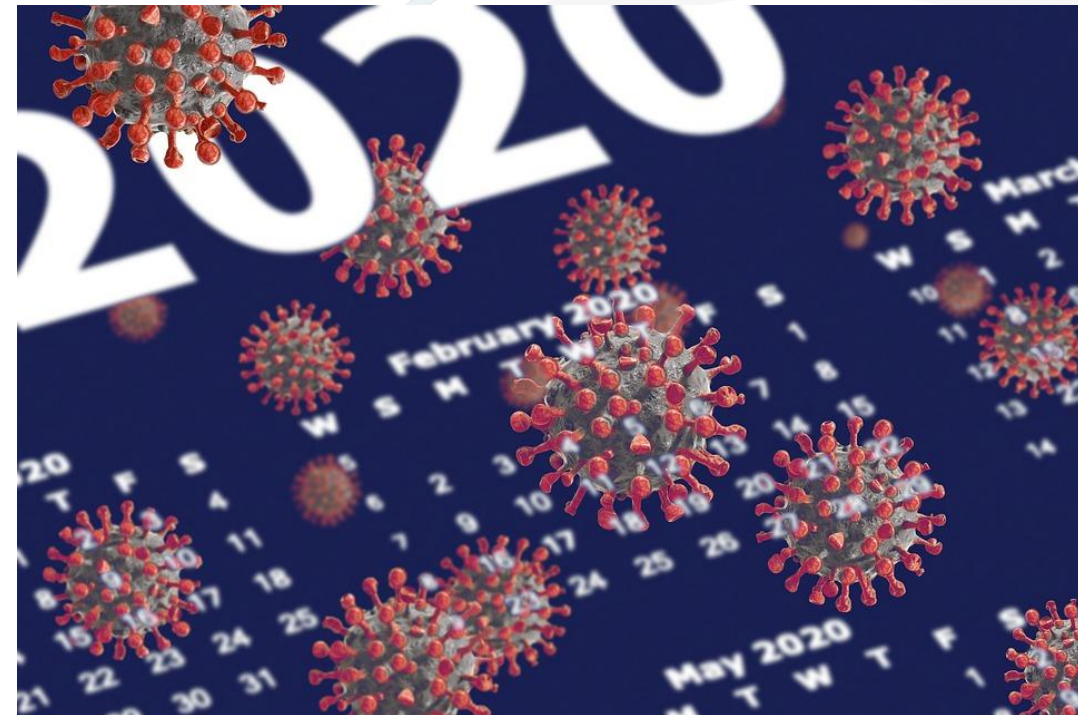
Zone Batches

For a given zone, finish KSK rolls, then proceed directly into algorithm rolls.

- **TLD Batches**
 - Proof of Concept (small subset of Afilias zones)
 - Afilias
 - PIR
 - newTLDs
 - ccTLDs
 - Australia
- **nic.\$TLD batches in parallel with parent zones**

Away We Go!

- Process start on Batch 1: 31 Aug 2020
- Most zones completed process in about 54 days
 - Each zone required 1 or 2 RZM requests
 - Re-signs on 1, 9, 17, 25 of each month
 - Most relevant TTLs were 86,400
- Current status: 416 / 417 completed
 - last TLD is finishing first KSK roll
- Expected finish: 30 Jun 2021

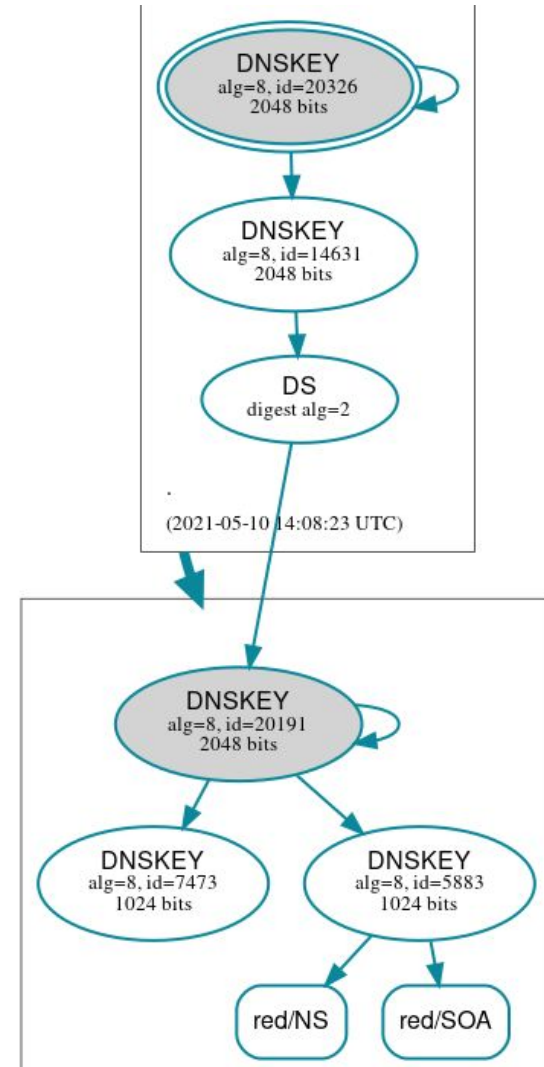
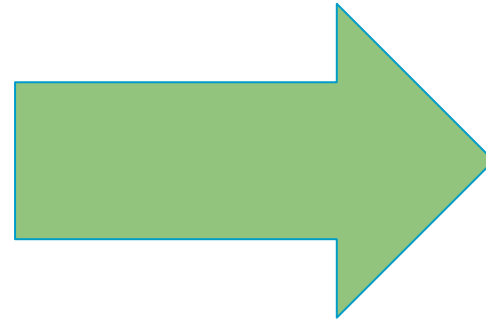
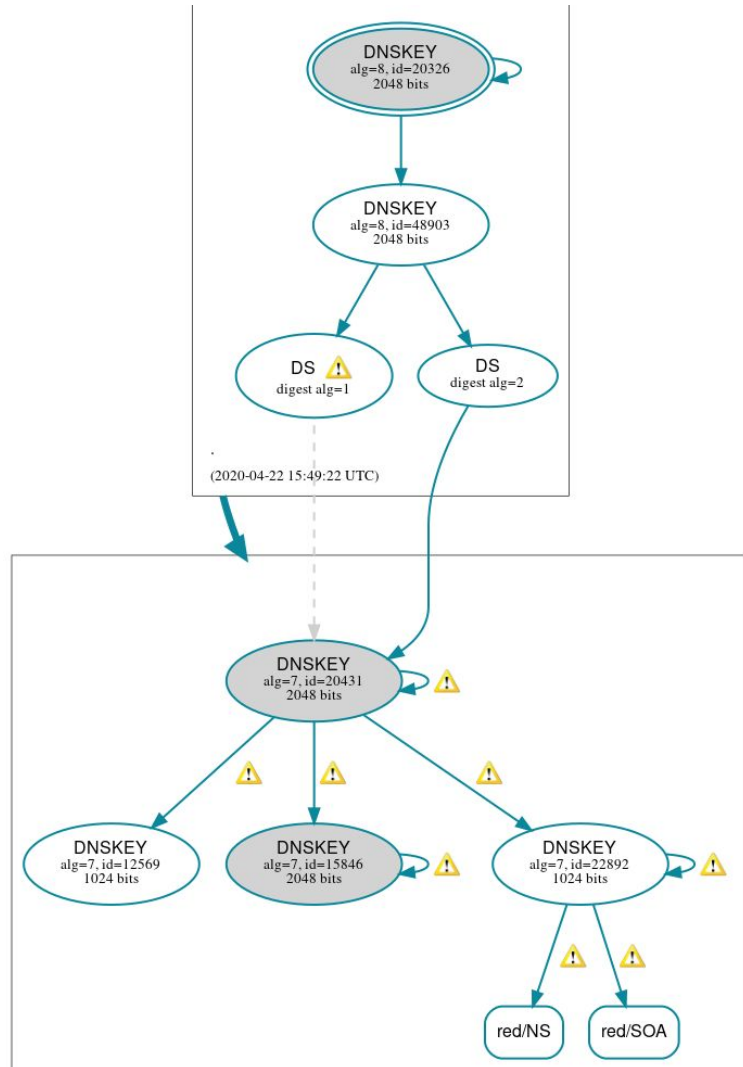


Results

- All zones now on algorithm 8
- Single DS, digest type 2
- Salt changed
- Hash iterations ultimately reduced to 10
- KSK pre-publish removed
- ZSK no longer signing DNSKEY RRSet

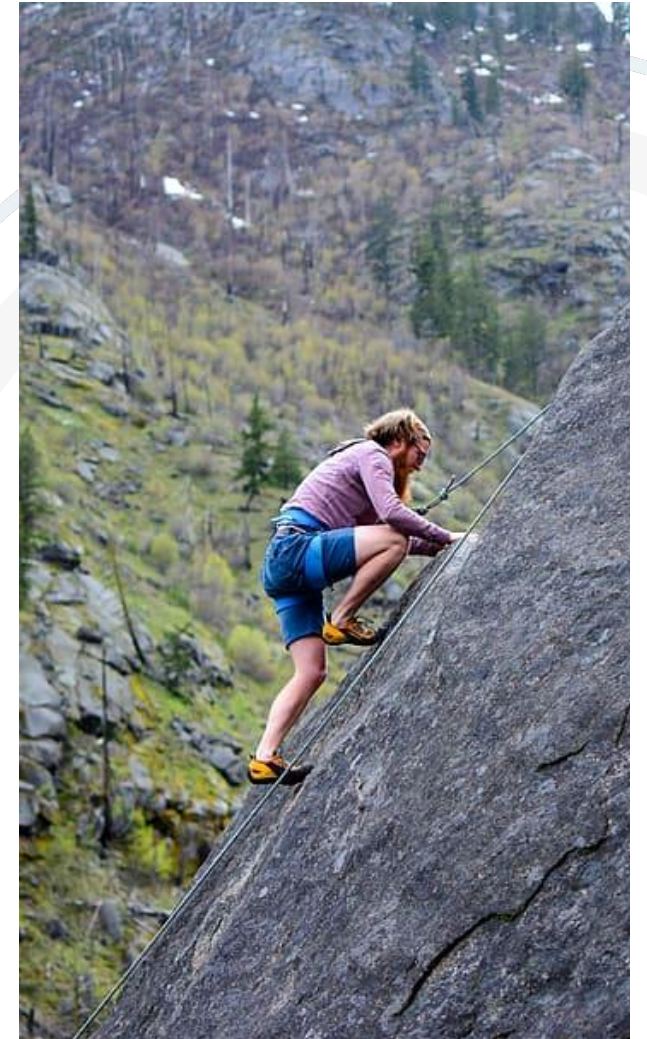


Before and After - red TLD



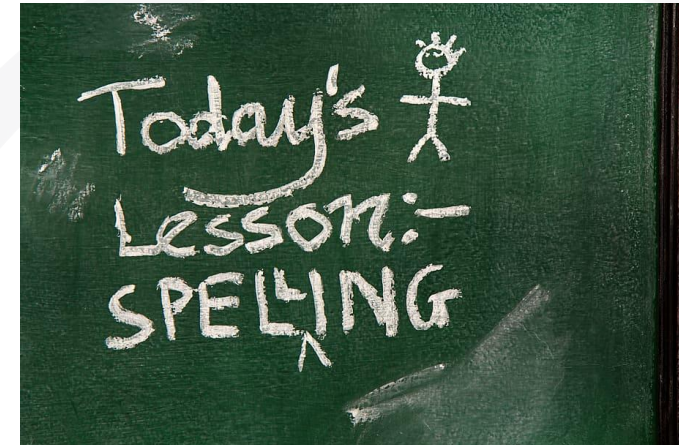
Challenges

- One zone had some signatures drop for short period of time
 - Signer bug triggered by configuration change
- “Auto-manual” RZM changes
 - Scripts to generate request data, check request before lodging, confirmation emails
 - Manual Q/C after each step, Notion updates
 - Couple of “odd” RZM process states - self-cleared?
- Delays waiting for ROs to confirm RZM requests
 - Some needed contact changes, “letterhead” style
- Plus something about a global pandemic...



Recommendations / Lessons Learned

- Keep IANA contacts current!
 - Role accounts, with group email addresses
- Watch timings carefully
 - Ensure you leave enough time between steps
 - Know which TTLs affect which steps
- Communications key
 - Inform everyone impacted - no avoidable surprises
- Know your systems limitations
 - Lab test **every** step



Shoutouts

Special thanks to the following:

- Carl Clements (Afilias): he did the real work!
- Joe Abley (PIR): recommendations and advice
- George Sarkisyan and Selina Harrington (IANA/PTI): troopers through all of these changes!



Thank You - Questions?

I can be reached at: heland@afiliat.com ^H^H^H howard@donuts.email

