
ICANN
VIRTUAL COMMUNITY FORUM
70

DNSSEC Deployment among TLDs

1 July 2011 to 15 March 2021

Edward Lewis

ICANN 70 DNSSEC and Security Workshop
24 March 2021

Agenda

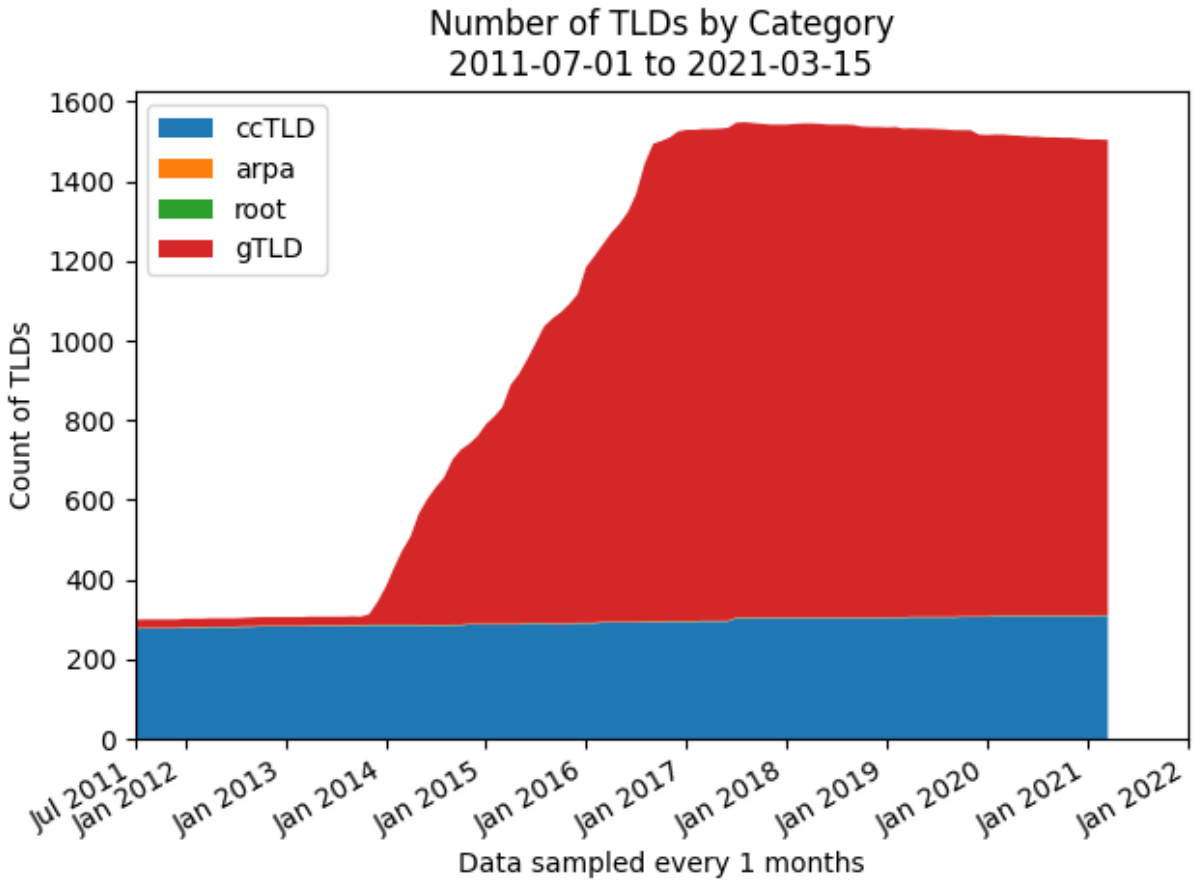
- Context: Changes to the Root Zone in the 2010's
- DNSSEC Deployment by "levels"
- Cryptographic and other operational choices
- Signs of change, even after a decade of operating

A decade of Root Zone changes

In the last 10 years,
gTLDs have grown to dominate the root zone

All new gTLDs after 2012 must start with full DNSSEC, skewing adoption curves

ccTLDs show a more "organic" growth of DNSSEC, qualifying this would overwhelm the slide

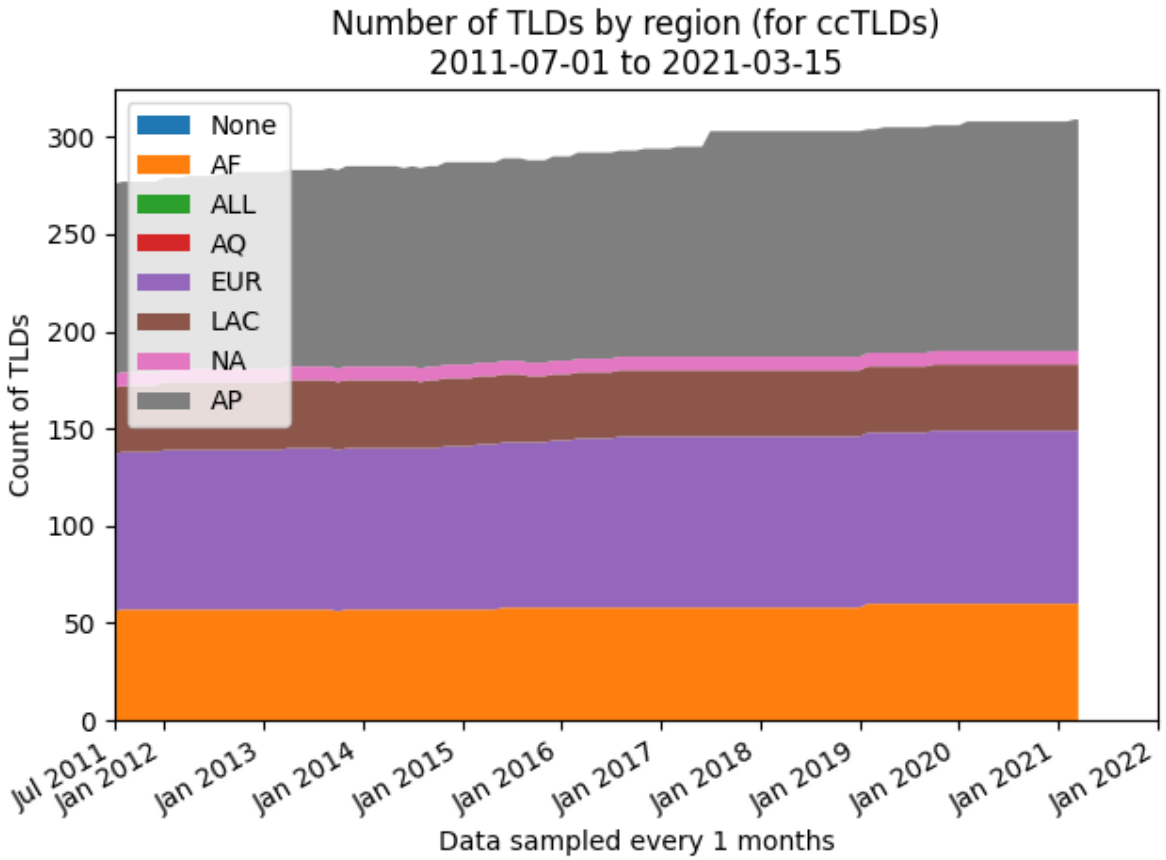


ccTLDs divided by regions

With a focus on ccTLDs, it's helpful to see the relative sizes of groupings used

ccTLDs have an inherent jurisdiction and thus a region

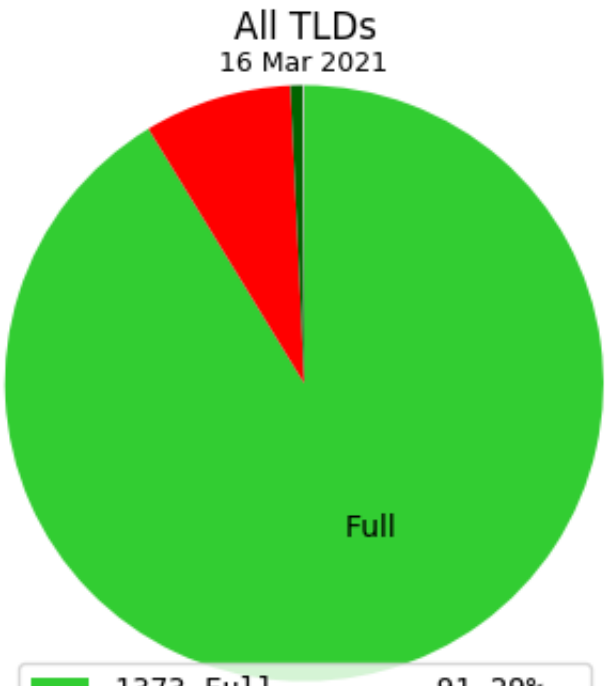
"Regions" taken from https://meetings.icann.org/en/regions

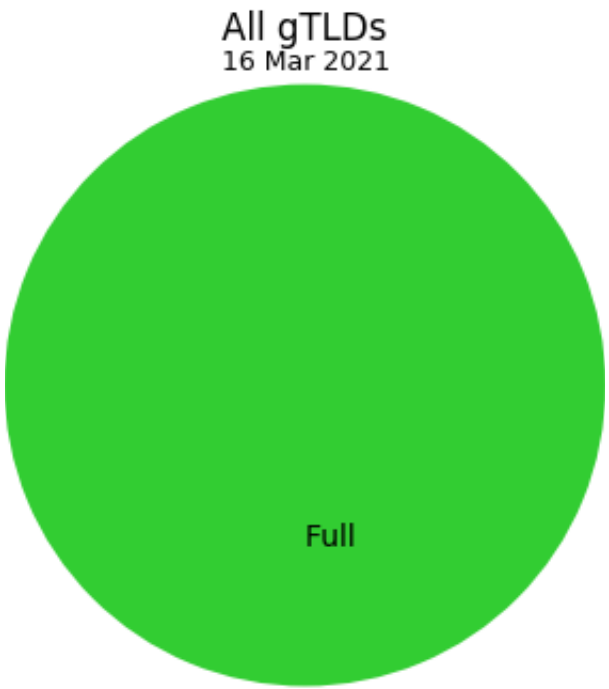


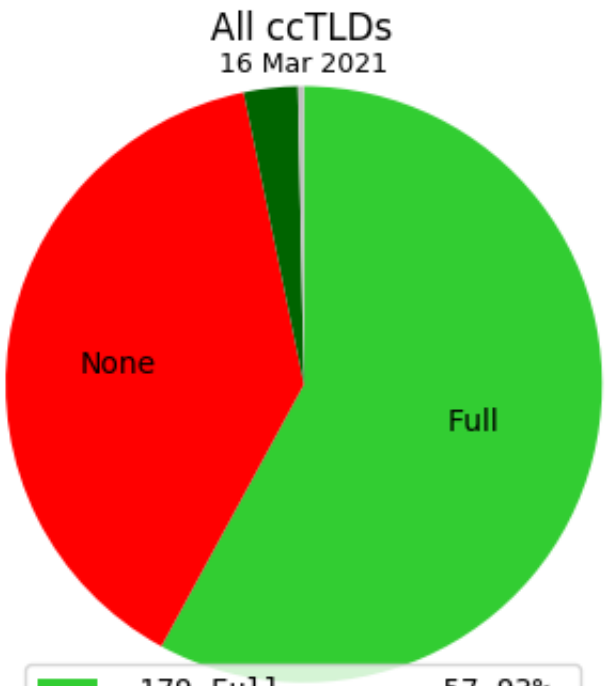
DNSSEC Deployment in TLDs

- In the following charts
  - "Full" – TLD is signed and has a DS record
  - "Signatures" – TLD publishes a signed zone
  - "Keys" – TLD publishes a key but no signatures
  - "None" – No DNSSEC deployment
- By those rules, the root zone is "only" rated as "Signatures" as there is no DS record for it (can't be one!)
- Not measured – delegations' (below, inside ccTLDs) DNSSEC, and the reverse map zones

DNSSEC Deployment Level

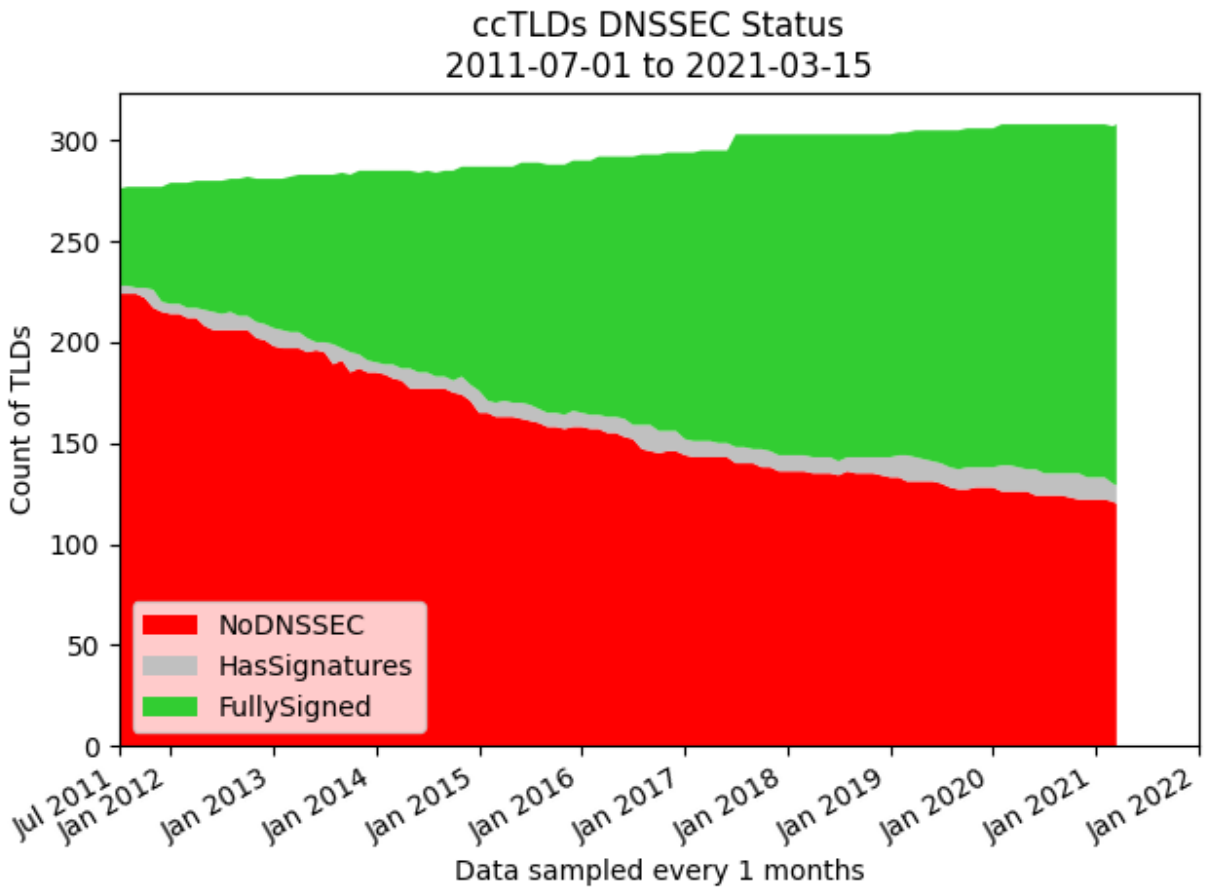






1504 – (1193 + 309) = 2, those "2" are ARPA and the root itself

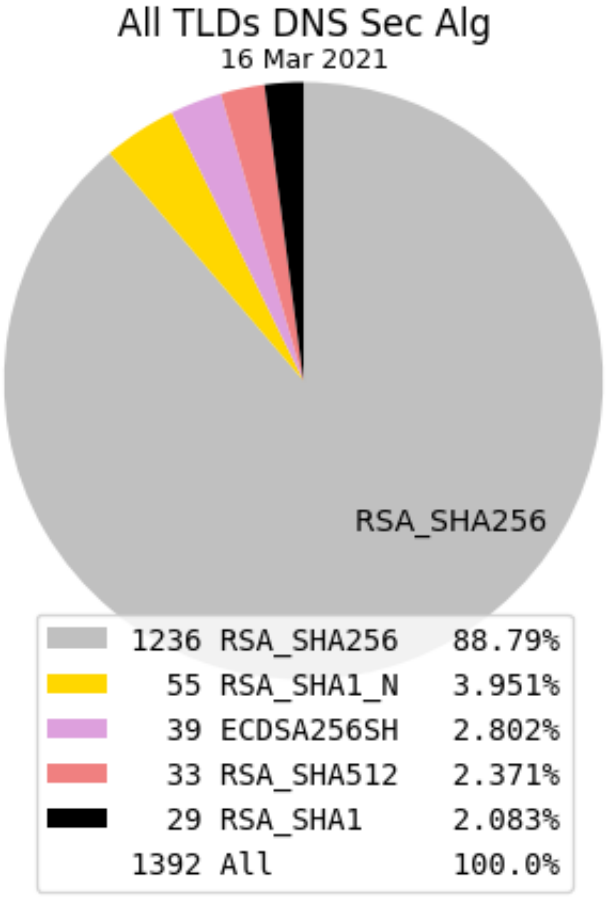
DNSSEC Deployment Level in ccTLDs - Trends

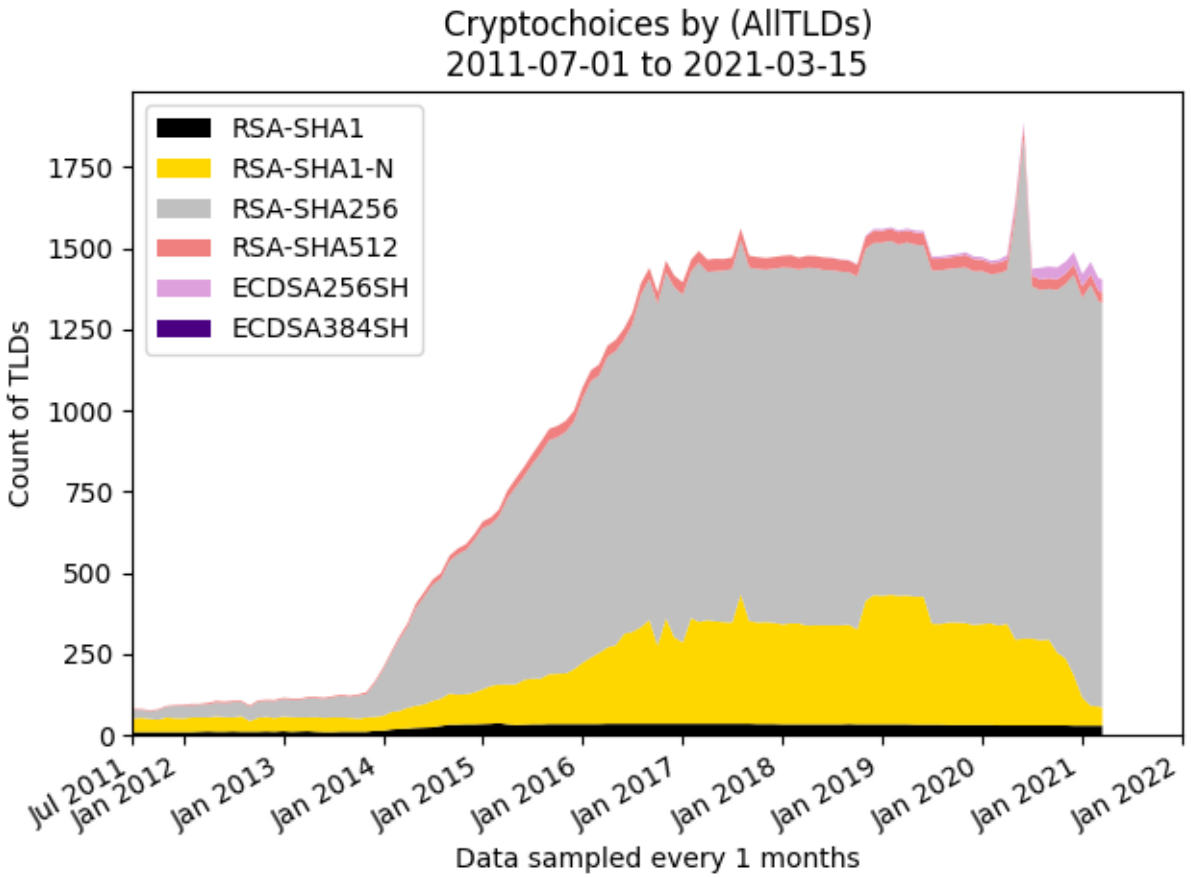


Cryptographic Choices

- DNSSEC Security Algorithm
  - Cryptography (DSA, RSA, Elliptic Curve, etc.)
  - Hash algorithm (SHA-1, SHA-256, etc.)
- The "best-est" algorithm changes over time
- A TLD may have more than one algorithm at one time

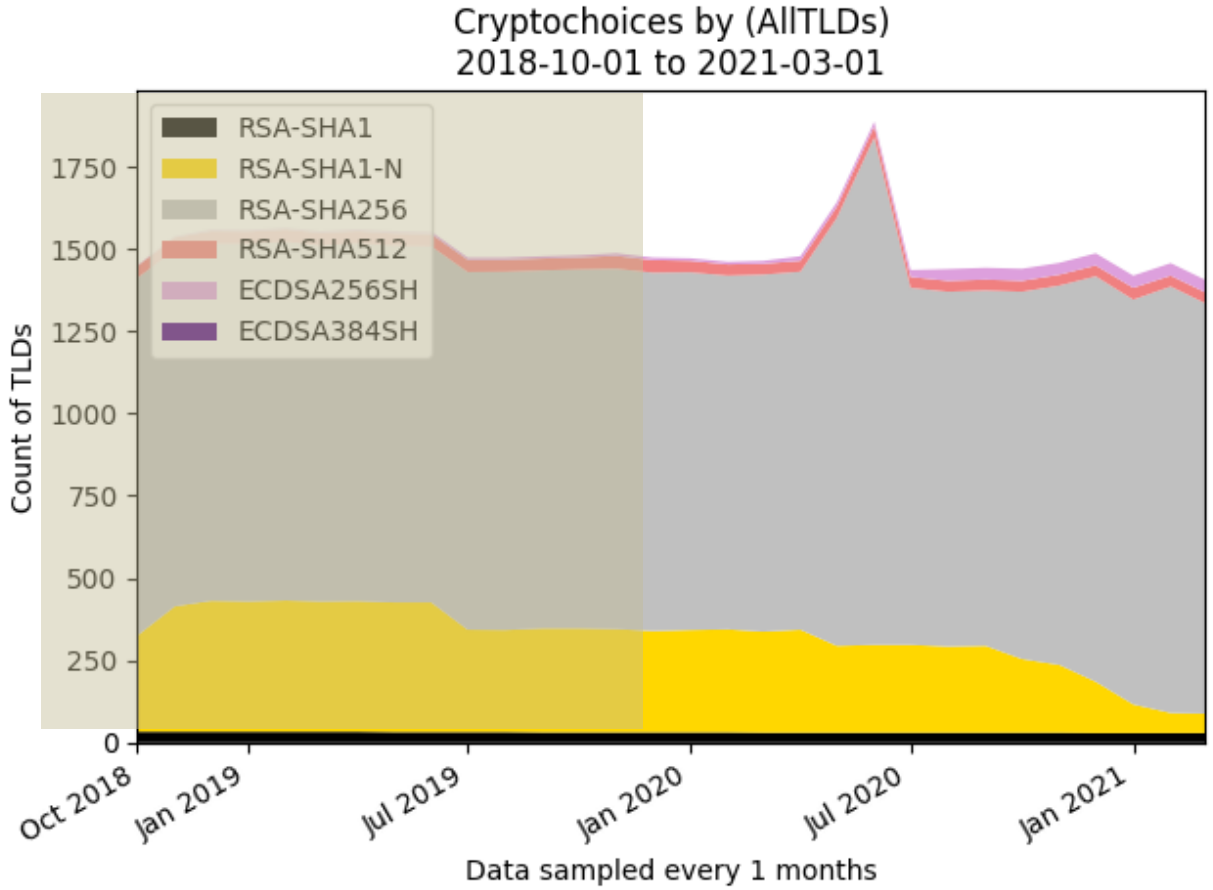
Cryptography Choices (All TLDs)





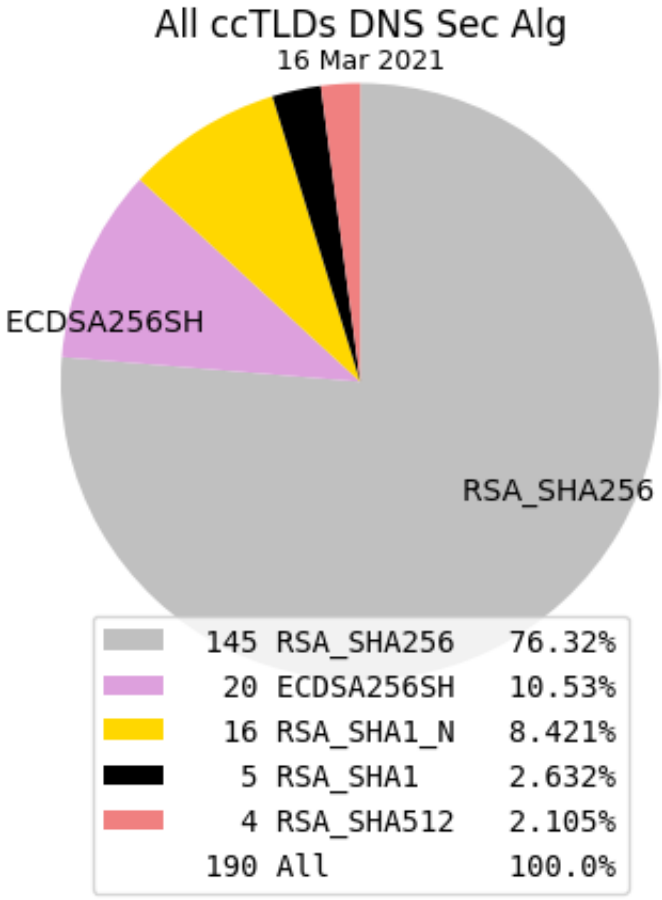
There are 1384 TLDs (including root) with keys; 1392 – 1384 = up to 8 TLDs have multiple

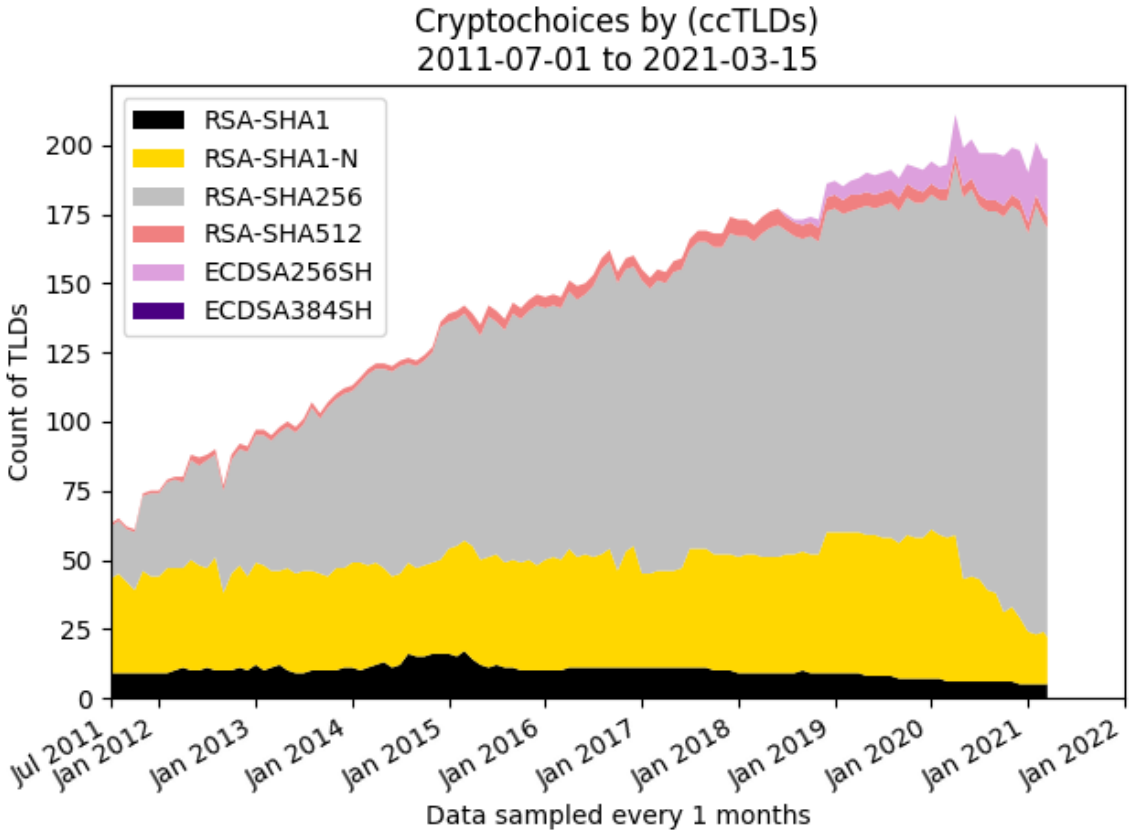
Cryptography Choice Changes during pandemic



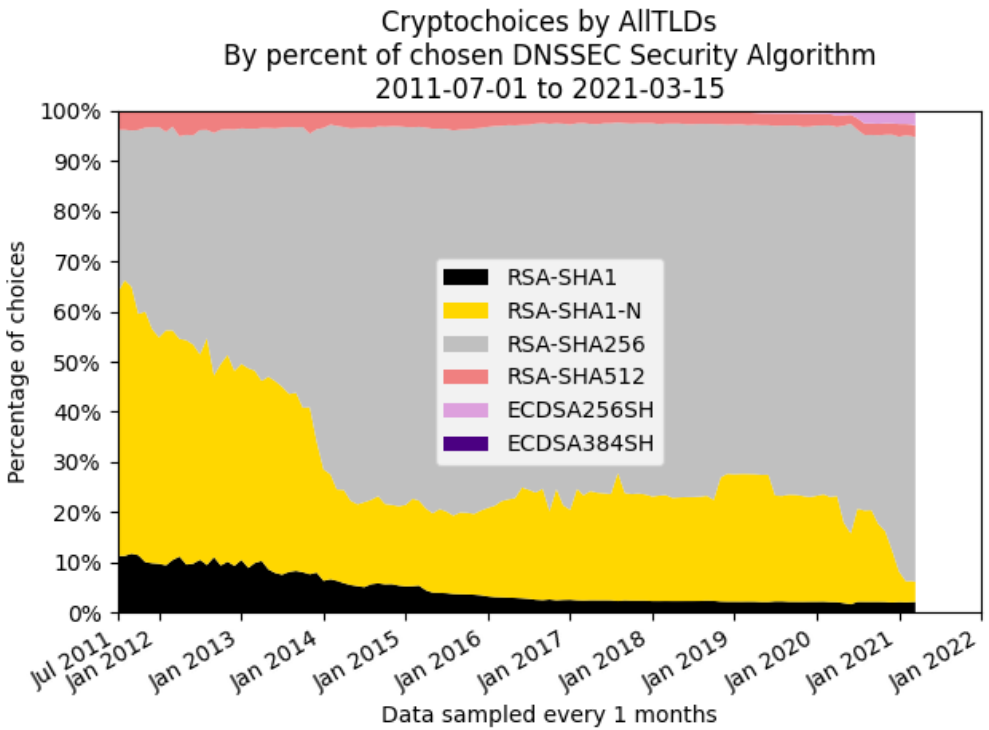
- Operators have been busy reconfiguring despite...
- Rate of change accelerated this year

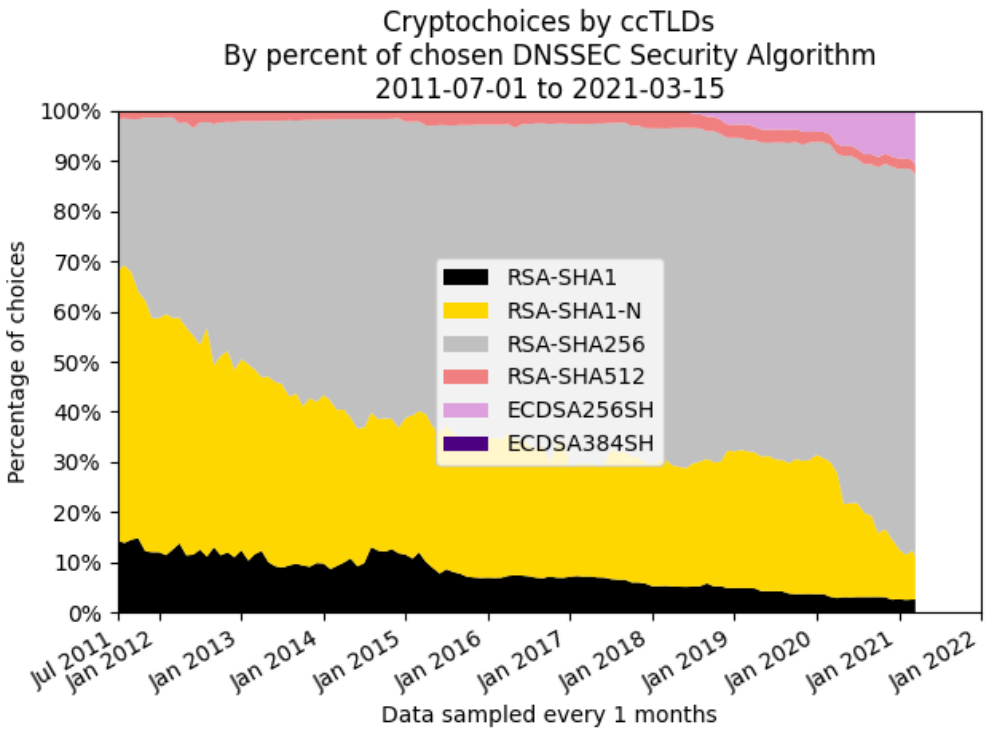
Cryptography Choices (ccTLDs)





Cryptography (All/ccTLD) – Trends using Percent

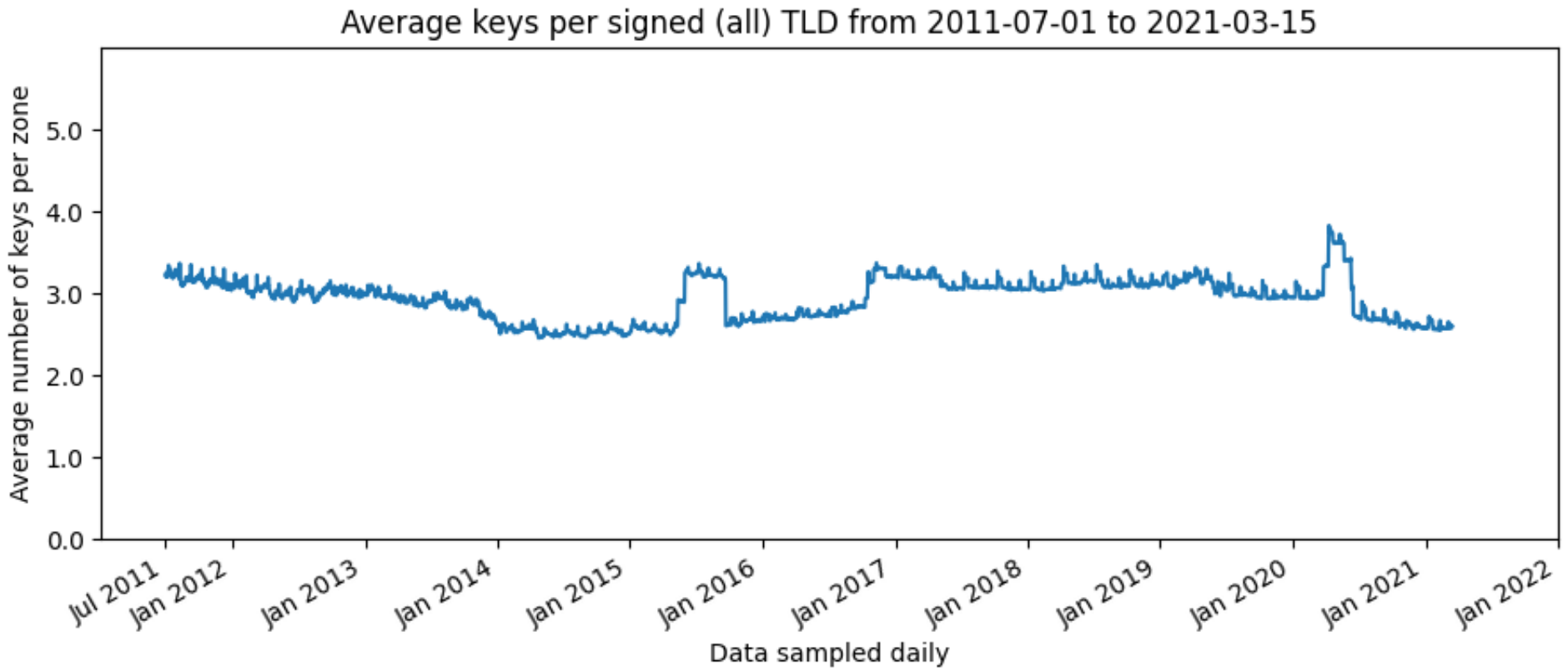




Number of Keys

- During the Root Zone KSK Rollover of 2017-2018
  - Concerned about the sizes of responses (bytes in a message)
- Noticed a few TLDs with many keys ("too many")
  - One experienced a failure, but unrelated to DNSSEC
  - Interviewed the engineer-on-deck, wasn't the "too many"
- Number of keys is not a primary measure
  - But charting it reveals patterns of operations (rolls)

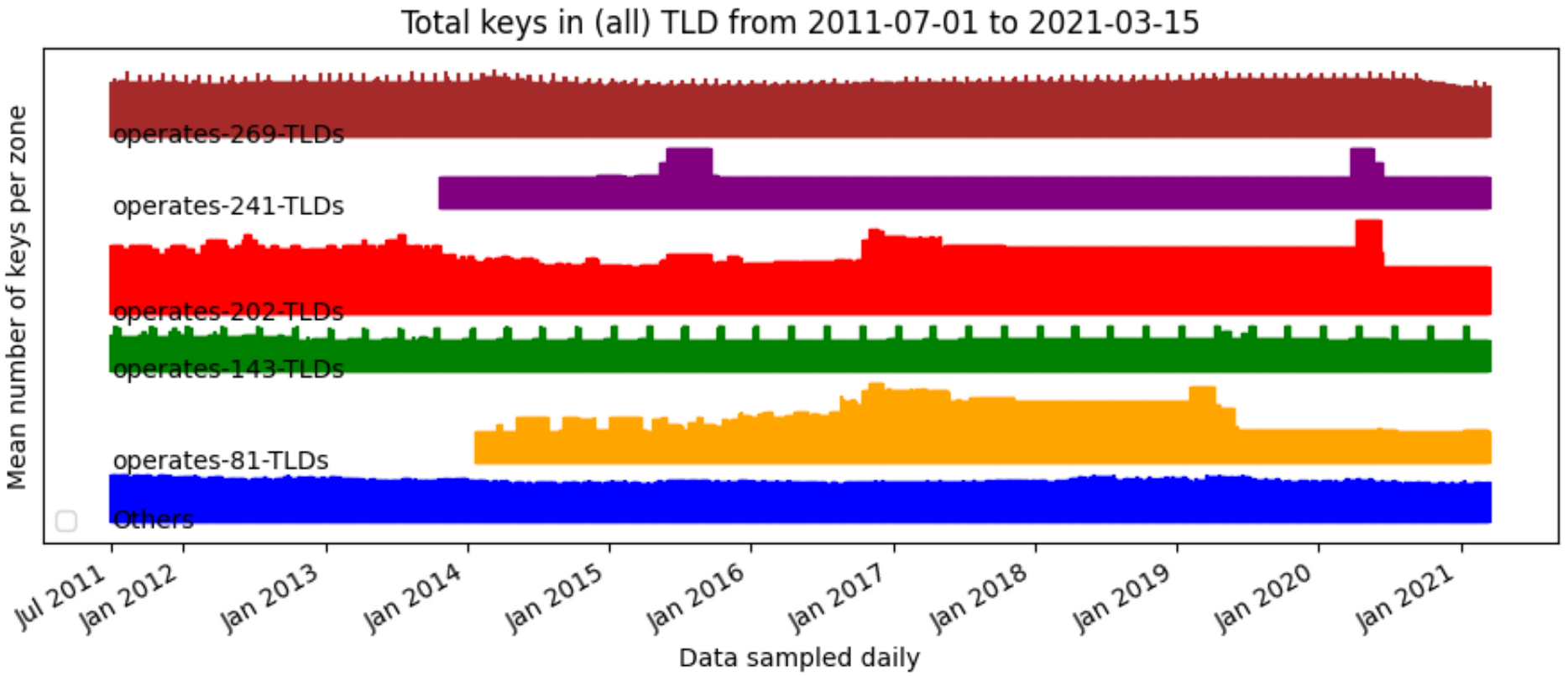
"Mean" Number of Keys (All)



Next two charts are a bit abstract

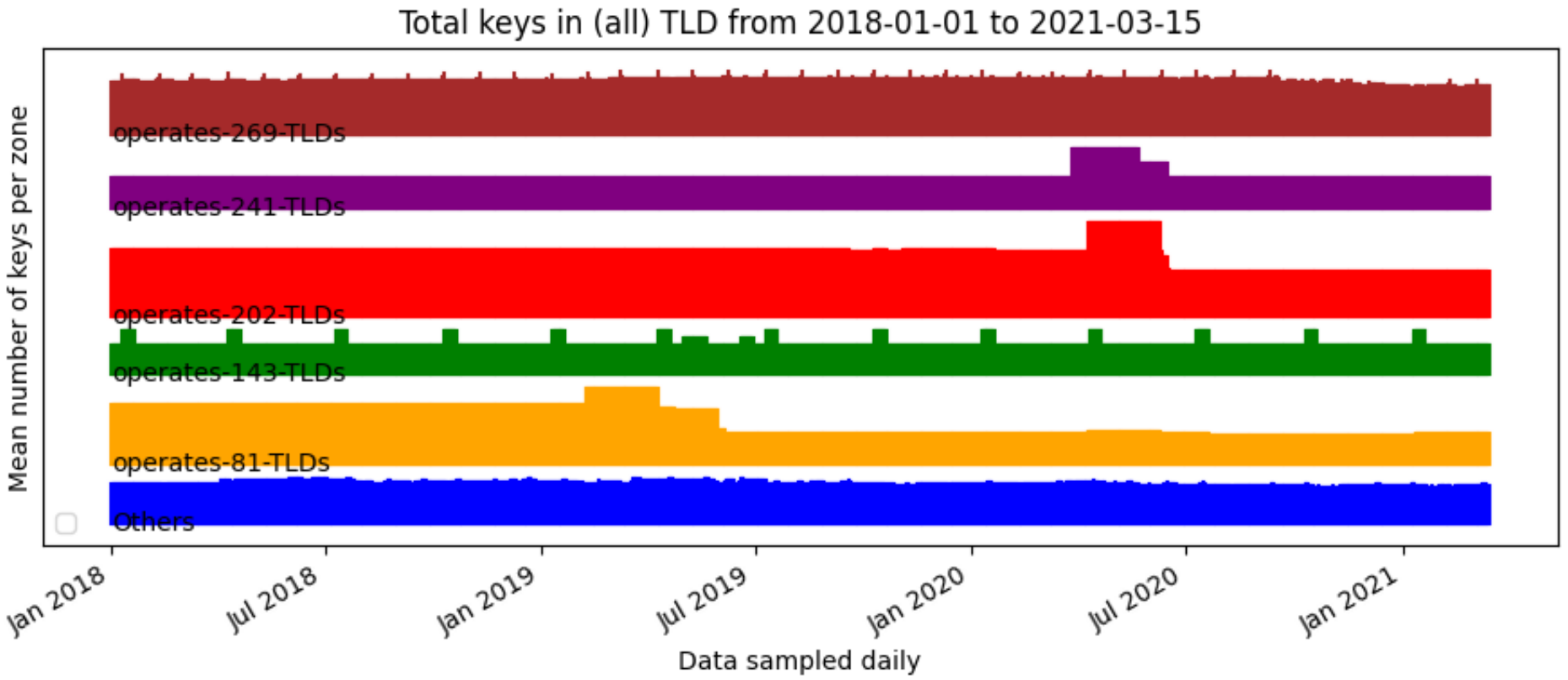
- Each color, except blue, represents the activity of one operator
- The height is the number of keys each uses divided by the number of zones; then multiplied by 10 to make the peaks more visible
- By selecting just a few years, each day is "wider" in pixels, to improve the visualization
- Two things are apparent – those that roll keys regularly and those who've changed their key publication strategy

Who's behind the bumps?



Back-end operators ("DNS House") – identified by a zone's SOA RR RNAME and IANA Technical Contact

Who's behind the bumps (2018-now)?

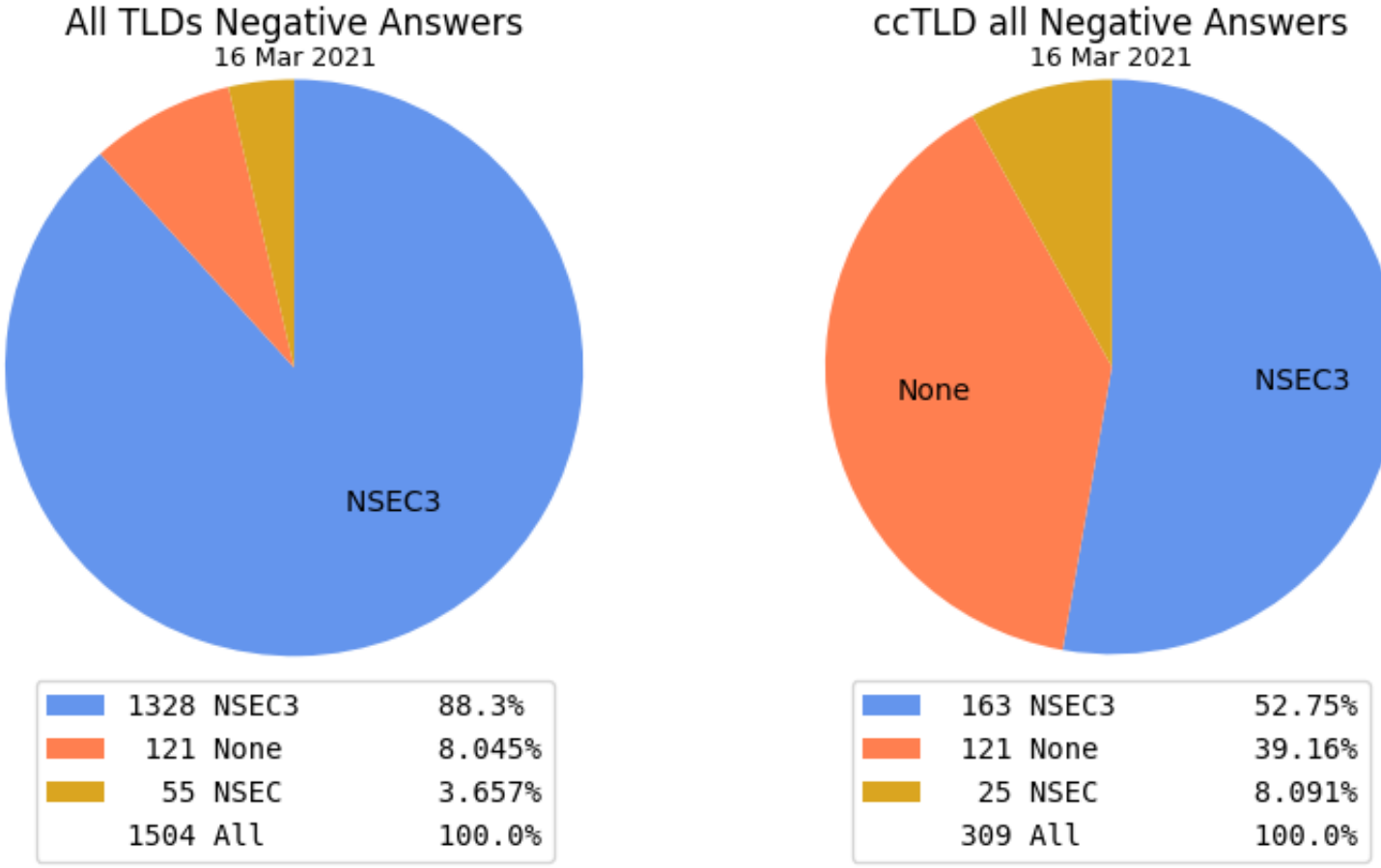


Negative Answer Choices

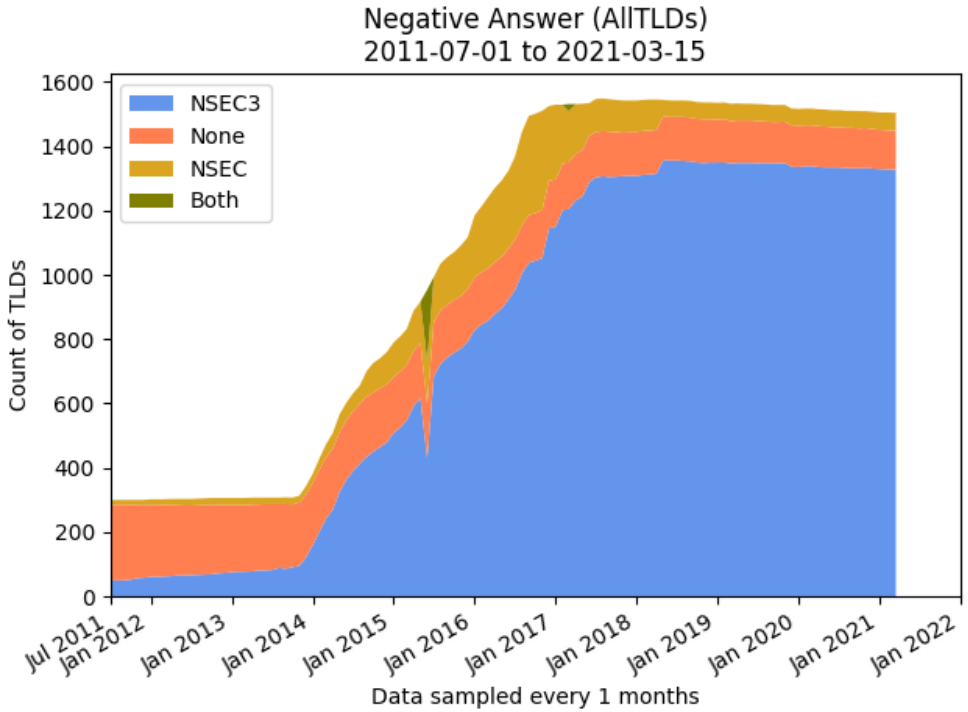
- NSEC vs. NSEC3
  - Consistently dominated by NSEC3 for TLDs
- "Both" means a TLD switched during a day of observations

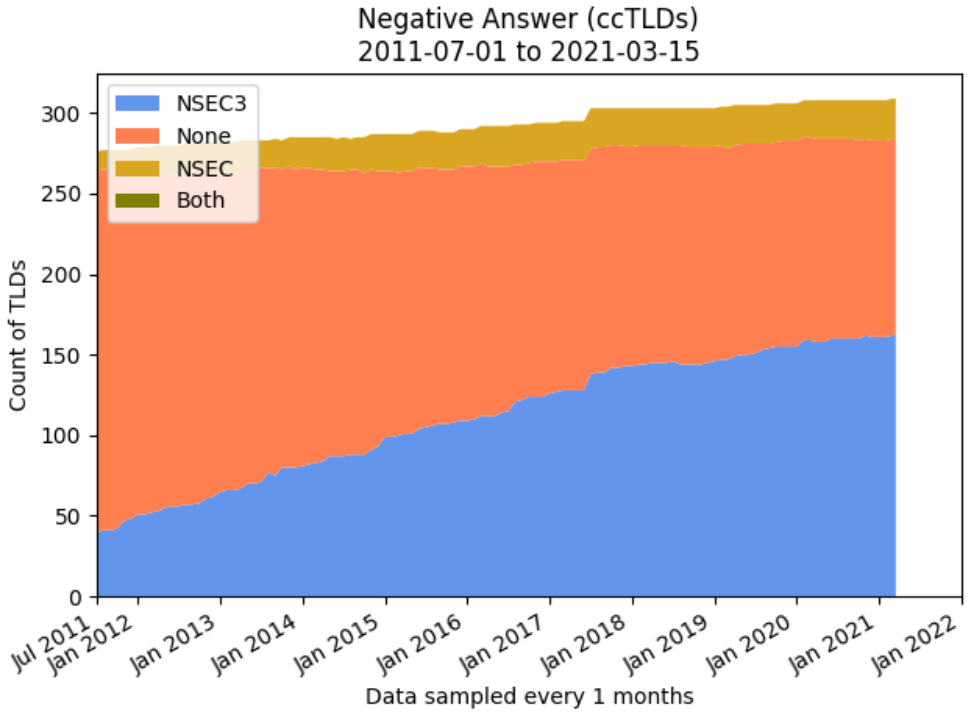
- NSEC 3 Iterations

Negative Answer Choices (All and ccTLDs)

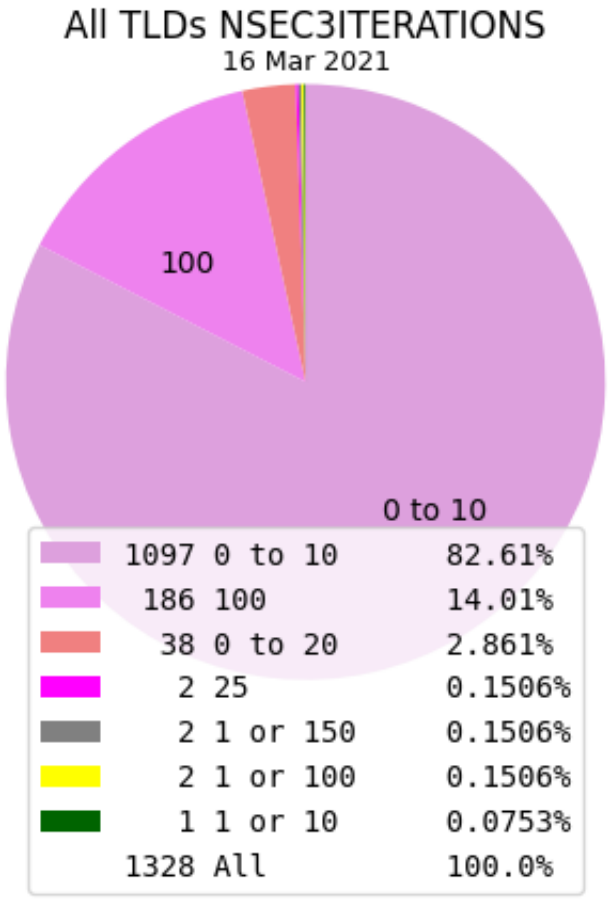


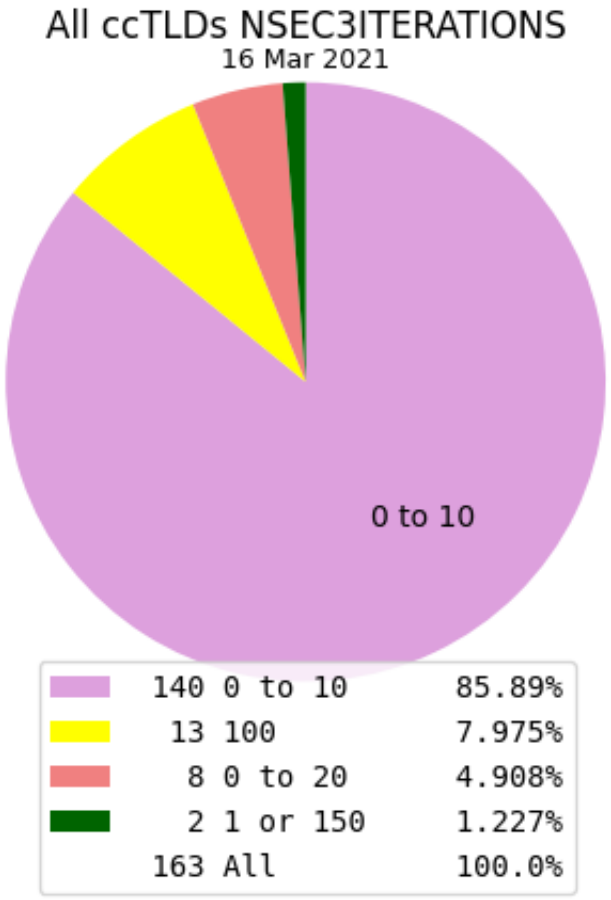
Negative Answer Choices (All and ccTLDs) - Trends





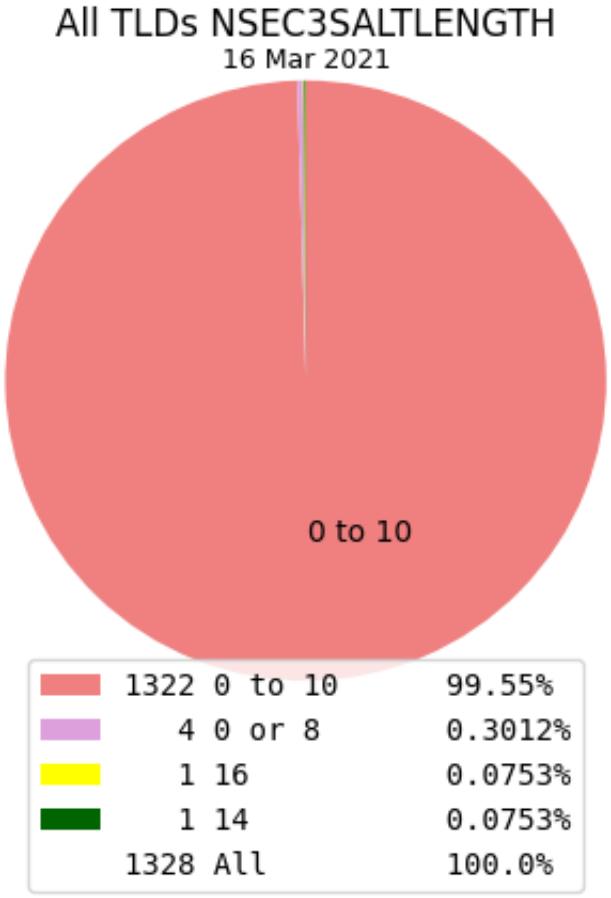
NSEC3 Iterations (All and ccTLDs)

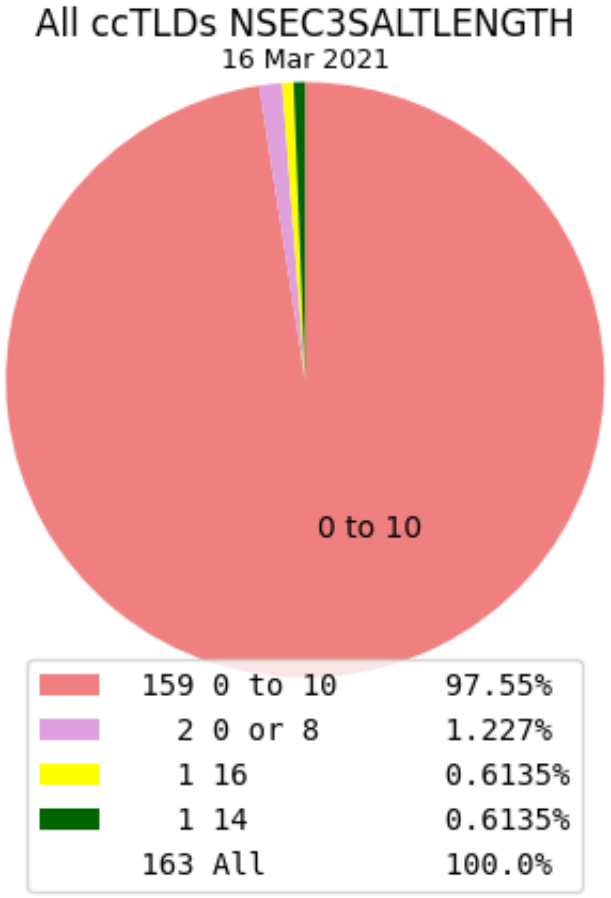




"x" or "y" – operators observed using different values; "x" to "y" means all values inclusive in the bucket

NSEC3 Salt Lengths - bytes (All and ccTLDs)



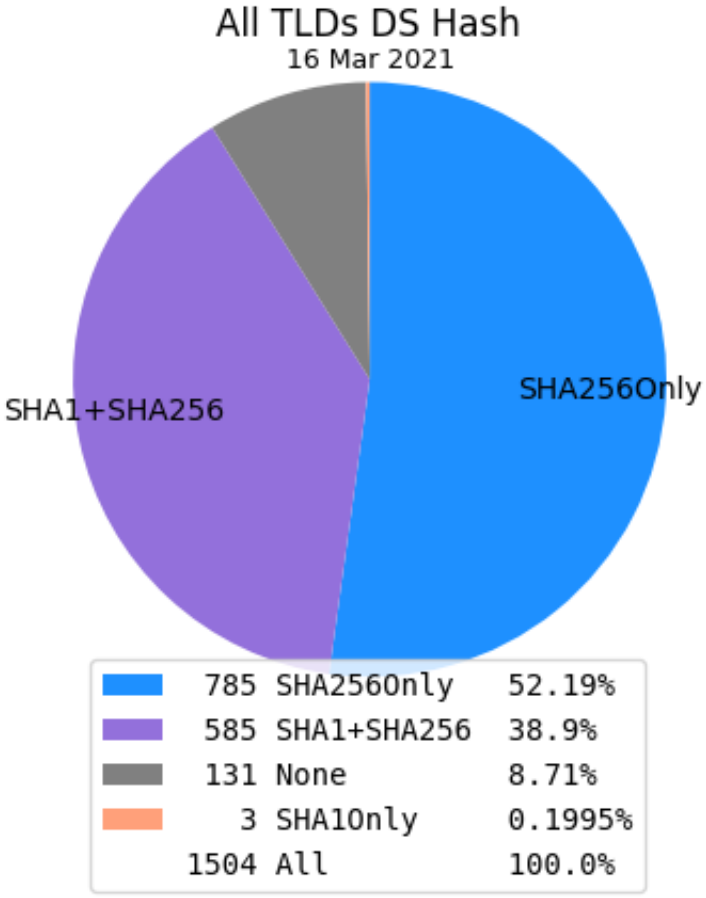


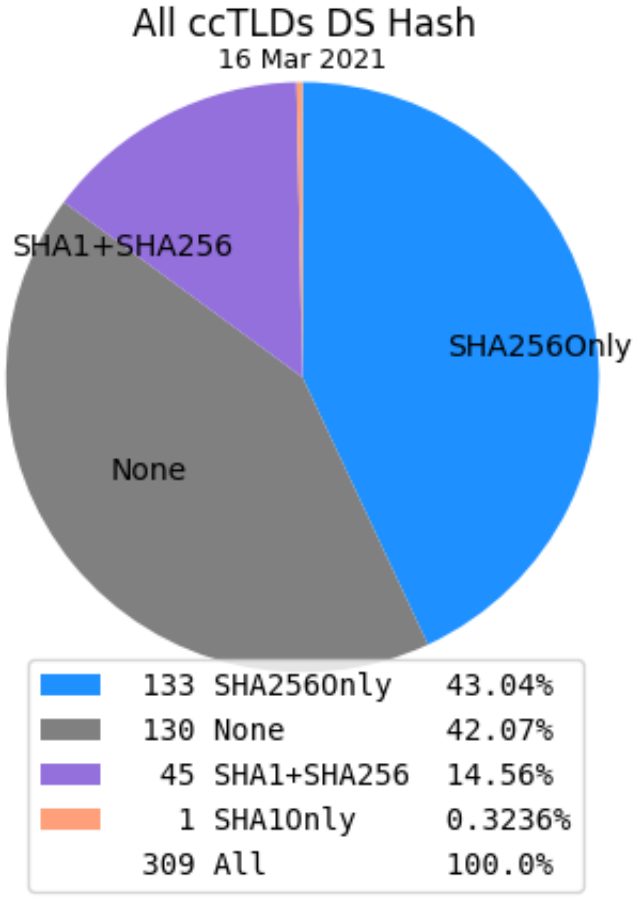
"x" or "y" – operators observed using different values; "x" to "y" means all values inclusive in the bucket

DS Hash Algorithm Choices

- A little more exciting than NSEC/3, but, still, not that interesting
- The DS Hash Algorithm determines the "bits" held in the DS resource record
  - Initially just SHA-1 was defined
  - Later SHA-256 was defined with a recommendation to replace SHA-1
- Some TLDs use both, some just SHA-256
  - But a dwindling few have only SHA-1

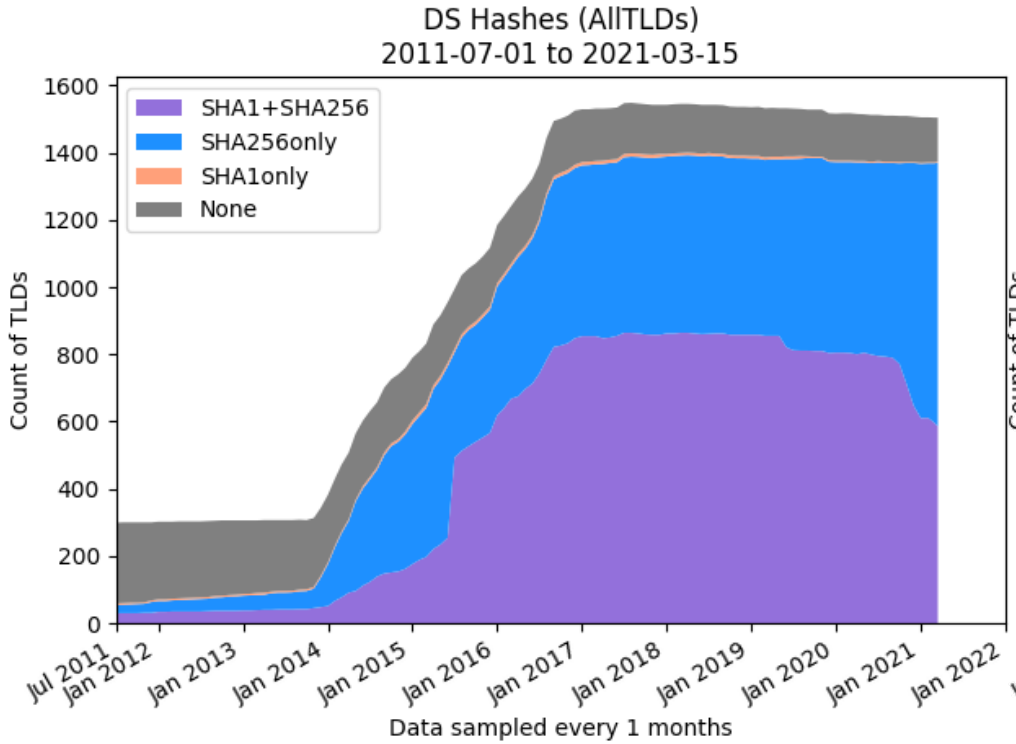
DS Hash Algorithm Choice (ALL and ccTLDs)

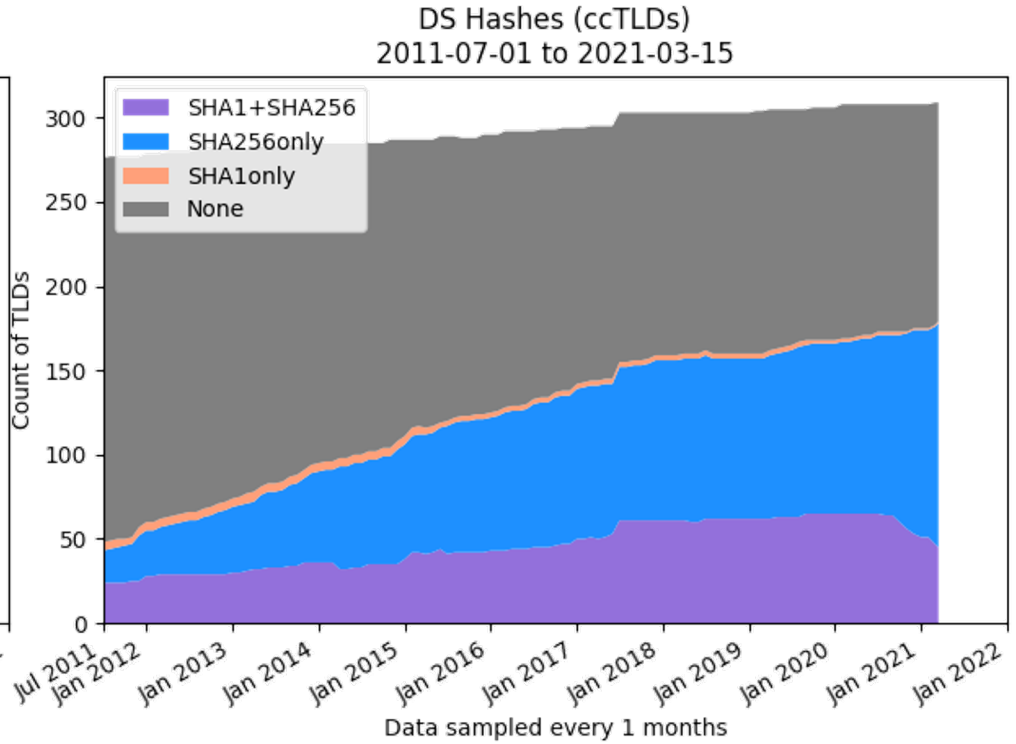




The difference in the *None*'s (131 – 130) is due to the root zone, per protocol, not having a DS record set.

DS Hash Algorithm - Trends





Another case of recent changes in late 2020

Discussion

- Questions?

- Always looking for suggested visualizations
  - What is "interesting" changes over time
    - E.g., dropping "signature durations" in favor of algorithm roll overs
    - NSEC3 iterations are coming under scrutiny

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: edward.lewis@icann.org

@icann

linkedin/company/icann

facebook.com/icannorg

slideshare/icannpresentations

youtube.com/icannnews

soundcloud/icann

flickr.com/icann

instagram.com/icannorg