DNSSEC Deployment among TLDs

"I promise not to make it boring."

Edward Lewis

ICANN69 vTechDay
19 October 2020

Agenda

- Context: Changes to the Root Zone in the 2010's
- DNSSEC Deployment by "levels"
- Cryptographic Choices
- Negative Answers
- DS Hashes
- Key Lifecycles, Rollovers and Algorithm Rollovers

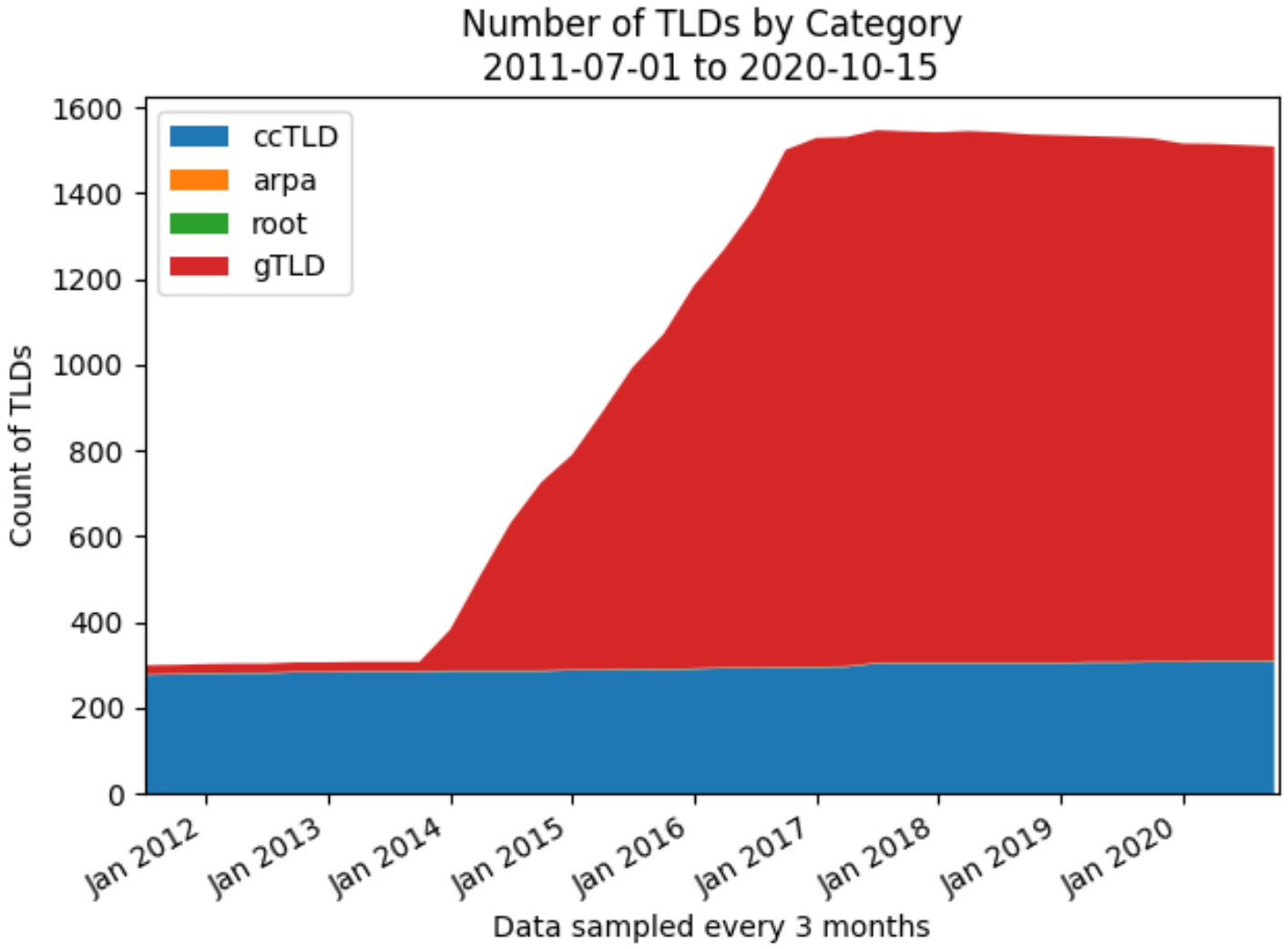
A decade of Root Zone changes

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

All gTLDs after 2012 must have full DNSSEC, skewing adoption curves

For "history", much of the focus will be on ccTLDs

(No reverse map zones)

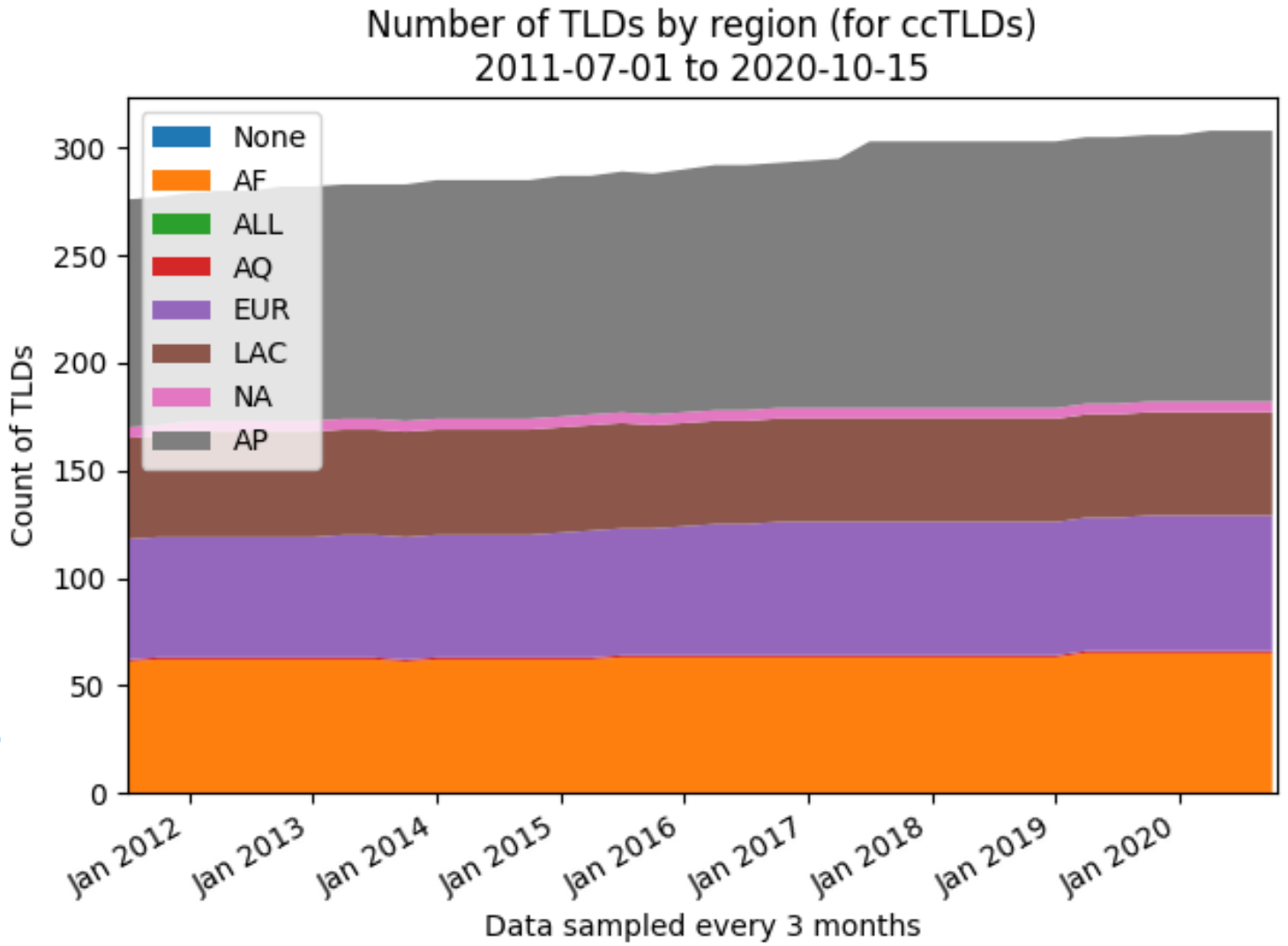


ccTLDs divided by regions

gTLDs are generally global, despite some named for locations

ccTLDs have an inherent location and thus a region

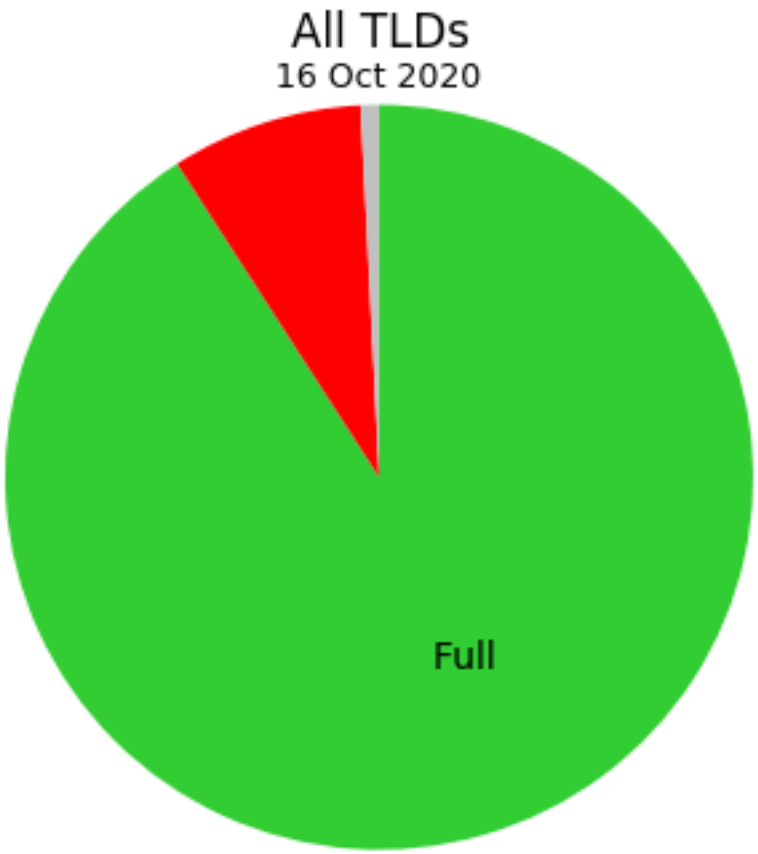
"Regions" taken from https://meetings.icann.org/en/regions



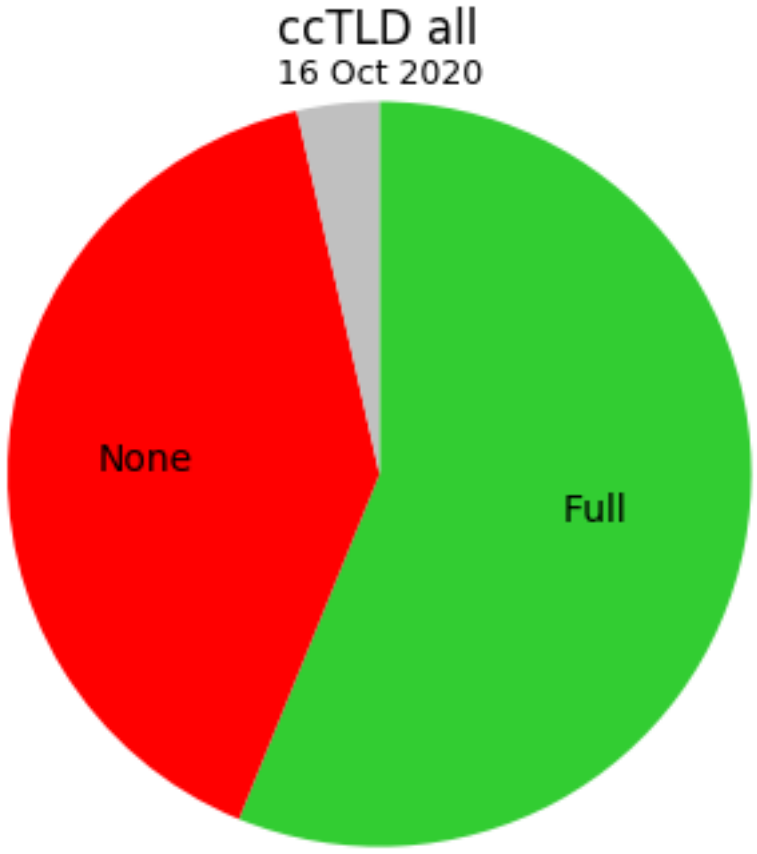
DNSSEC Deployment in TLDs

- In the following charts
  - "Full" – TLD is signed and has a DS record
  - "Signatures" – TLD publishes a signed zone ("Almost")
  - "None" – No DNSSEC deployment
- Not measured – delegations' (below, inside ccTLDs) DNSSEC

DNSSEC Deployment Level - All TLDs vs. ccTLDs

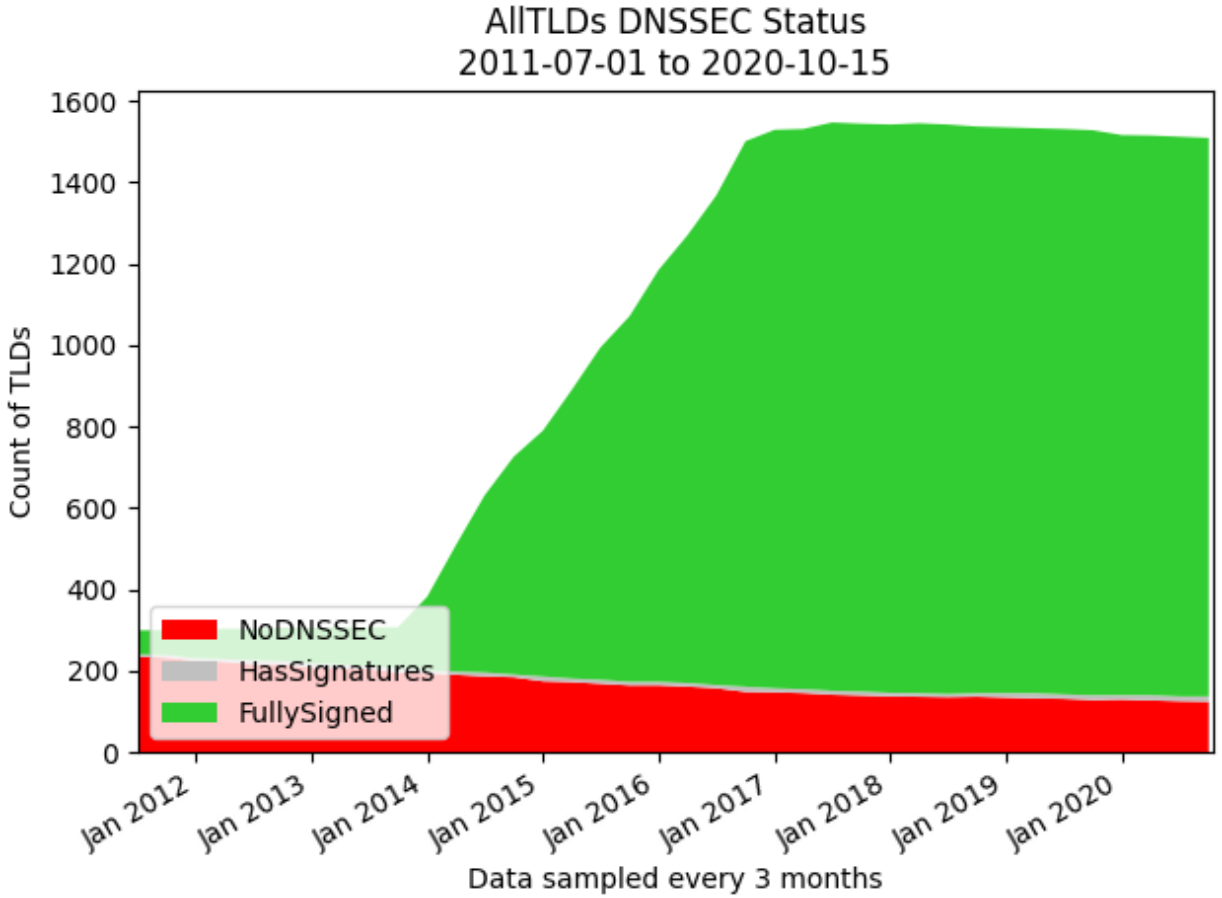


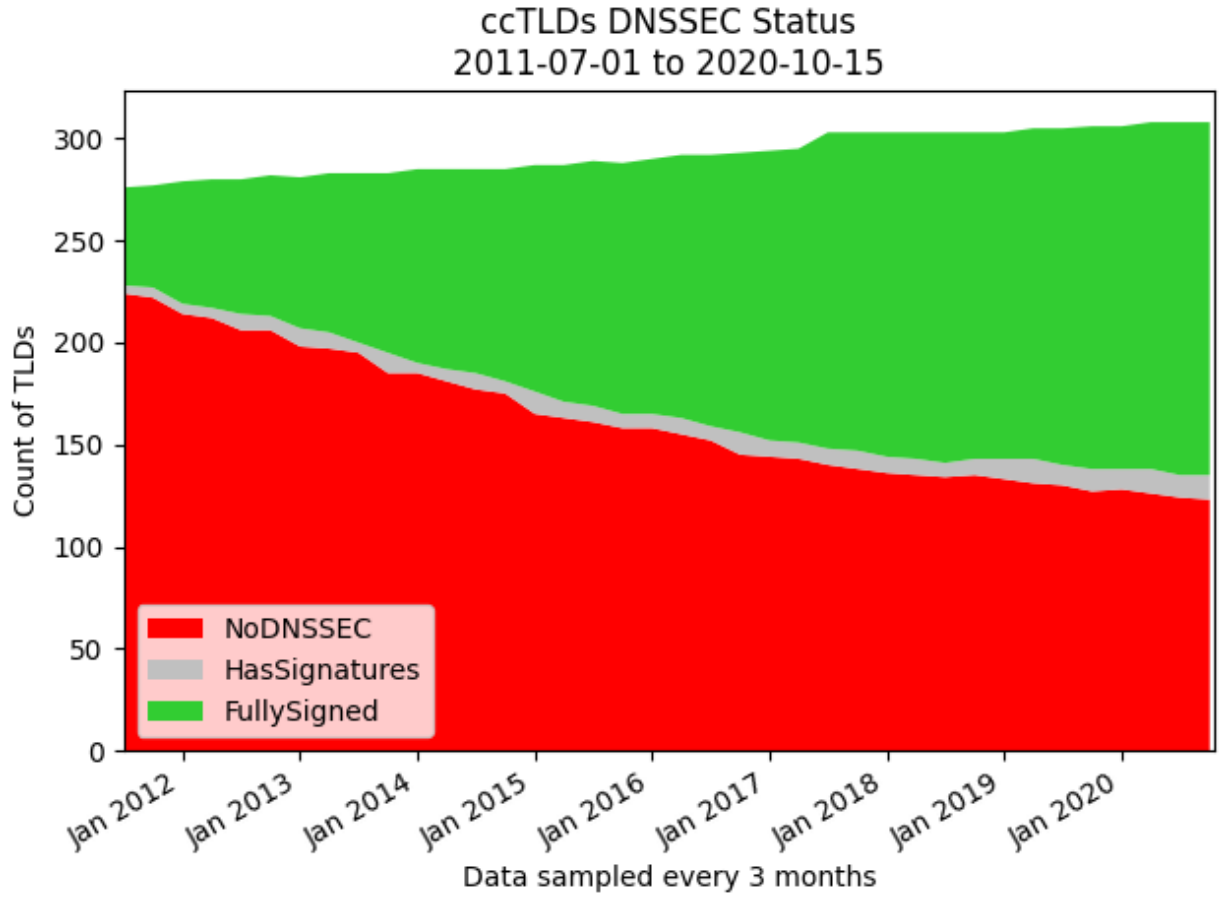
1371	Full	90.92%
125	None	8.289%
12	Signatures	0.7958%
1508	All	100.0%



173	Full	56.17%
124	None	40.26%
11	Signatures	3.571%
308	All	100.0%

DNSSEC Deployment Level All TLDs vs. ccTLDs - Trends

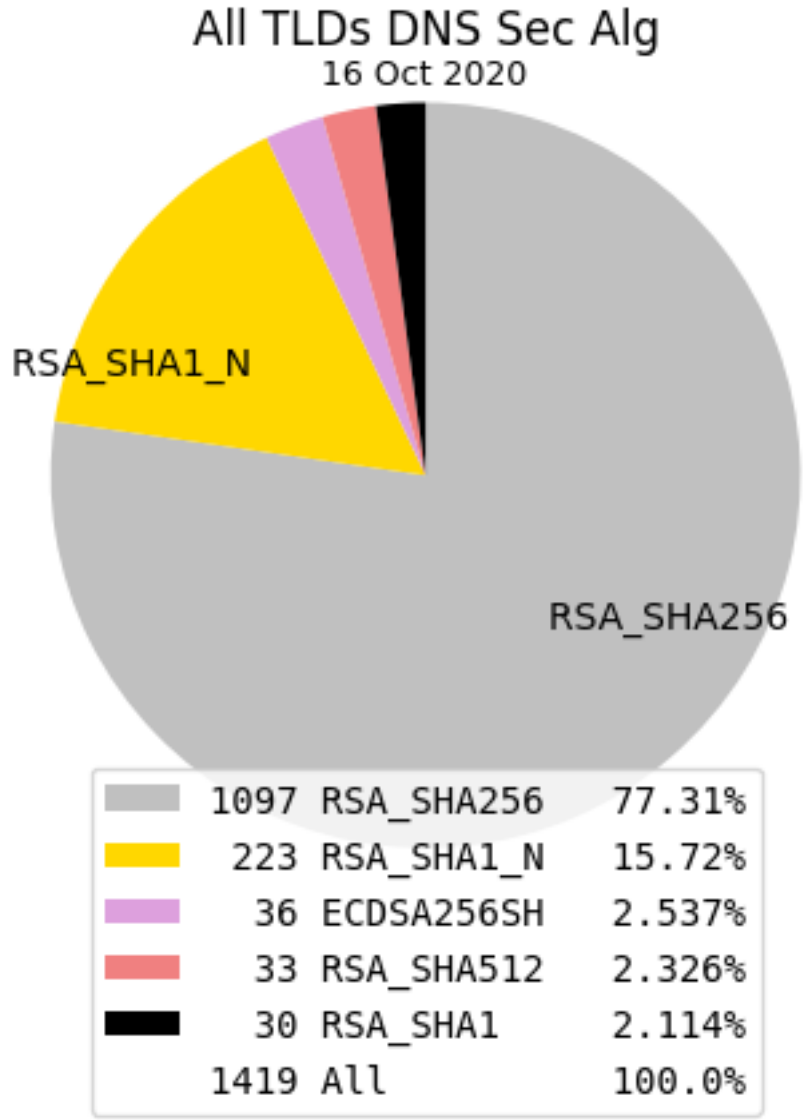


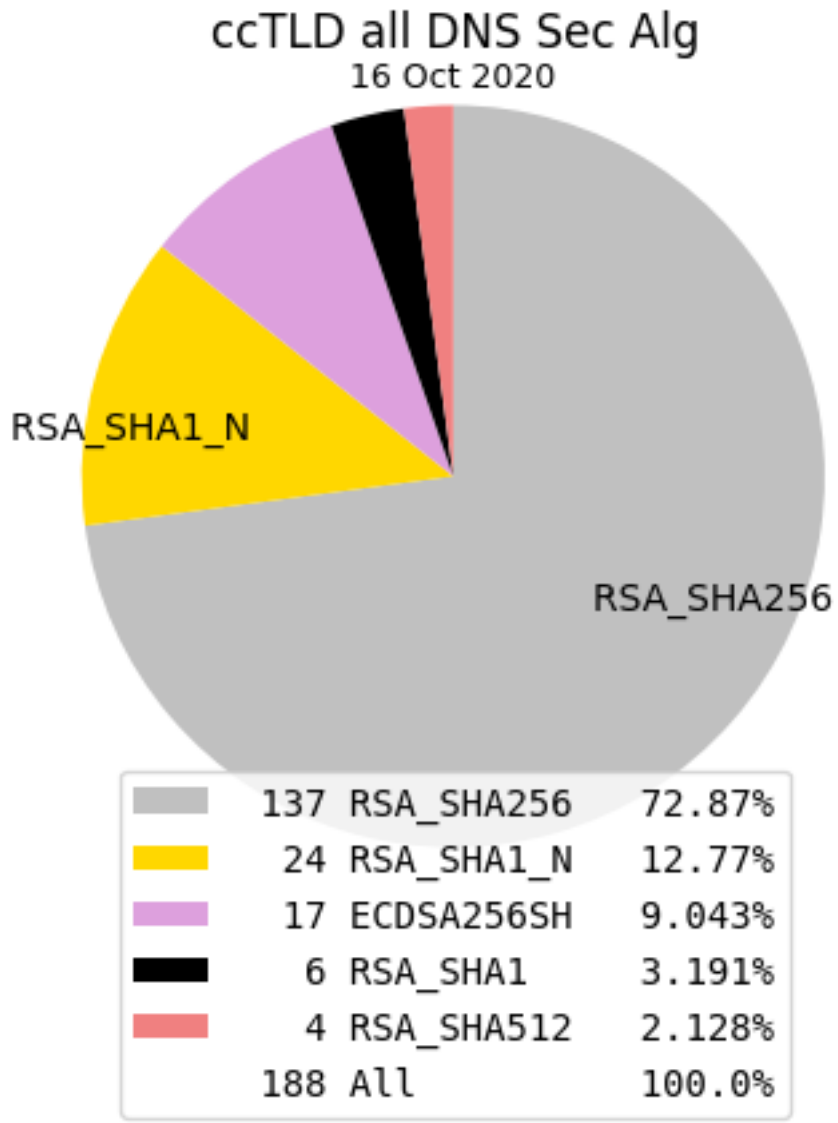


Cryptographic Choices

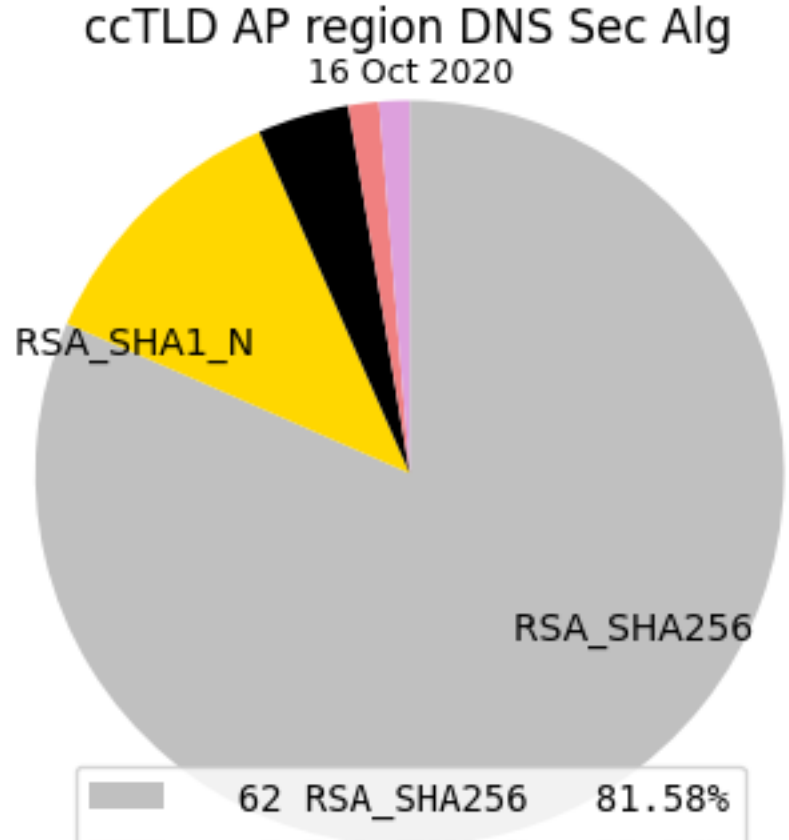
- DNSSEC Security Algorithm
  - Cryptography (DSA, RSA, Elliptic Curve, etc.)
  - Hash algorithm (SHA-1, SHA-256, etc.)
- The "best-est" algorithm changes over time
- A TLD may have more than one algorithm at one time

Cryptography Choices (All/ccTLD)

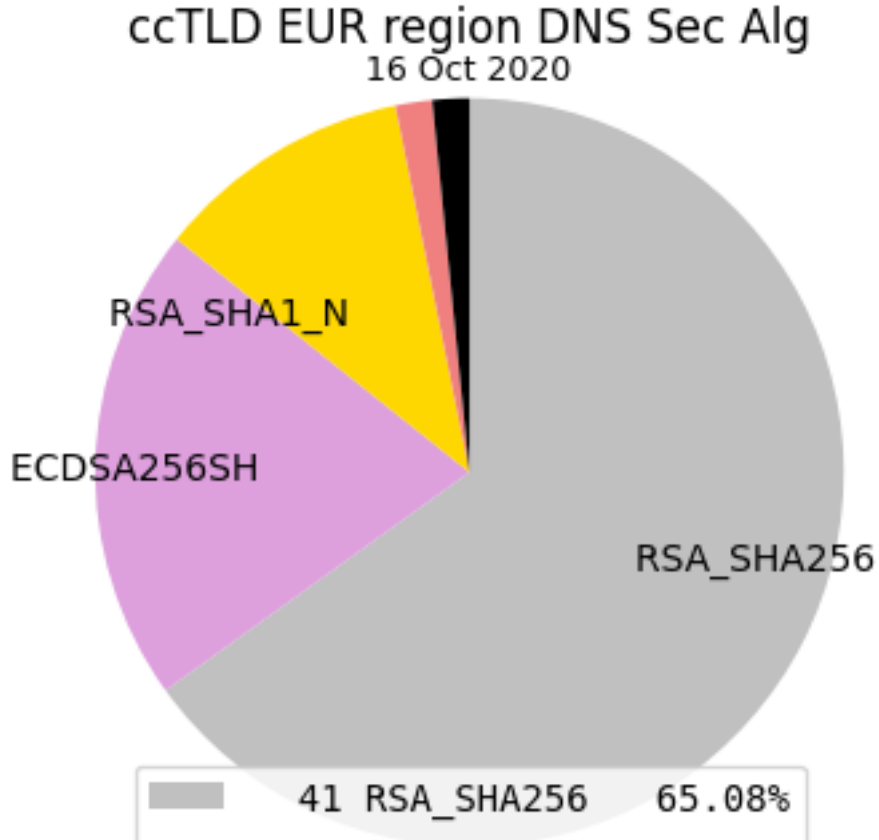




Cryptography Asia Pacific vs. Europe (ECDSA difference)

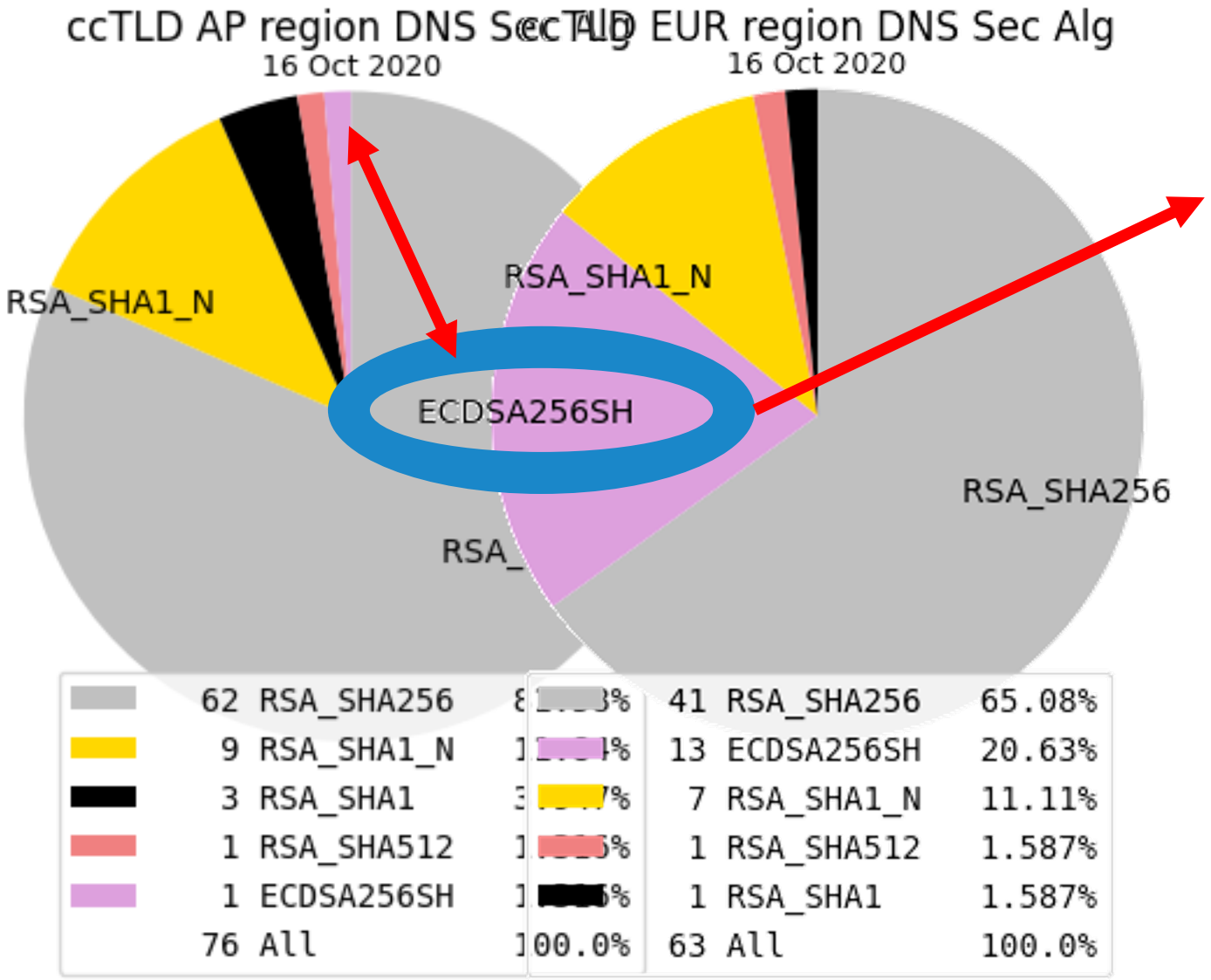


	62	RSA_SHA256	81.58%
	9	RSA_SHA1_N	11.84%
	3	RSA_SHA1	3.947%
	1	RSA_SHA512	1.316%
	1	ECDSA256SH	1.316%
	76	All	100.0%



	41	RSA_SHA256	65.08%
	13	ECDSA256SH	20.63%
	7	RSA_SHA1_N	11.11%
	1	RSA_SHA512	1.587%
	1	RSA_SHA1	1.587%
	63	All	100.0%

The ECDSA difference



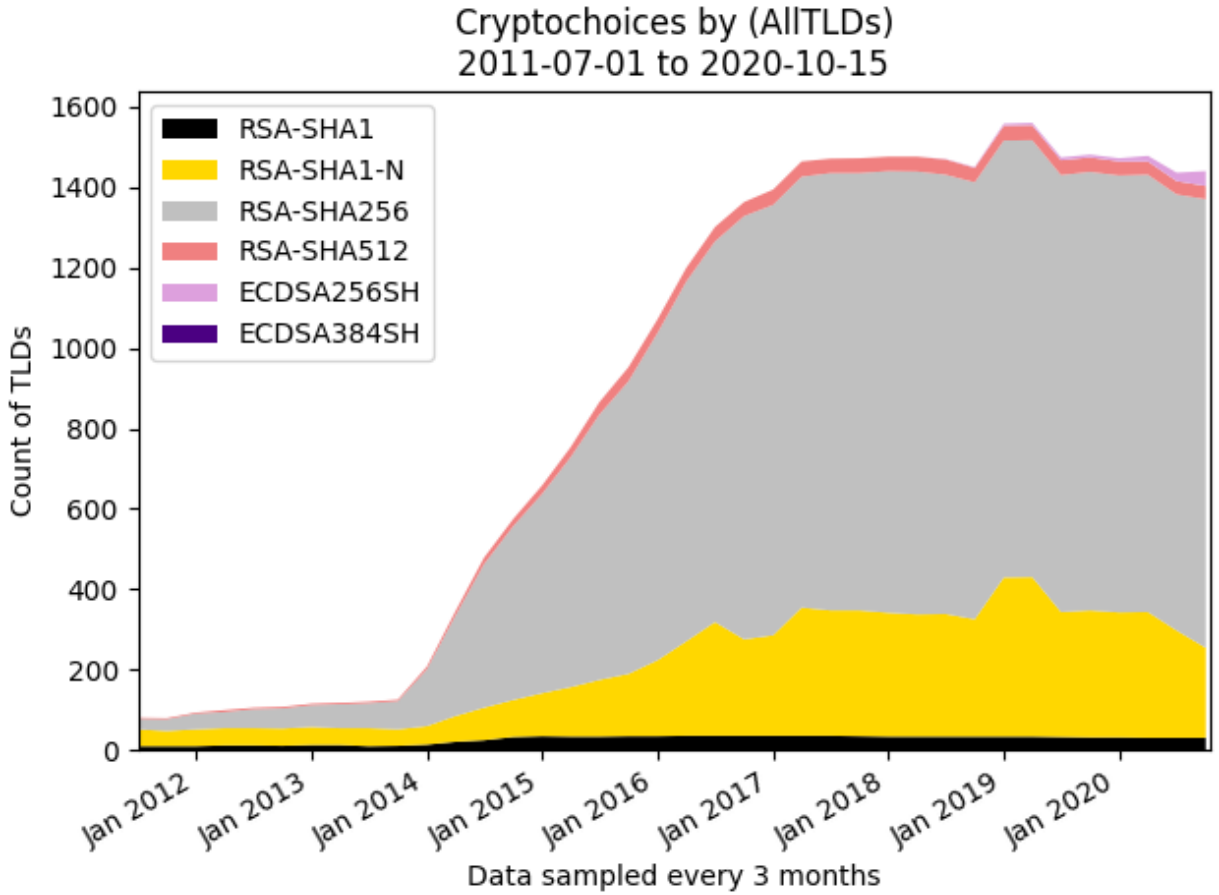
Note the difference in ECDSA256

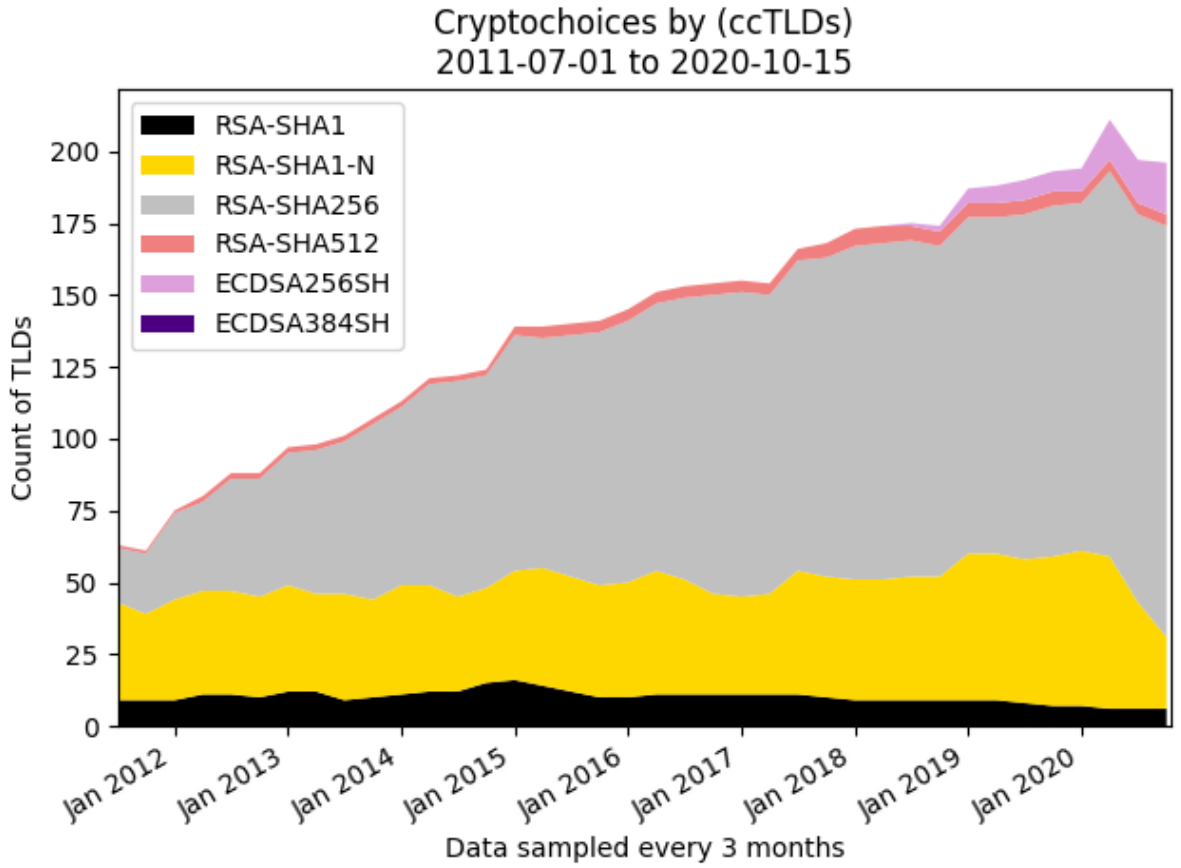
5th place in Asia Pacific
2nd place in Europe

ECDSA is a space-saving algorithm, but it is new
- "better" but "perhaps not widely deployed"

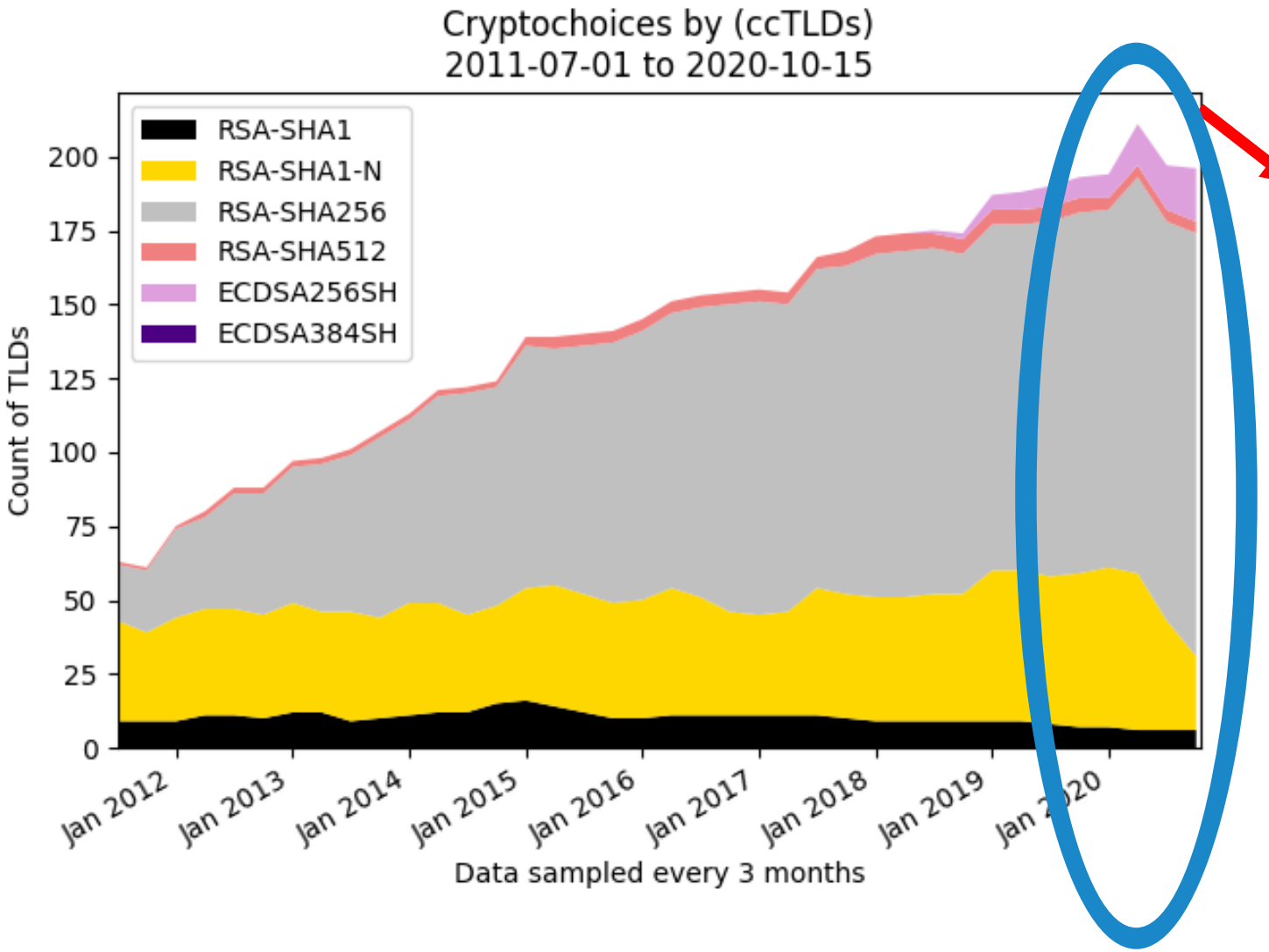
This is the single most visible regional difference

Cryptography (All/ccTLD) – Trends using counts





Cryptography – that ccTLD 2020 "peak"



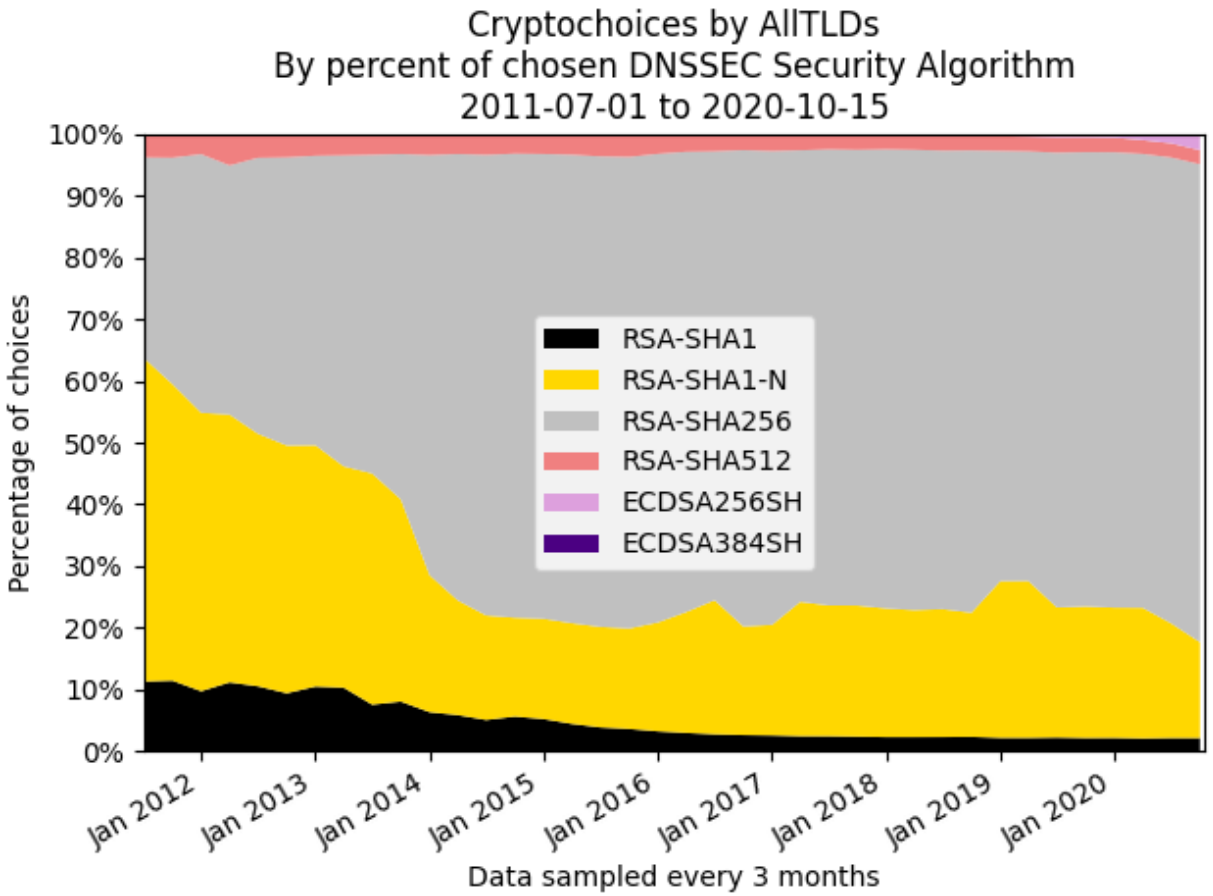
Hypothesis:

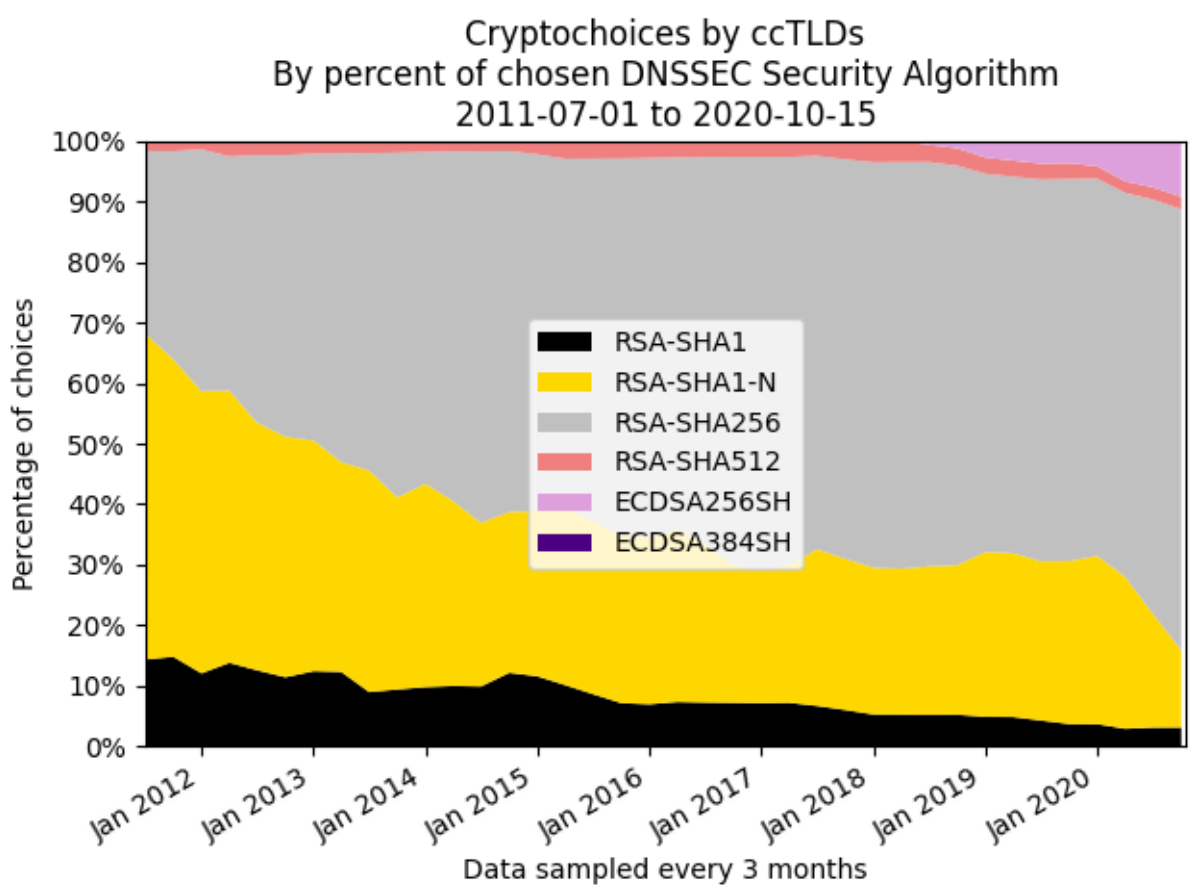
The "peak" is the introduction of the ECDSA algorithm (keys, signatures) in parallel with what it replaces

The "fall" is the removal of the RSA-SHA1 "for NSEC3" algorithm (keys and signatures)

A sign of algorithm key rollover

Cryptography (All/ccTLD) – Trends using Percent

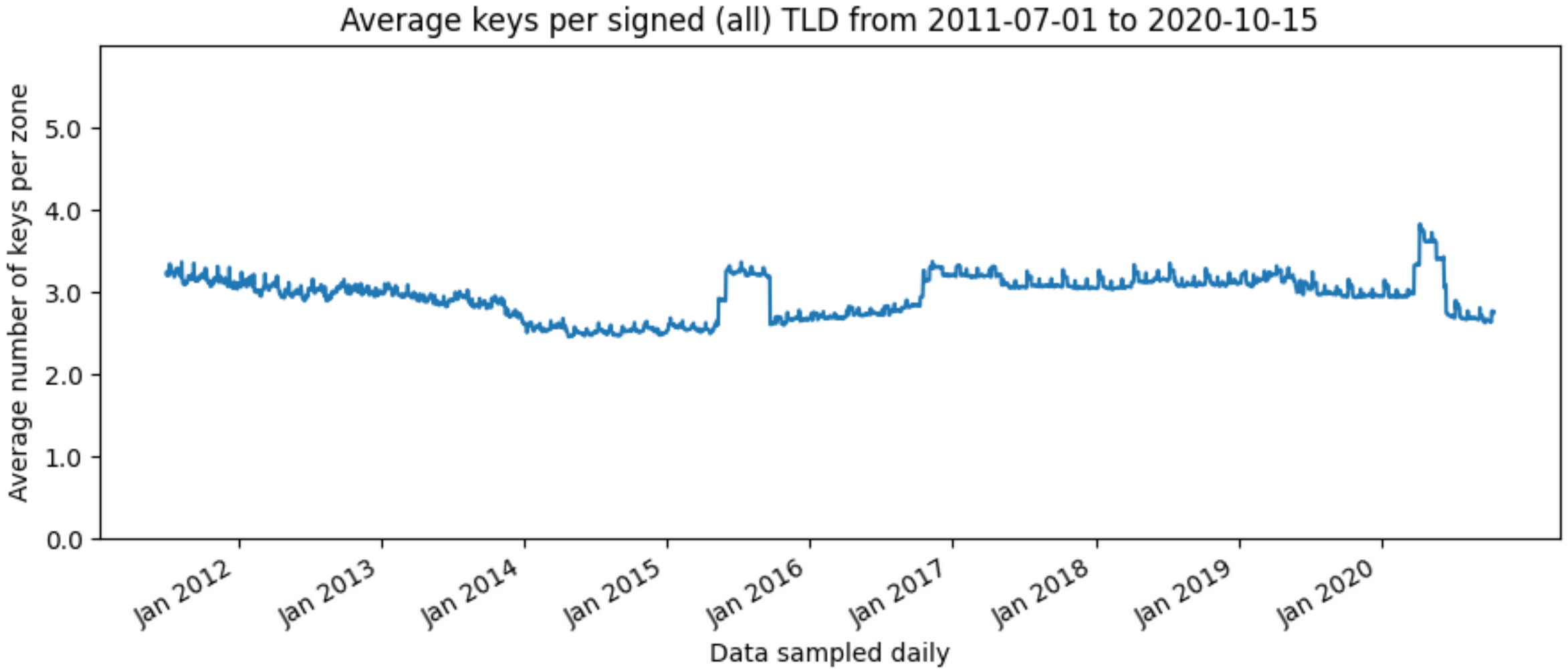




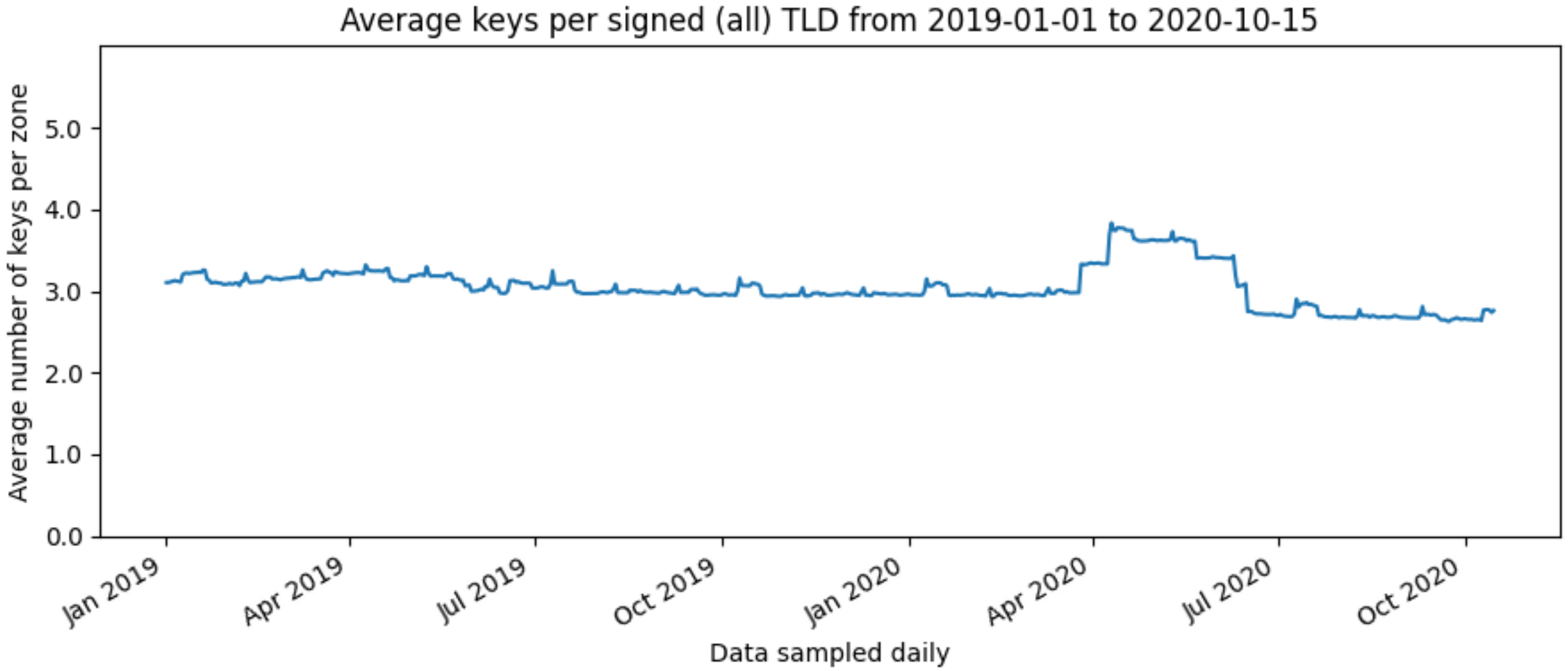
Number of Keys

- 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, learned about issue
- Number of keys is not a primary measure
  - But charting it reveals patterns of operations (rolls)

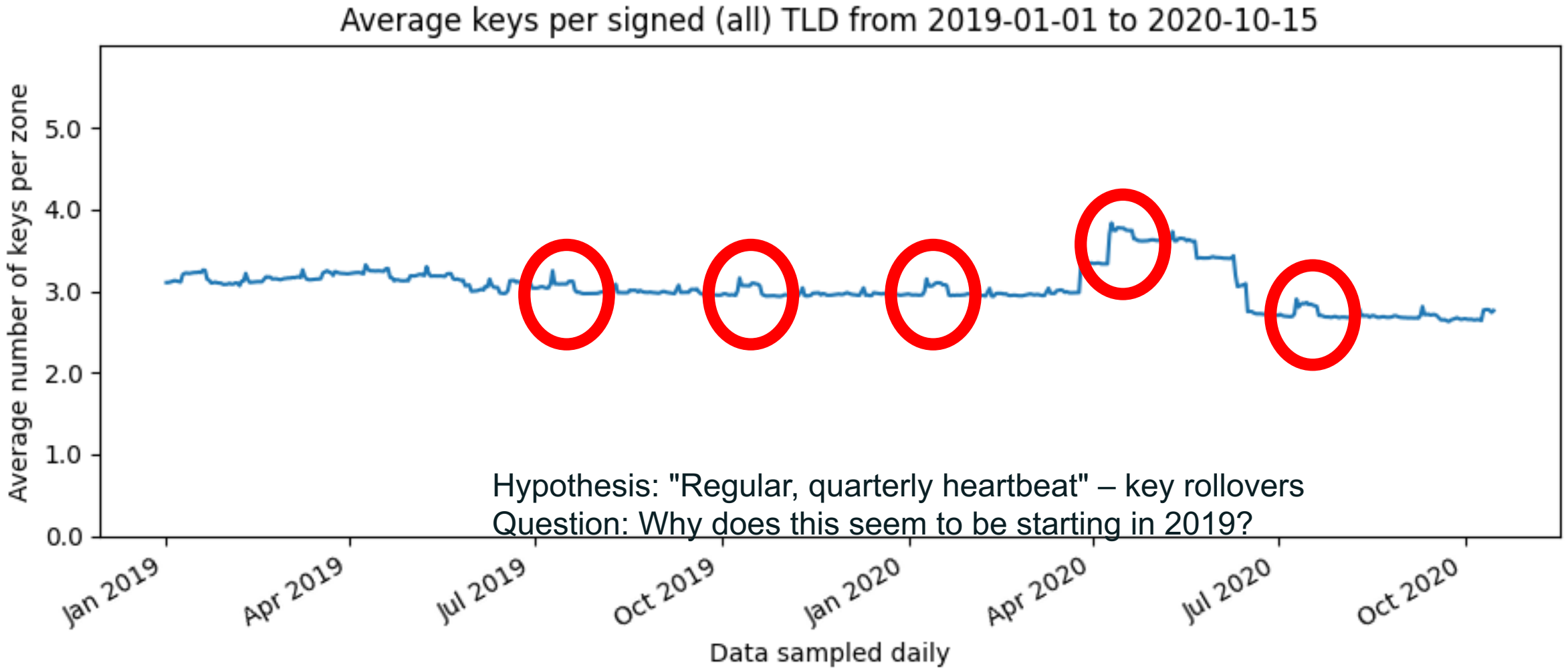
Average Number of Keys (All)



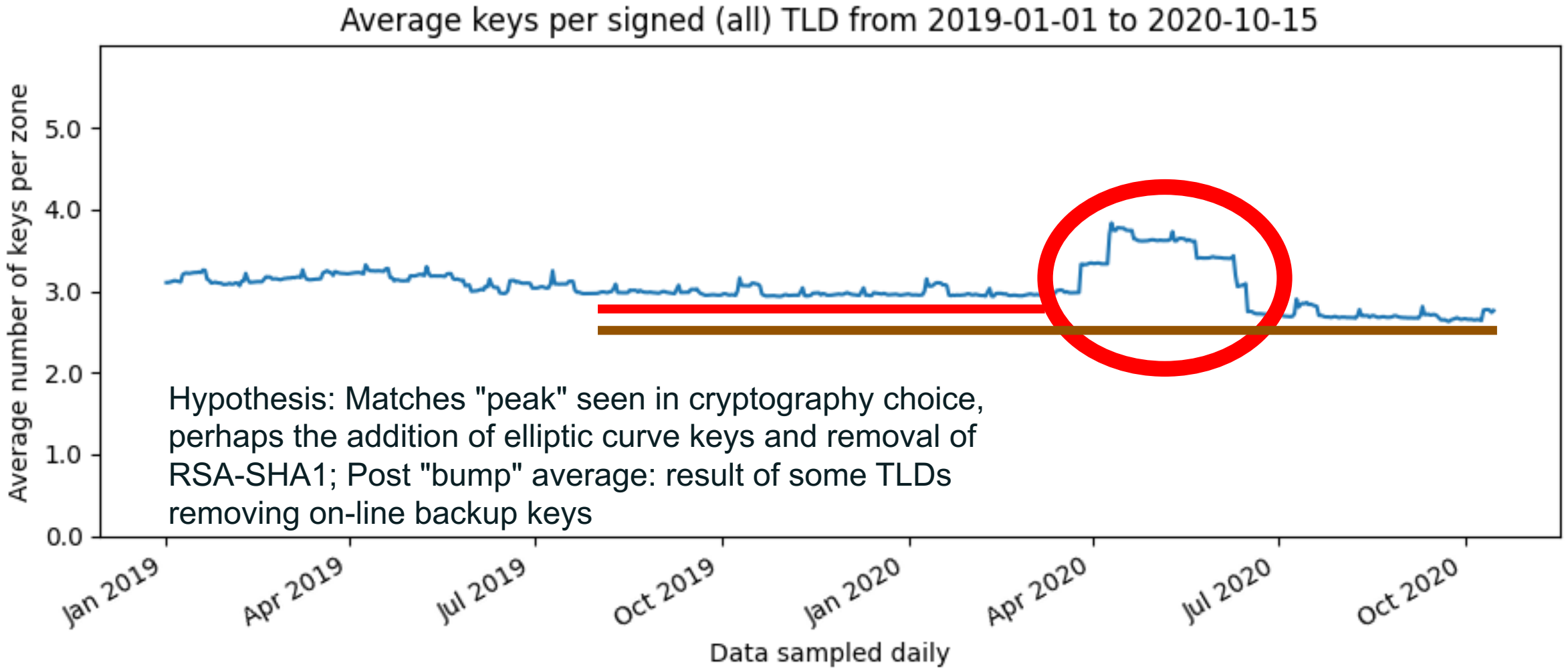
Average Number of Keys (All TLDs, 2019 and 2020 only)



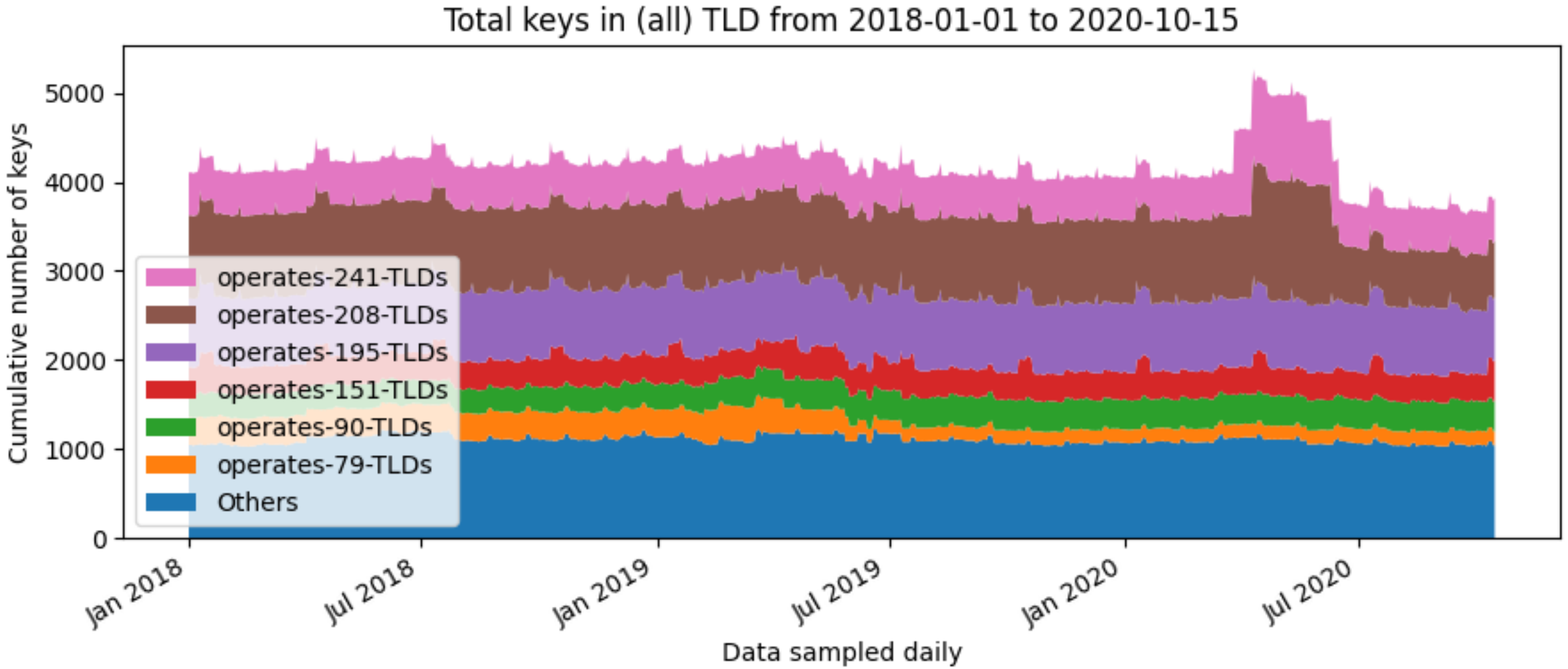
Average Number of Keys (All, last two years) – Highlights I



Average Number of Keys (All, last two years) – Highlights 2



Who's behind the bumps? Colors indicate back-end operators

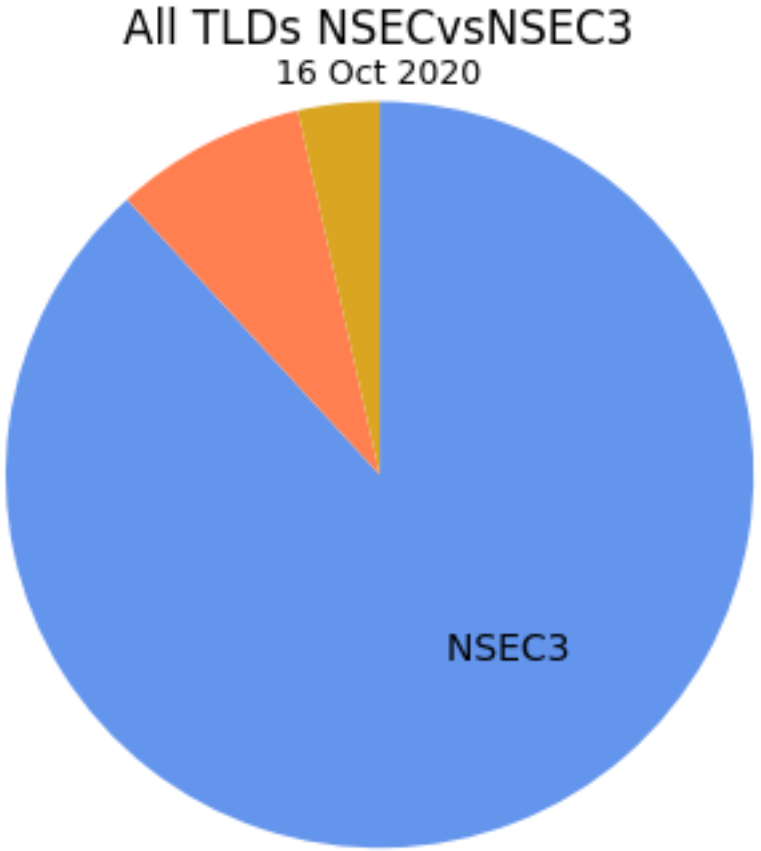


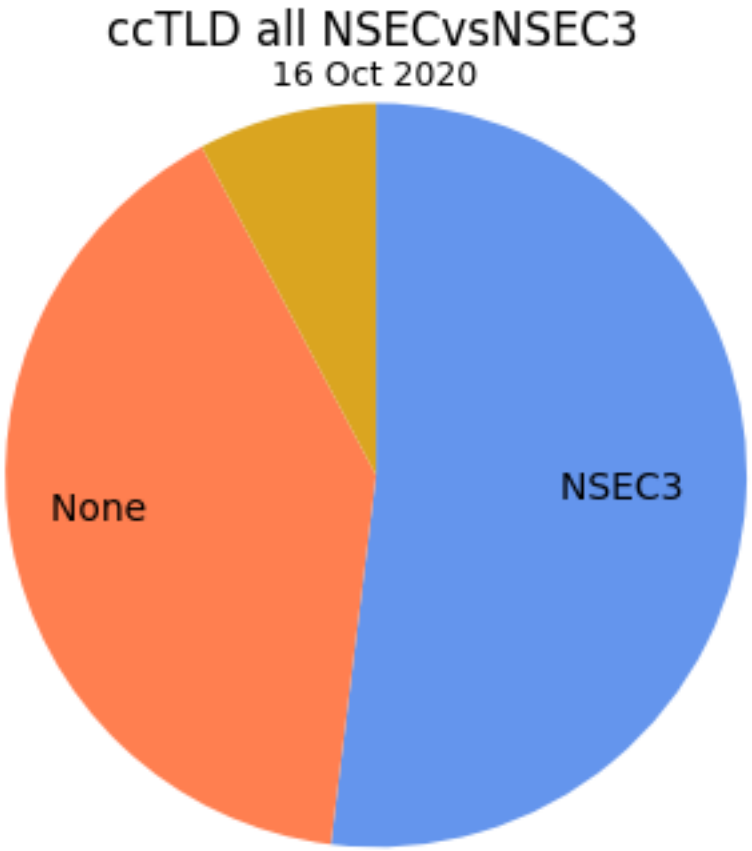
Back-end operators ("DNS House") – identified by a zone's SOA RR RNAME and IANA Technical Contact

Negative Answer Choices

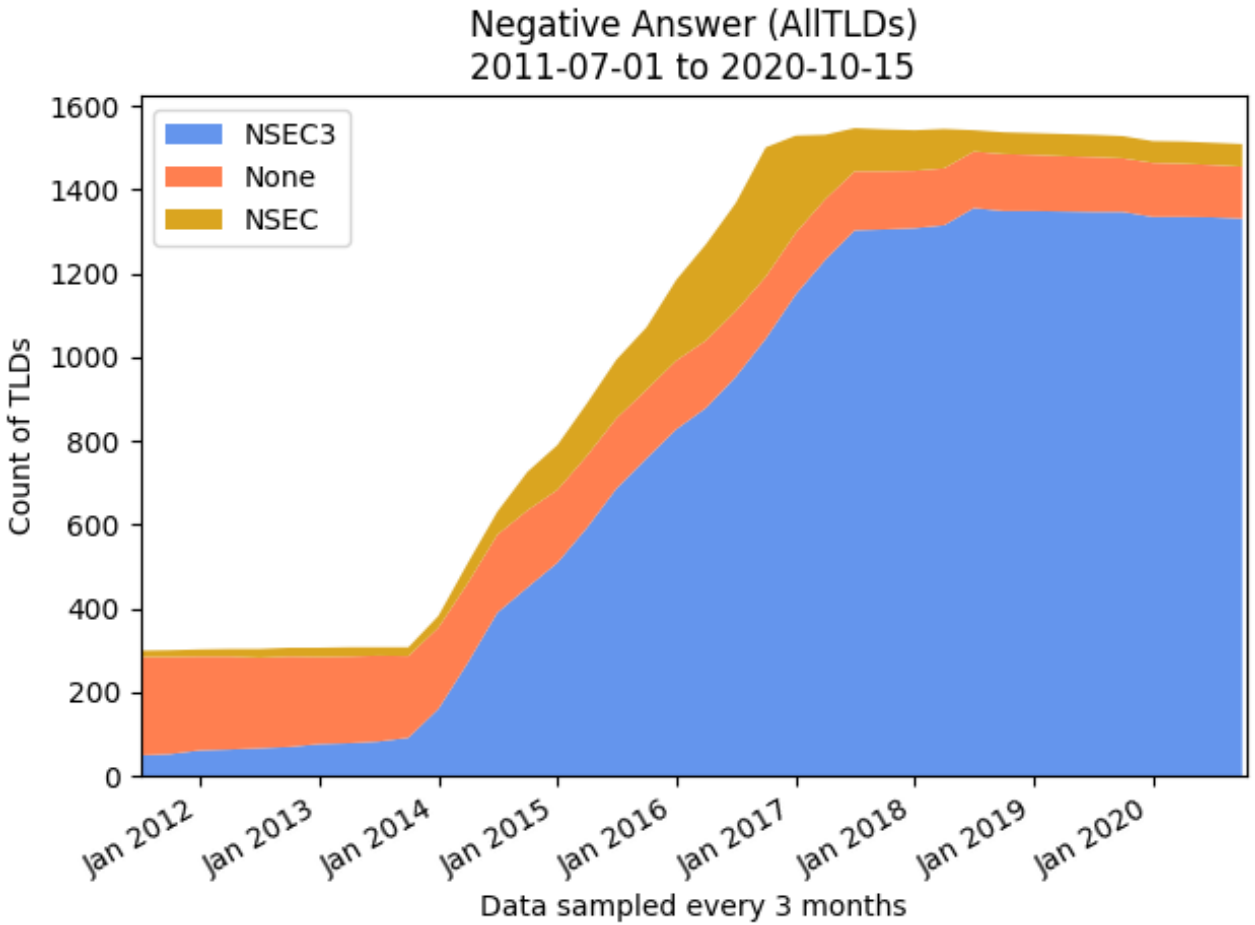
- This isn't an exciting topic
  - So I'll knock it off the list here (before anyone else falls asleep)
  - NSEC vs. NSEC3
    - Consistently dominated by NSEC3 for TLDs
  - "Both" means a TLD switched during a day of observations

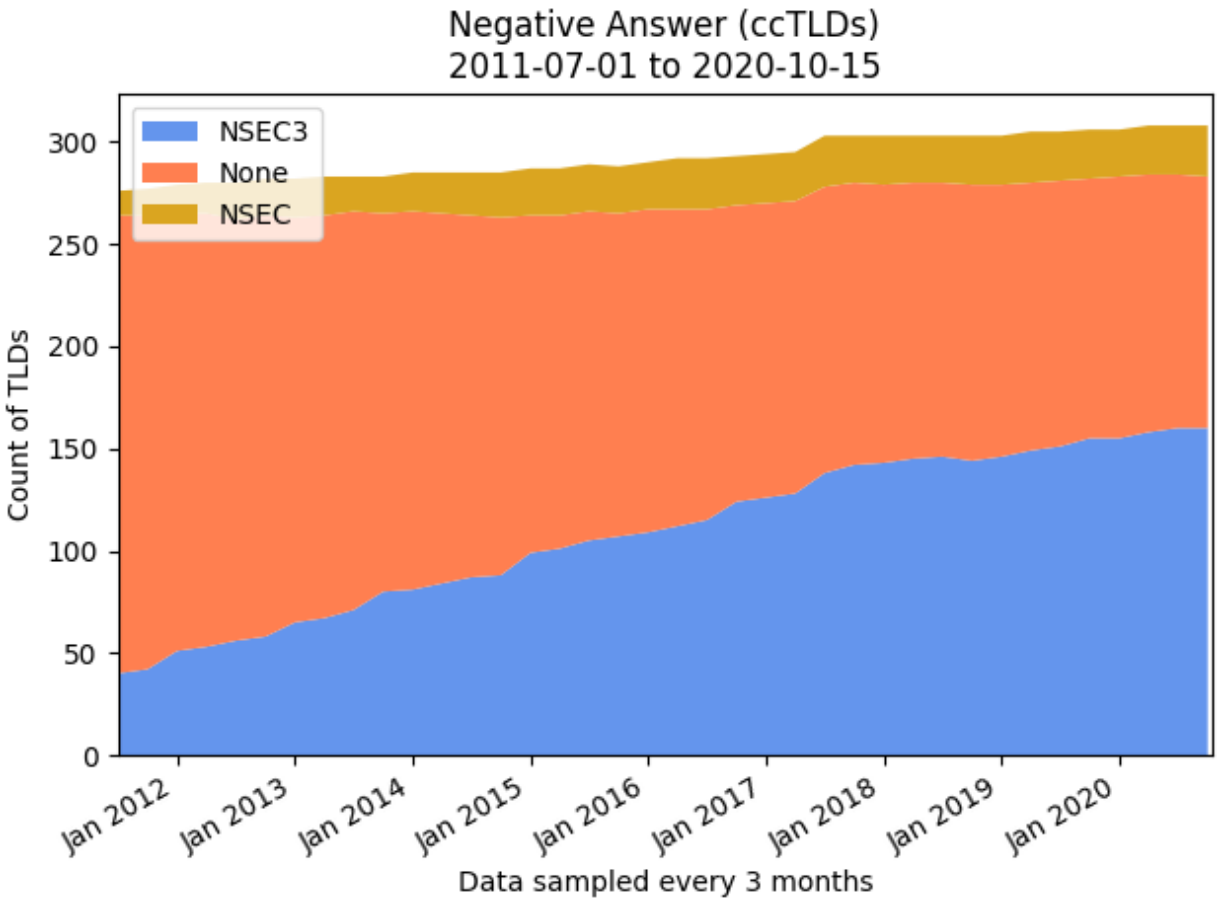
Negative Answer Choices (All and ccTLDs)





Negative Answer Choices (All and ccTLDs) - Trends

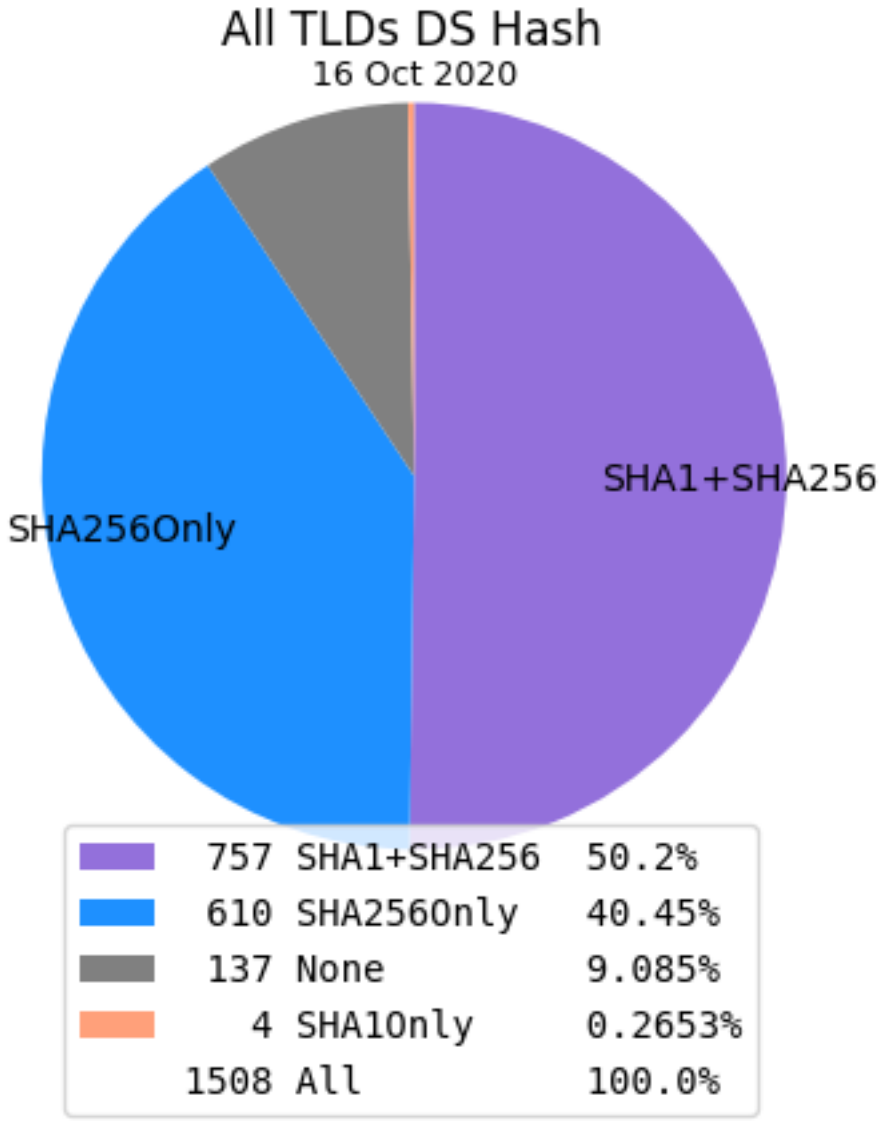


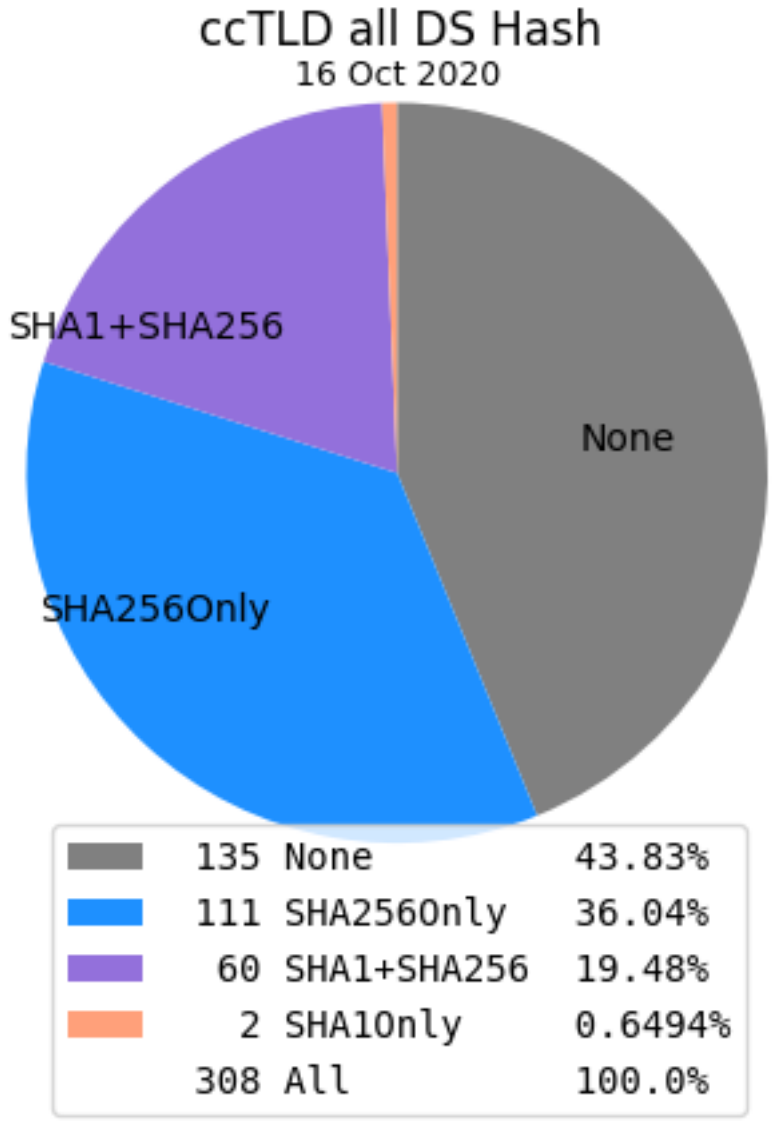


DS Hash Algorithm Choices

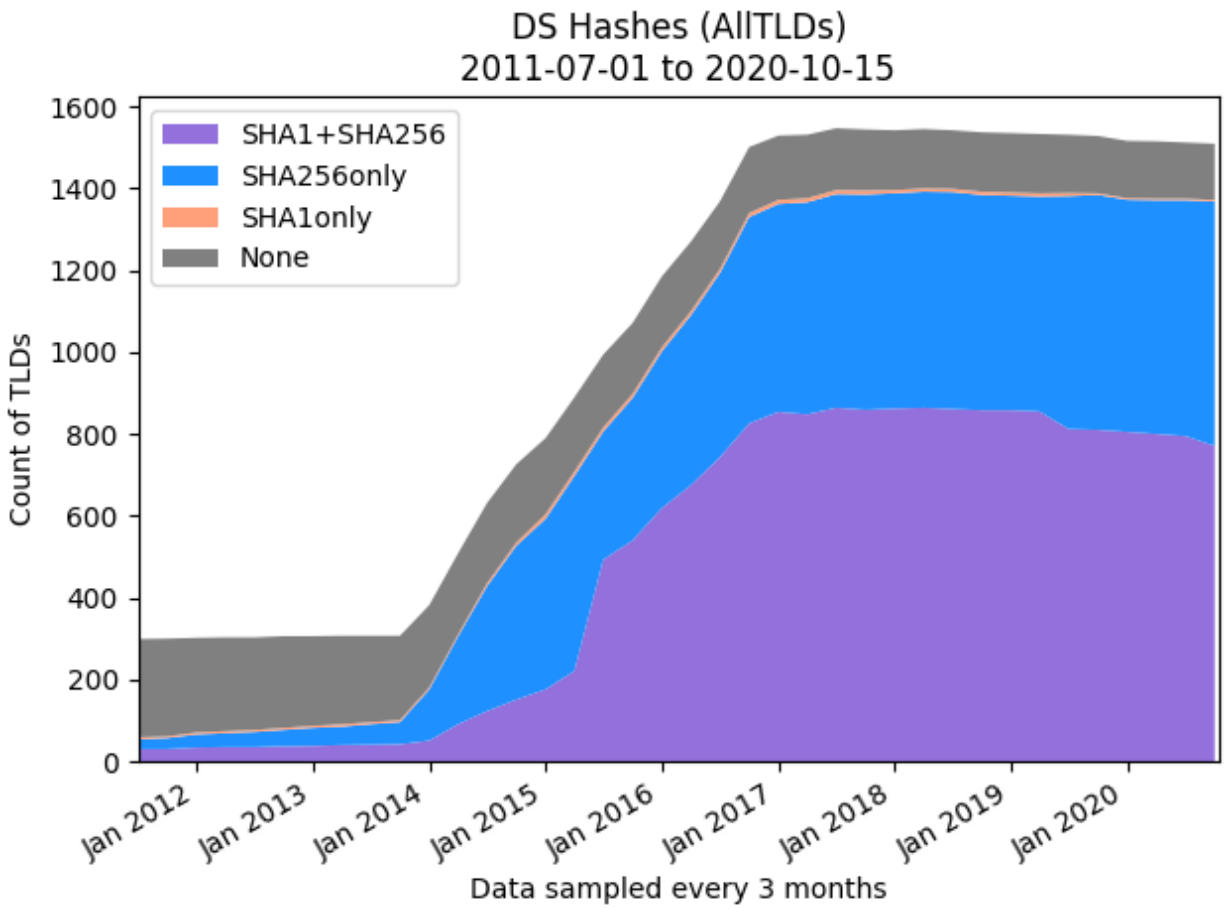
- A little more exciting than NSEC/3, but, still, not that interesting
- The DS Hash Algorithm determines the "bits" held in the DS resource record
  - Initially just SHA-1 was defined
  - Later SHA-256 was defined with a recommendation to replace SHA-1
- Some TLDs use both, some just SHA-256
  - But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

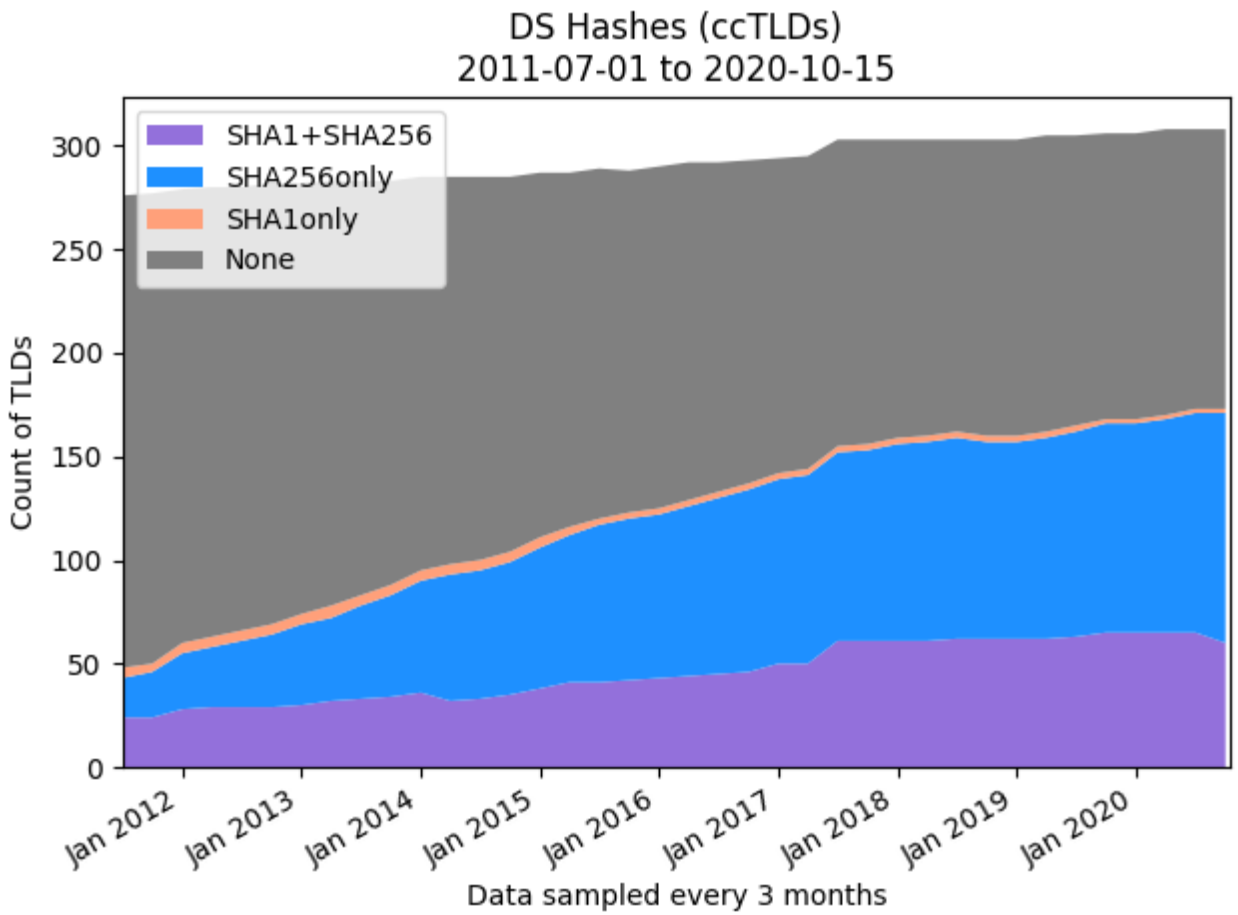
DS Hash Algorithm Choice (ALL and ccTLDs)





DS Hash Algorithm - Trends





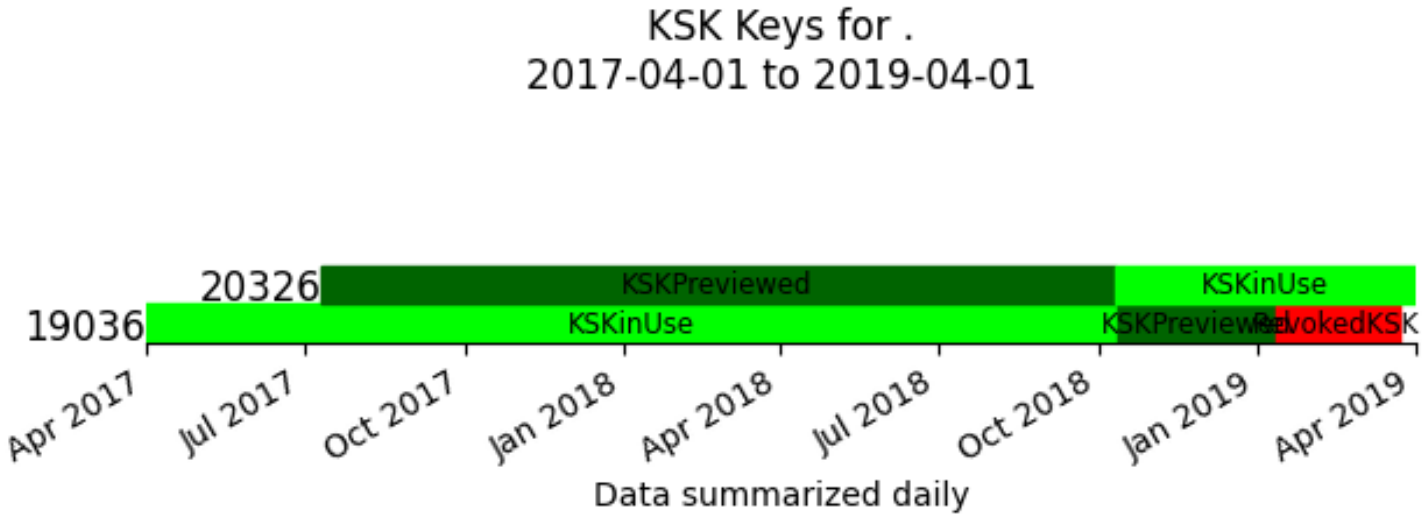
Key Lifecycles

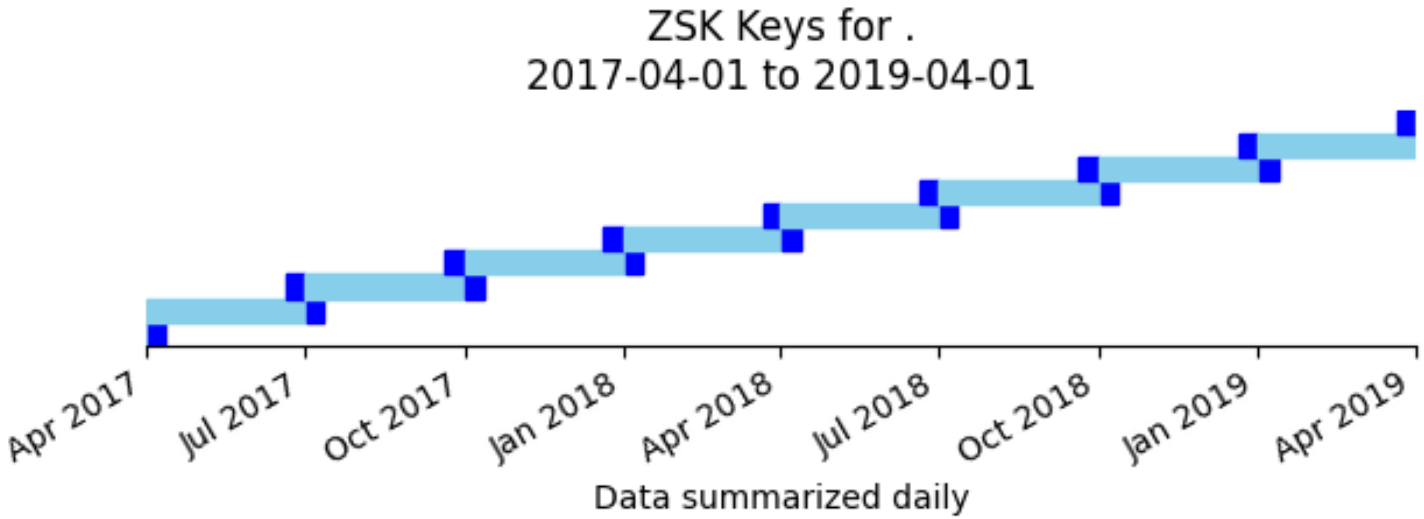
- The following charts are visualizations of changes to keys in various TLDs over time
- In most cases, the names of the TLD are masked
  - "To protect the innocent"
- Some charts reveal the state of the key (pre-published, active, revoked)
- Other charts reveal the DNSSEC Sec Alg (to see key rollovers)

Key Lifecycles

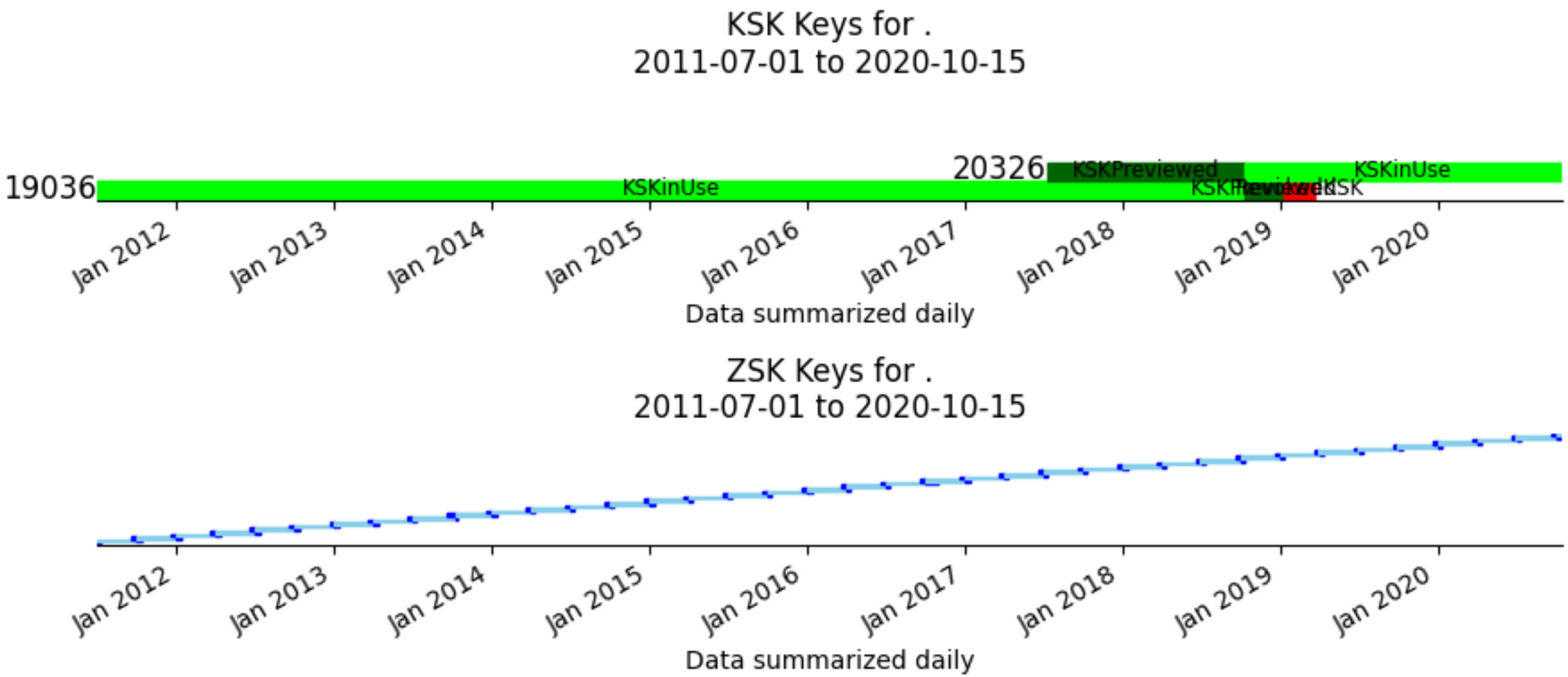
This chart the root zone's 2018 KSK rollover

-Dark colors: pre-publication
-Red: revocation
-Light colors: normal operations

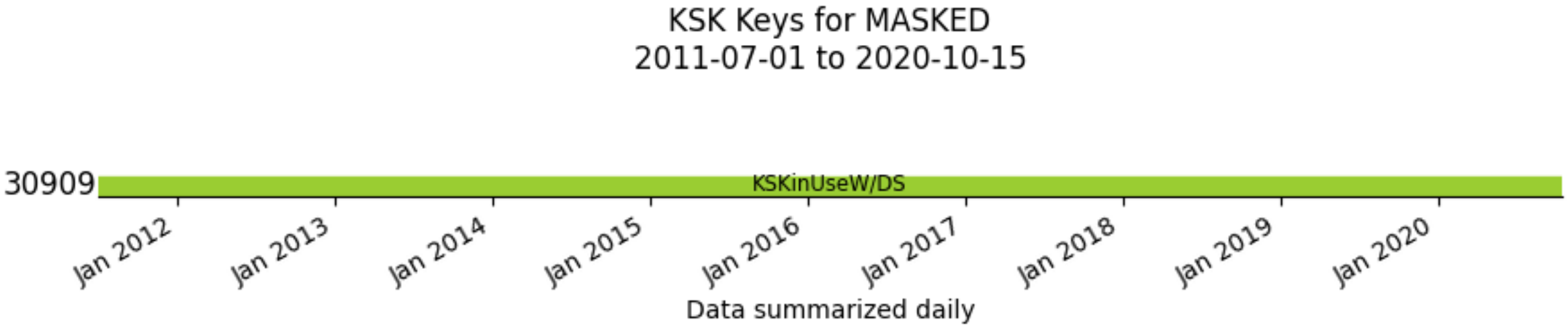


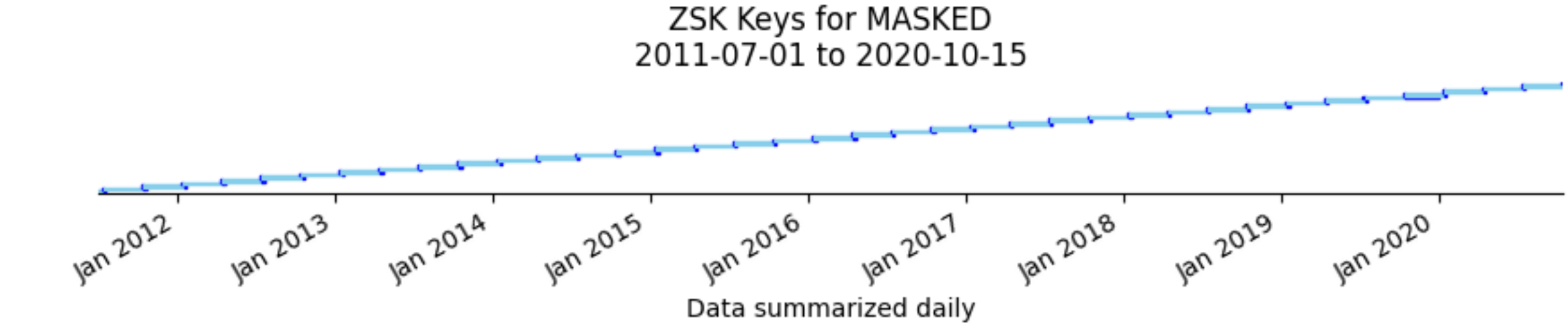


Key Lifecycles – The root zone since 2011

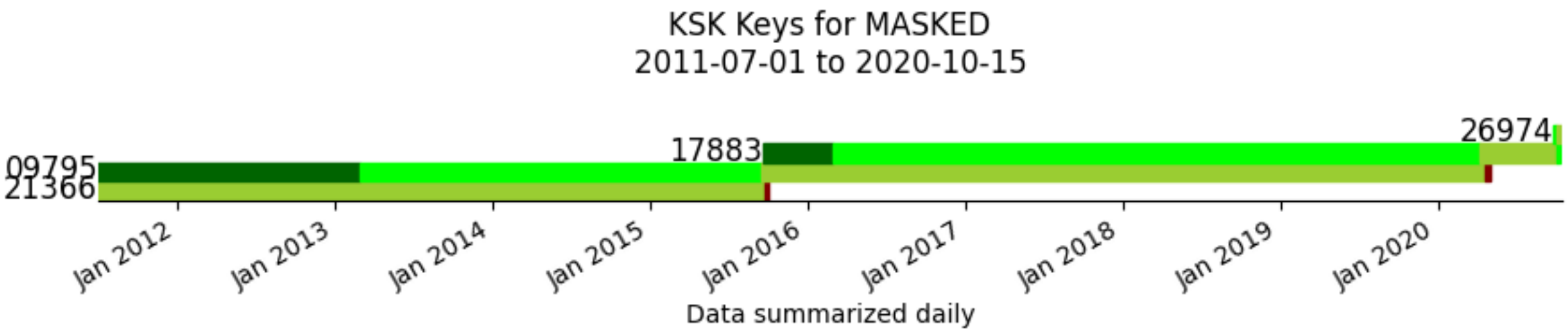


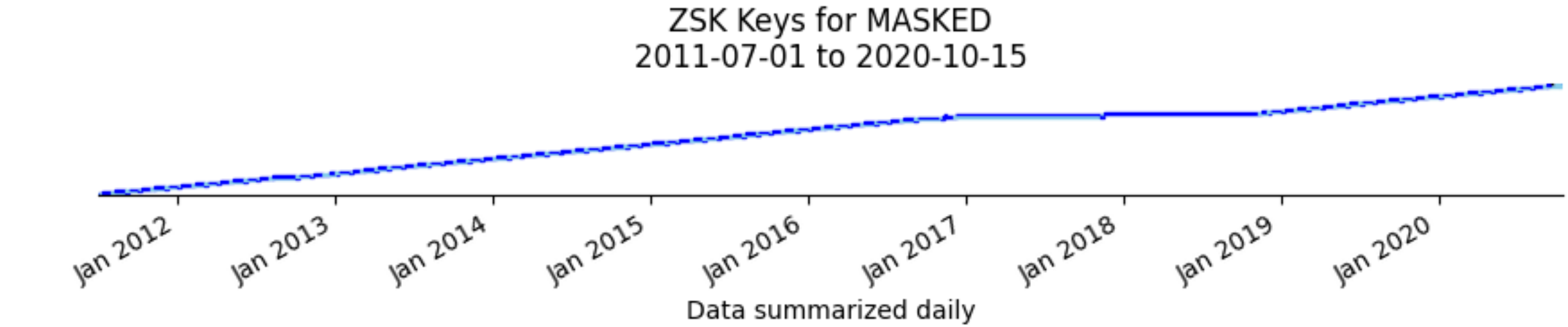
Key Lifecycles – a pre-2012 gTLD



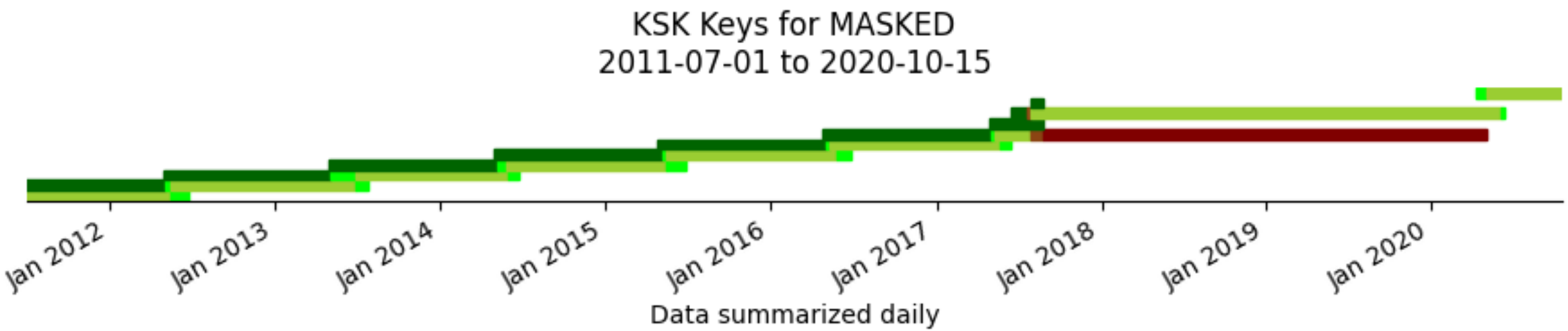


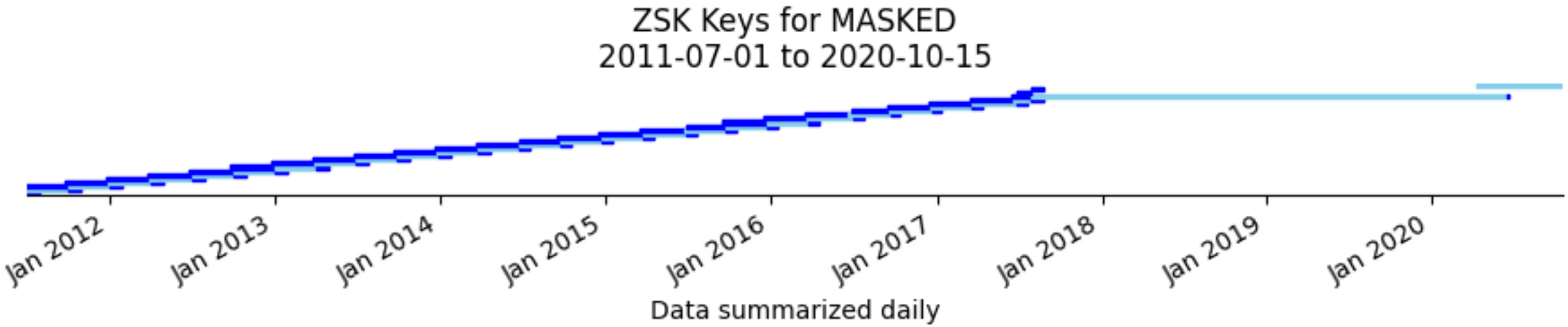
Key Lifecycles – another pre-2012 gTLD



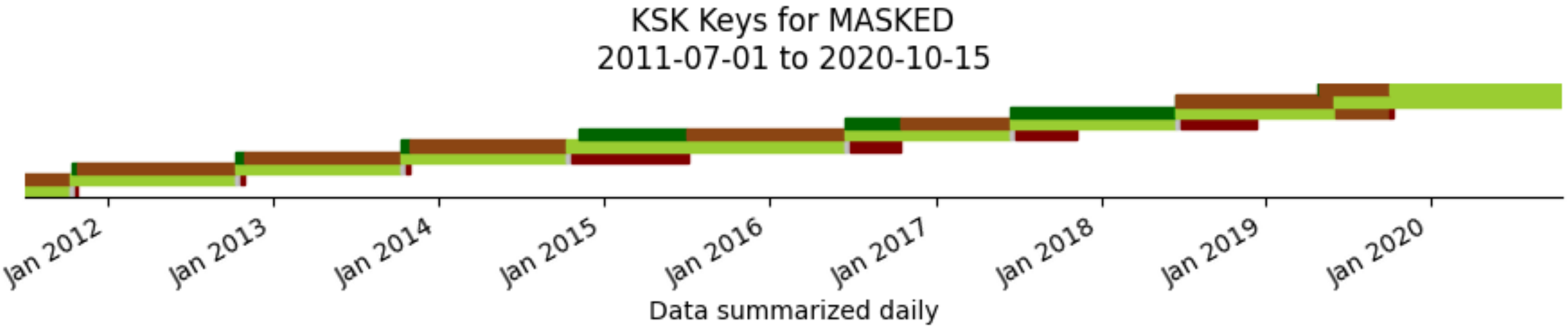


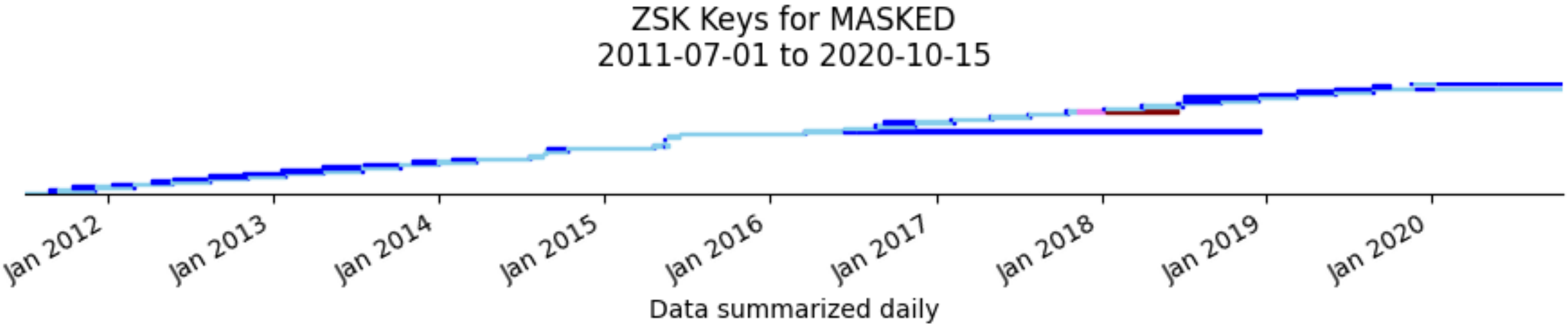
Key Lifecycles – yet another pre-2012 gTLD



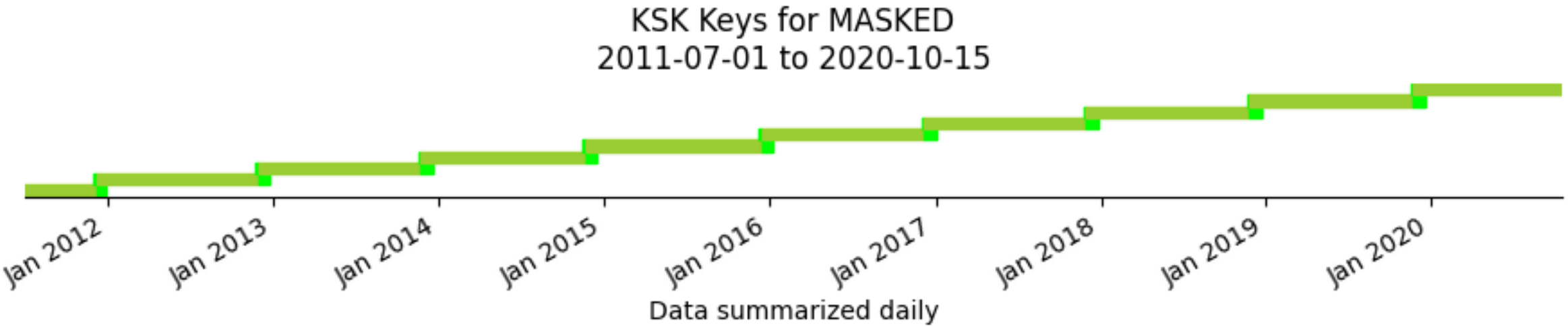


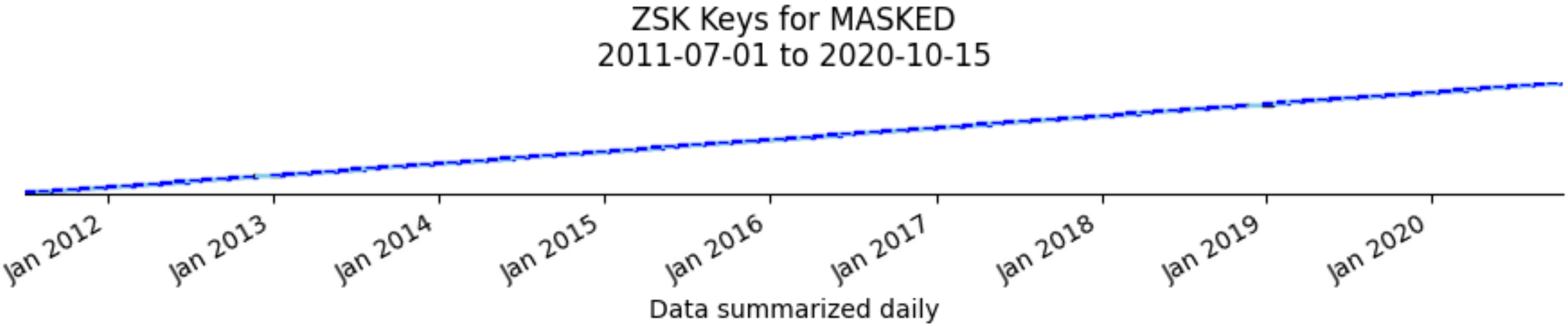
Key Lifecycles – one of the ccTLD, initially with RFC5011



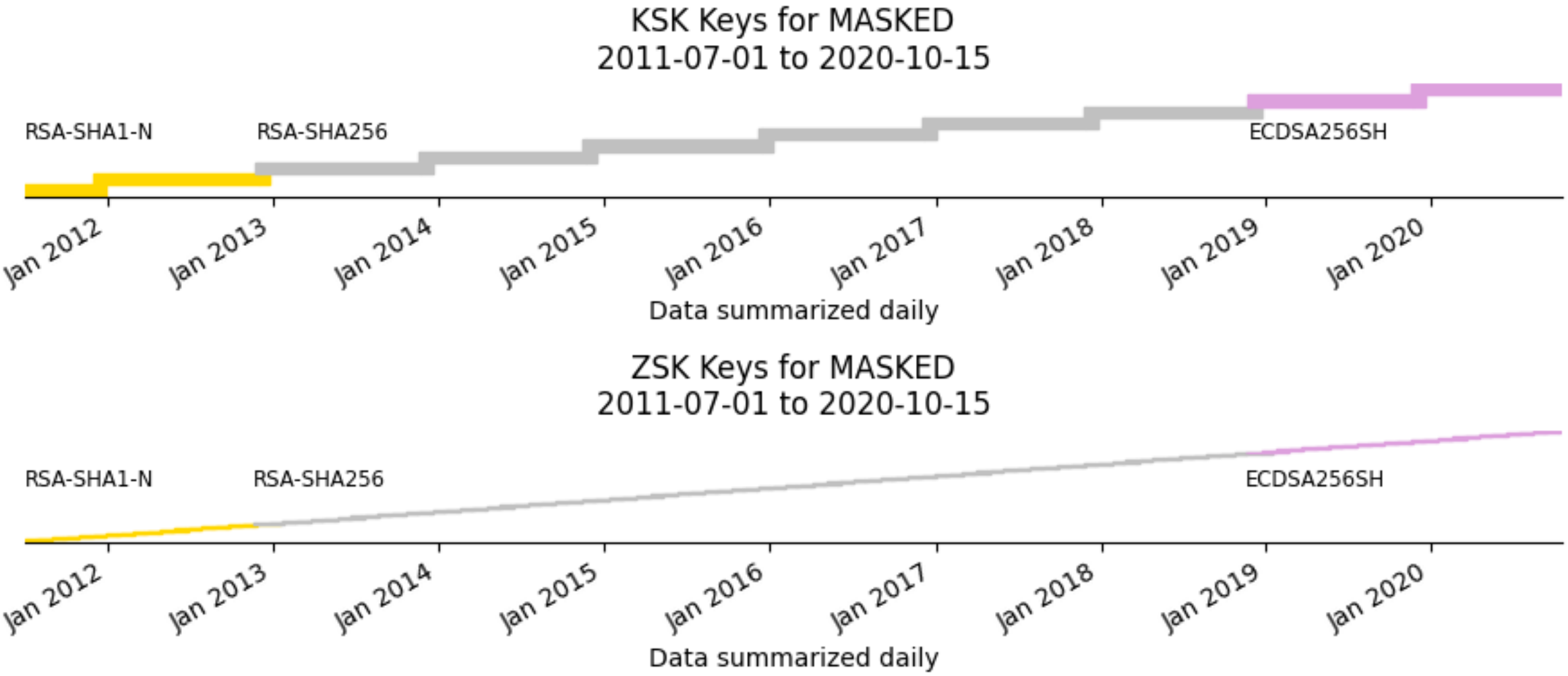


Key Lifecycles – a ccTLD rolling algorithms (slide 1)

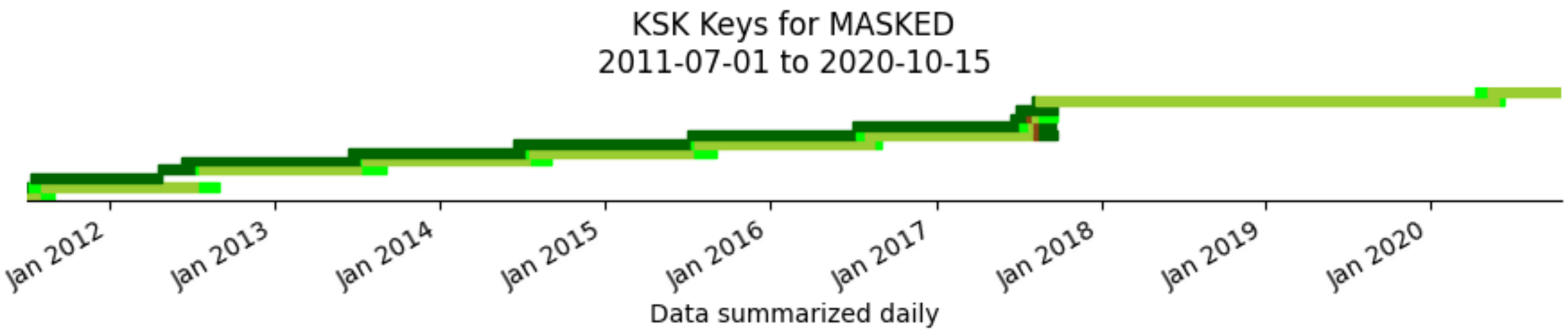


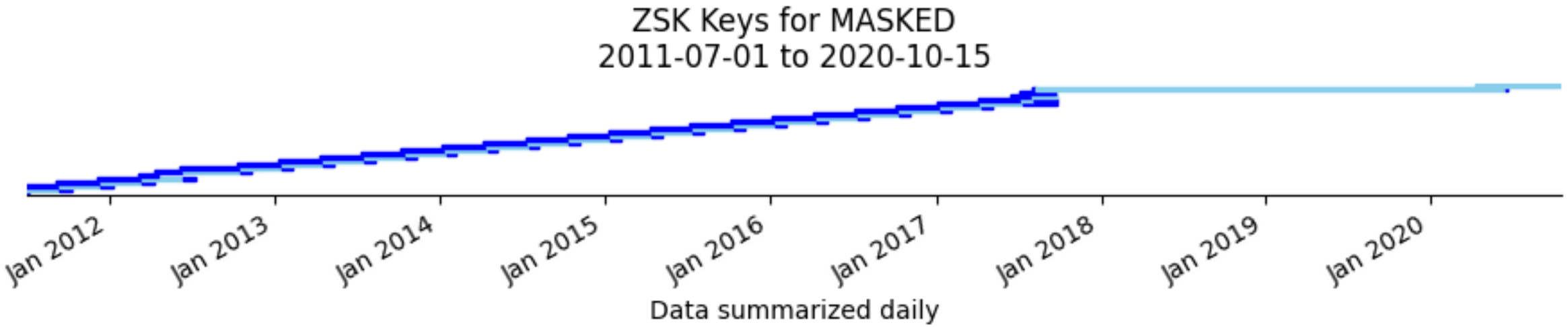


Key Lifecycles – a ccTLD rolling algorithms (slide 2)

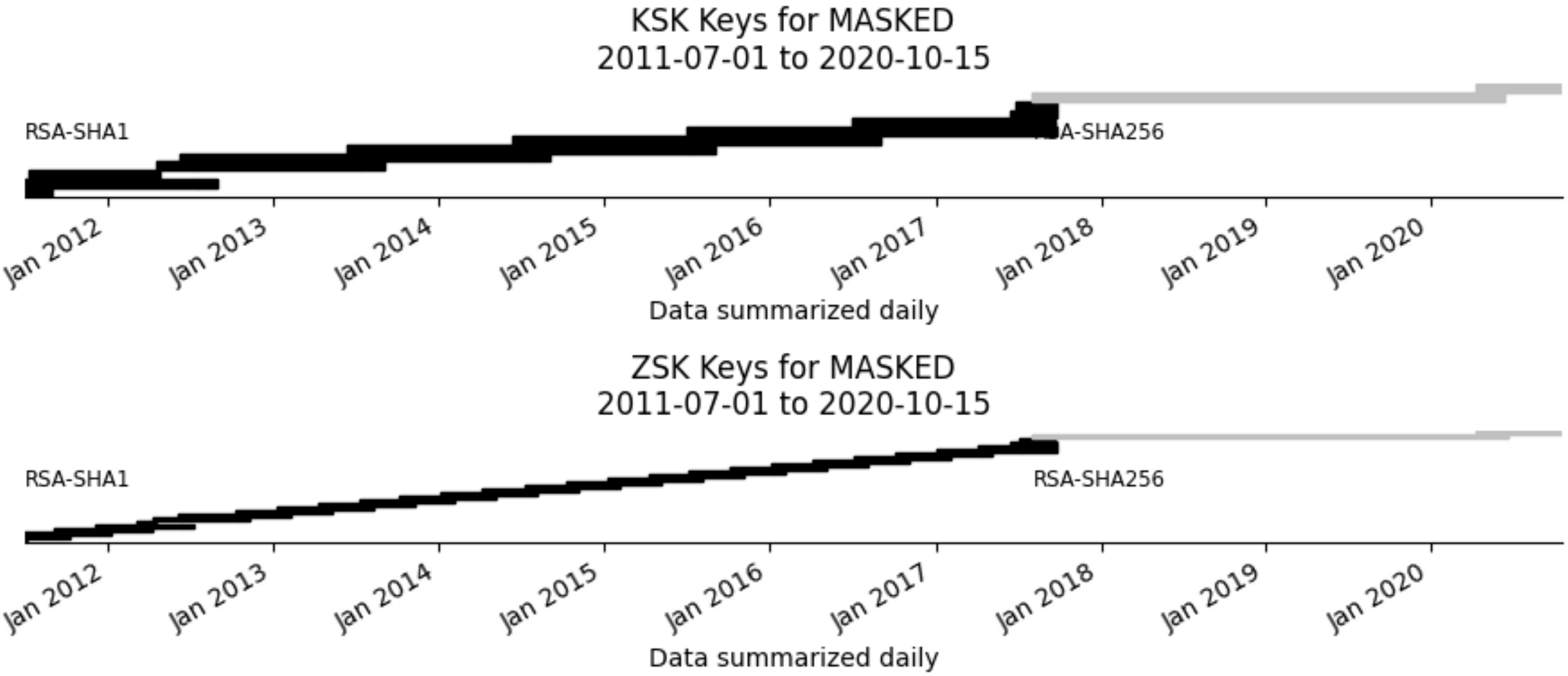


Key Lifecycles – another ccTLD, making changes (slide 1)

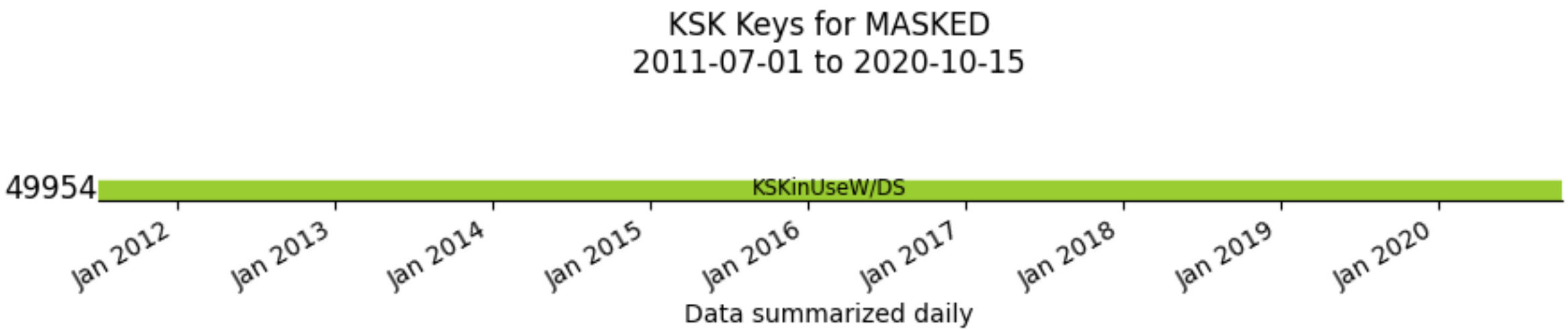


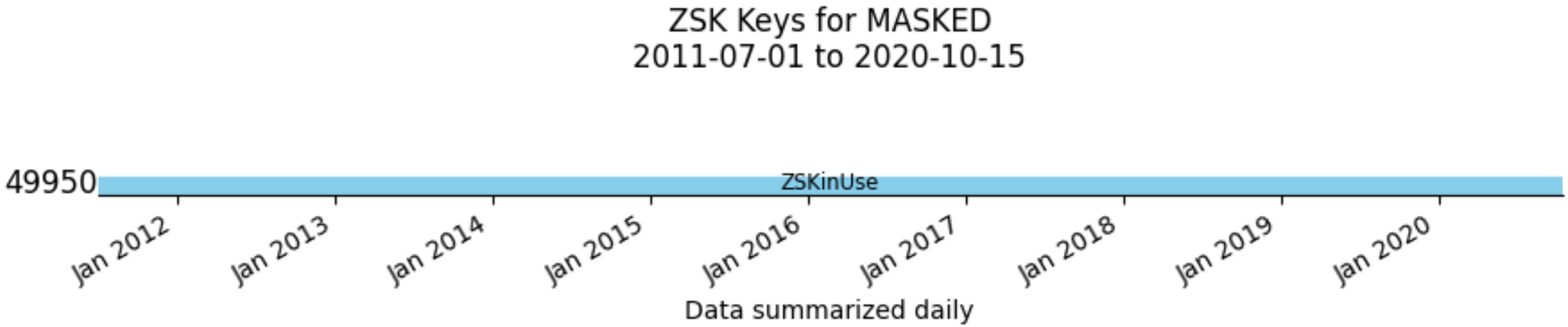


Key Lifecycles – another ccTLD, making changes (slide 2)

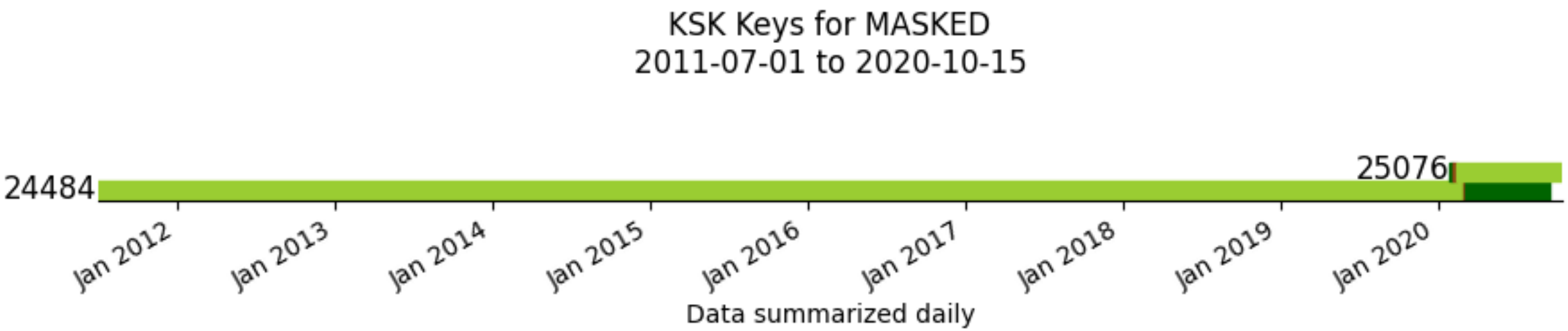


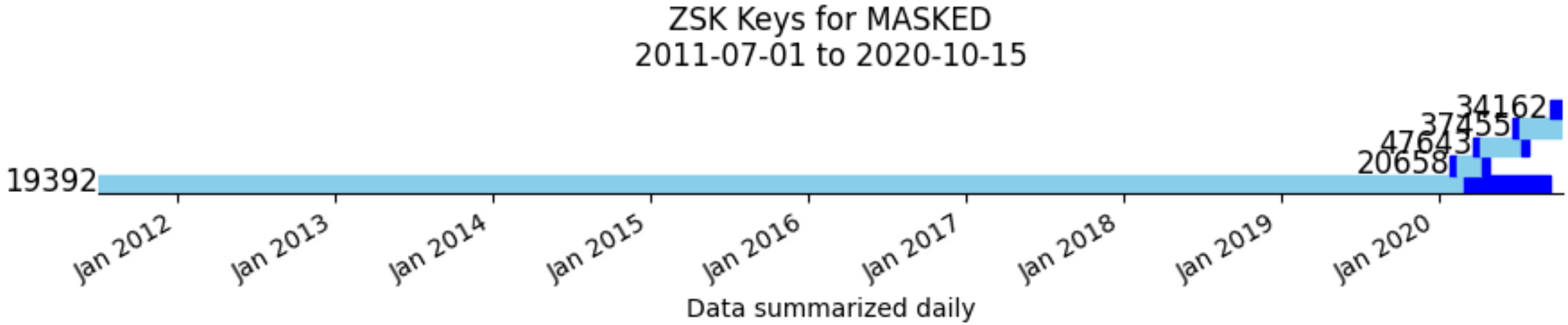
Key Lifecycles – "fire and forget" ccTLD



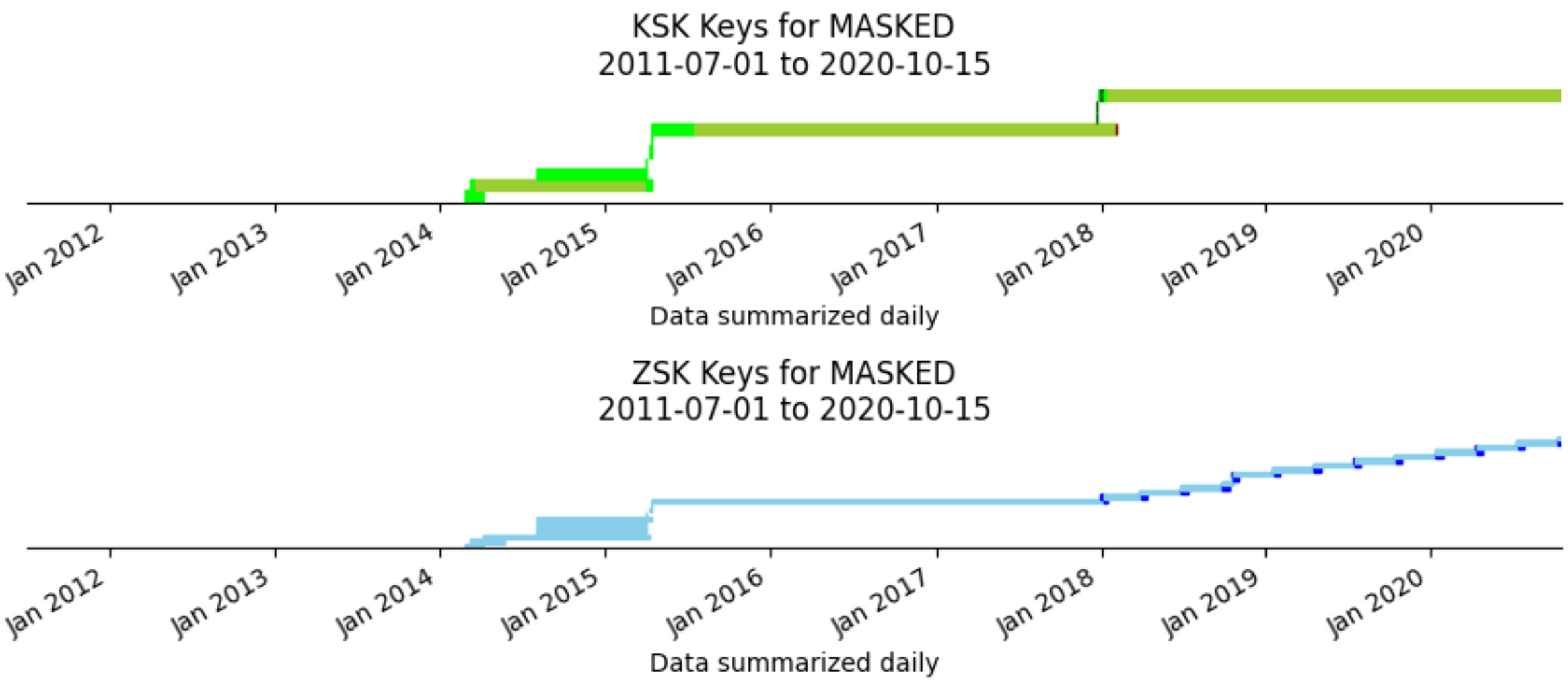


Key Lifecycles – a no longer a "fire and forget" ccTLD

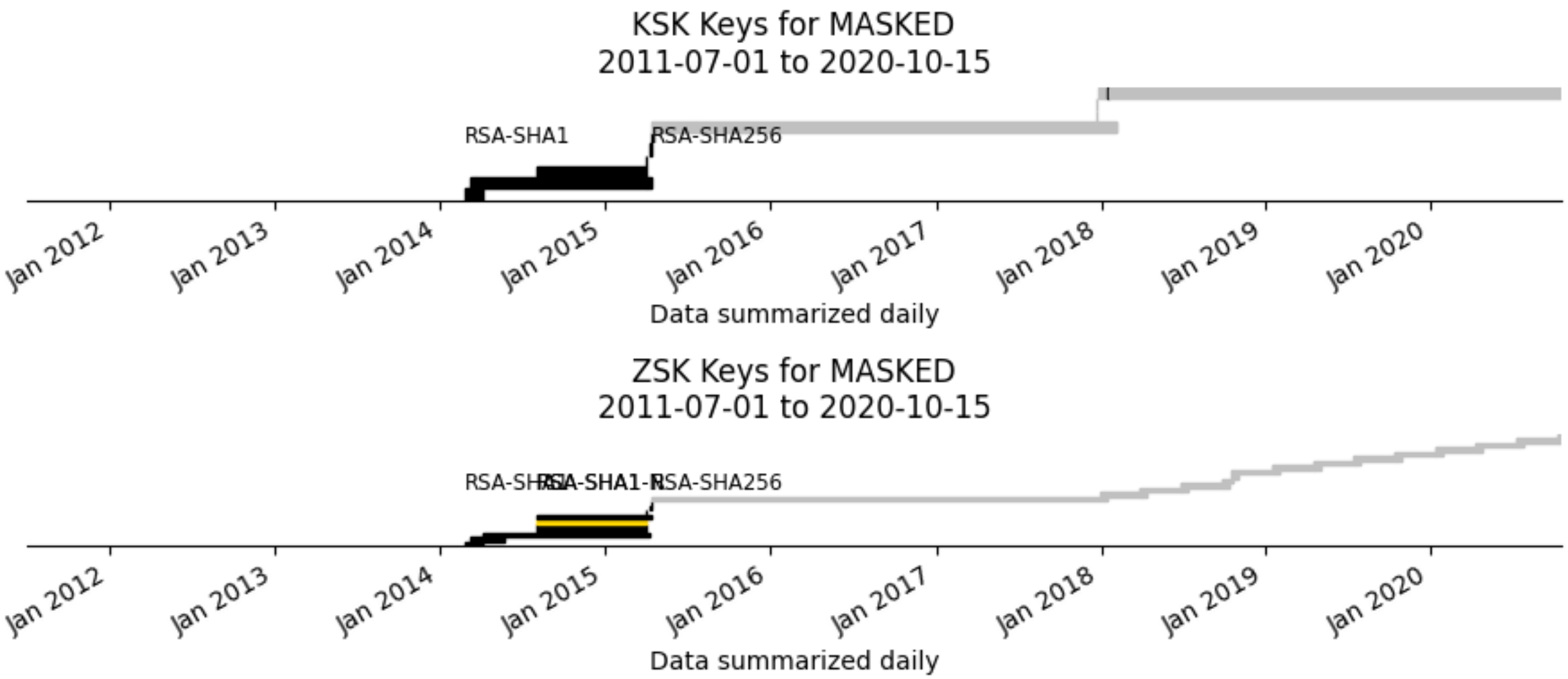




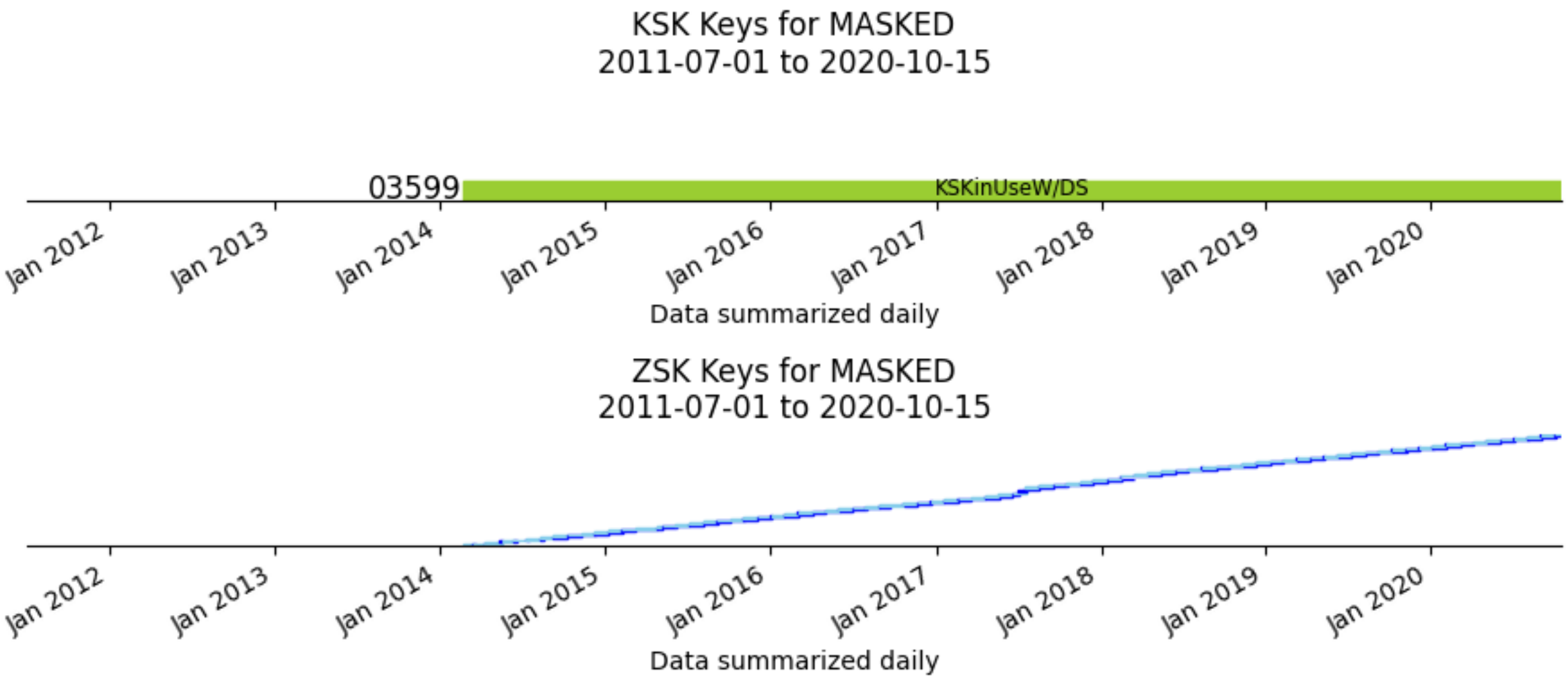
Key Lifecycles – a ccTLD that crashed and has overcome



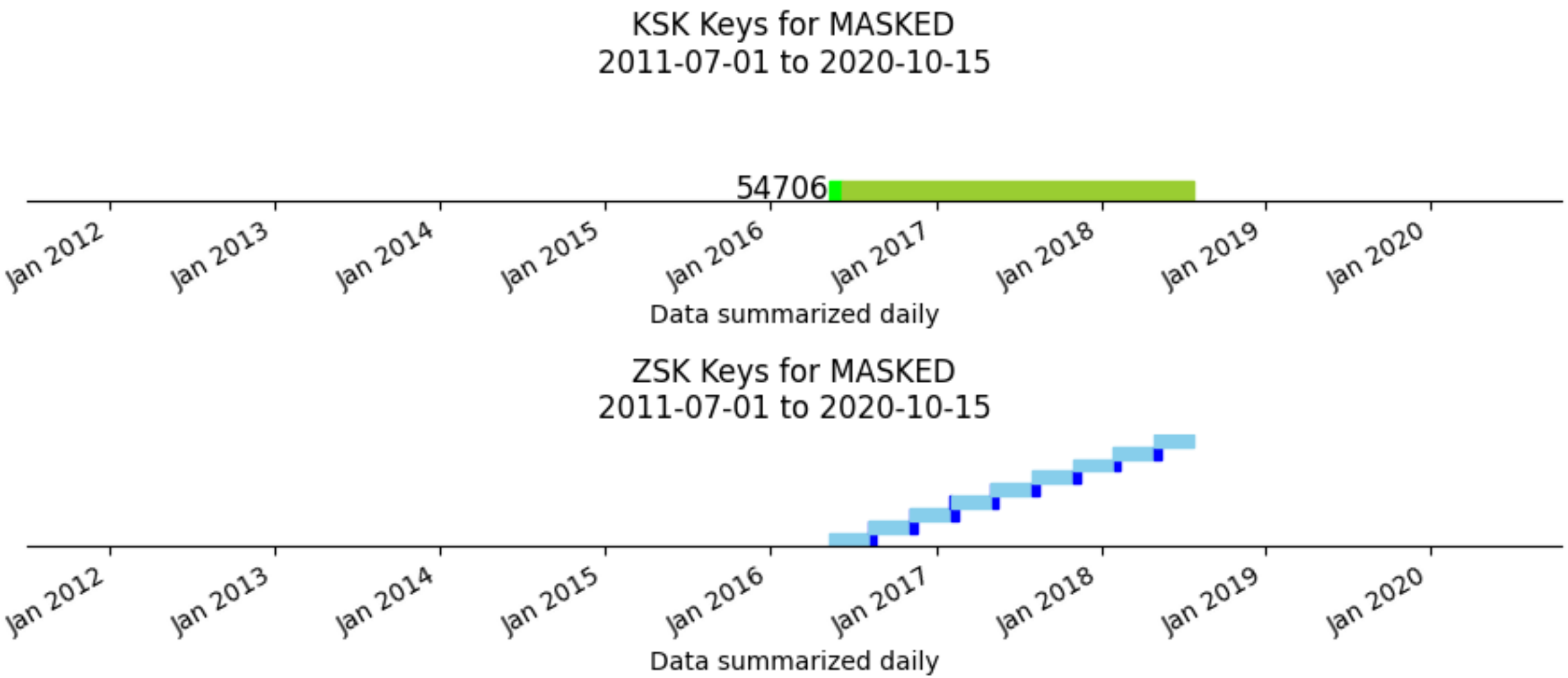
Key Lifecycles – same ccTLD that crashed ... (algs)



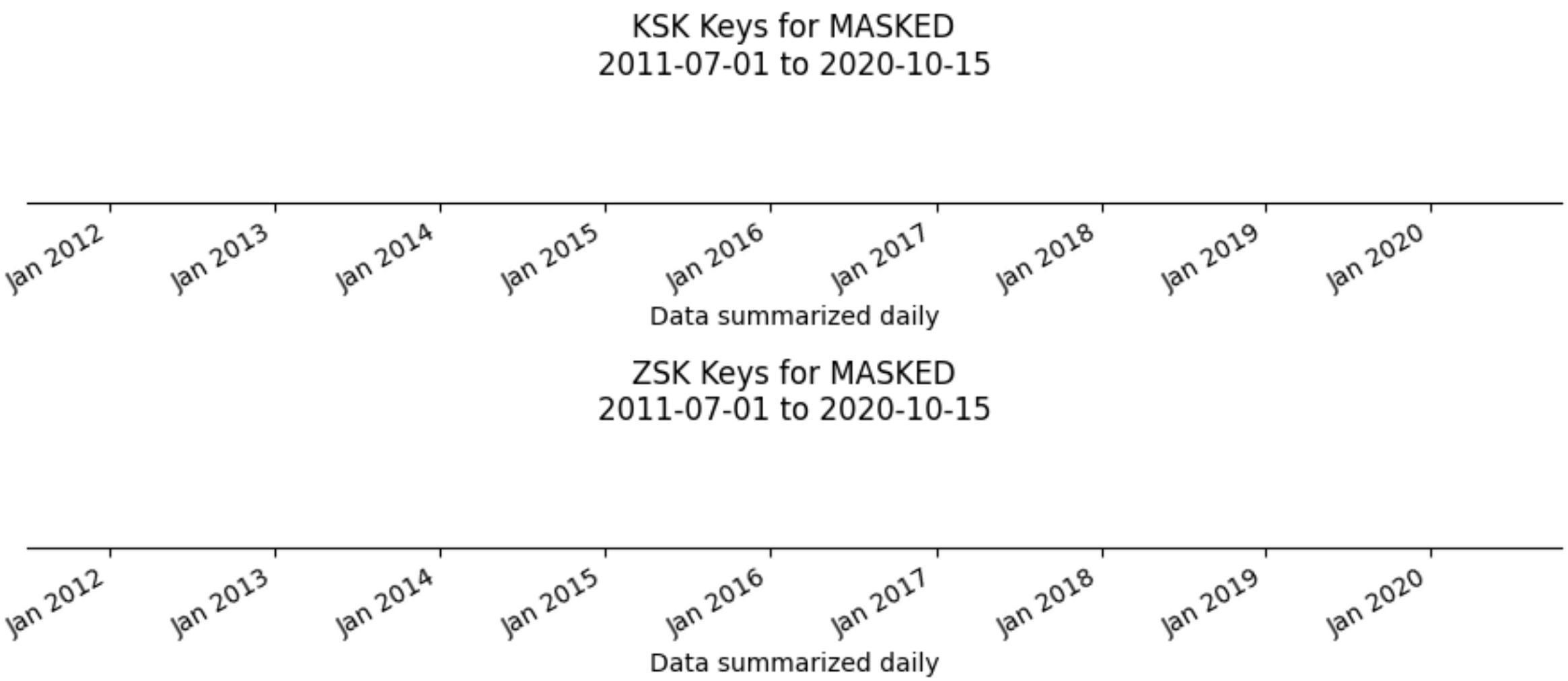
Key Lifecycles – a class-of-2012 gTLD



Key Lifecycles – a ccTLD that has suspended DNSSEC



Key Lifecycles – a TLD that has not done DNSSEC



Discussion

- Questions?

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

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