DNSSEC Algorithm Choices

TLD Choice of DNSSEC Security Algorithms

Edward Lewis

ICANN 72 ccNSO TechDay
25 October 2021

Agenda

- A look at what DNSSEC security algorithms are in use by Top-Level Domains over time
- What makes this interesting?
- gTLD vs. ccTLD, and ICANN regional categorizations (ccTLDs)

DNSSEC Security Algorithm

- Combination of a hash algorithm and a cryptographic algorithm for signing
- IANA managed registry: https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml#dns-sec-alg-numbers-1

Value	Mnemonic	Crypto	Hash	Color In Charts
1	RSAMD5	RSA	MD5	
5	RSASHA1	RSA	SHA-1	⬛
7	RSASHA1-**NSEC3**-SHA1	RSA	SHA-1	🟨
8	RSASHA256	RSA	SHA-256	⬜
10	RSASHA512	RSA	SHA-512	🟥
12	ECC-GOST	GOST	GOST Hash	
13	ECDSAP256SHA256	Elliptic Curve	SHA-256	🟪
14	ECDSAP384SHA384	Elliptic Curve	SHA-384	🟪
15	ED25519	Edwards Curve	Integral to the crypto	
16	ED448	Edwards Curve	Integral to the crypto	
Others...				

DNSSEC Security Algorithms 5 (black) and 7 (yellow)

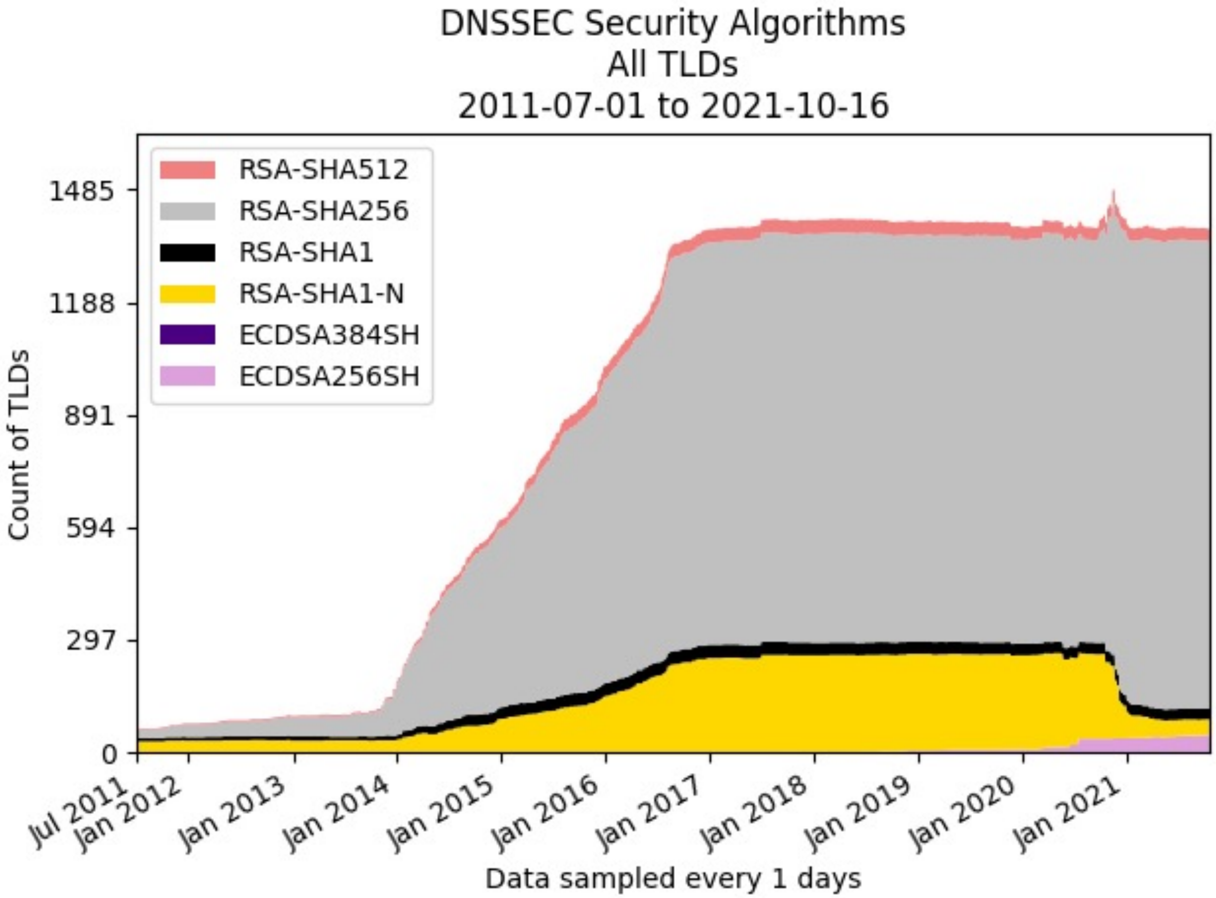
- These two use the same hash (SHA-1) and the same cryptographic signing algorithm (RSA)
- The difference is – one indicates that the “newly defined” (way back then) NSEC3 would be in use in the zone
- So, DNSSEC security algorithms 5 and 7 share the same algorithmic fate
- In the charts they are different colors, just to track them
  - And the colors (black and yellow) are chosen to highlight them
  - Because there is interest in their use, not as a judgement

Choice of Algorithm; Changes

- Cryptography is a mysterious field
  - Few know the difference between “RSA” and “Elliptic Curve”
  - For DNSSEC, the “crypto” is “just a parameter”
    - Data, Signature, Public Key --> Some Algorithm --> “Pass/Fail”
  - When an operator needs to choose, pick the “best”
    - Maybe the latest? Maybe the most recommended? **Maybe the tool’s default!**

- Changing the cryptography in use
  - Possible-but-not-trivial in DNSSEC (“Algorithm Roll”)
  - Costs:
    - Period of large responses (old and new signatures carried)
    - Risk of disruption
  - Benefit:
    - “Better” (*in quotes*) security - hopefully

All TLDs

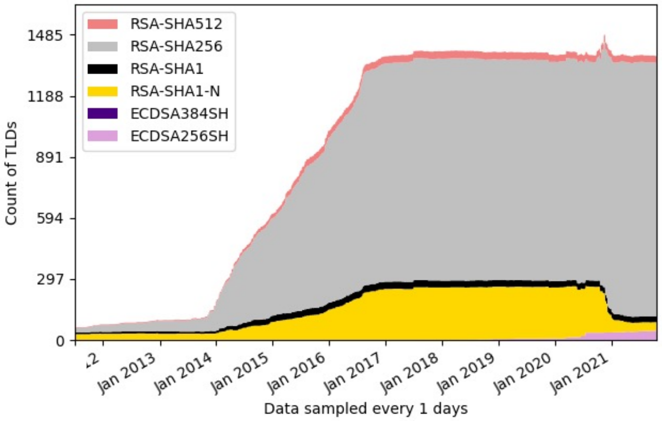

DNSSEC Security Algorithms
All TLDs
2011-07-01 to 2021-10-16
RSA-SHA512
RSA-SHA256
RSA-SHA1
RSA-SHA1-N
ECDSA384SH
ECDSA256SH
Count of TLDs
1485
1188
891
594
297
0
Jul 2011
Jan 2012
Jan 2013
Jan 2014
Jan 2015
Jan 2016
Jan 2017
Jan 2018
Jan 2019
Jan 2020
Jan 2021
Data sampled every 1 days

Why are there “spiky peaks”?

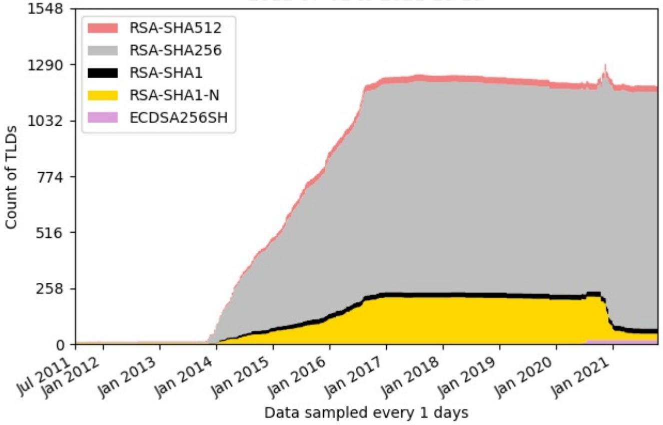
- At any give time, a TLD may use more than one DNSSEC security algorithm
  - Most choose one at a time because each DNS response must carry a signature of each DNSSEC security algorithm in use
  - That makes for large answers
- To change algorithms one approach is to add the new algorithm first and then withdraw the old algorithm next
  - Because of DNS caching!
- So, there will may be a sharp rise in one algorithm, followed by a sharp fall in another
  - The magnitude of the rise and fall is determined by how many TLDs are operated by the same back-end platform
  - Operators like consistency across their work, so they will often change many at a time (after testing a few)

All TLDs vs gTLDs vs ccTLDs

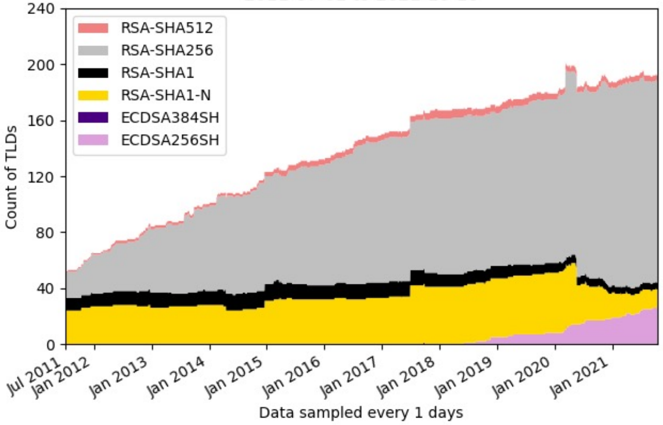
DNSSEC Security Algorithms
All TLDs
2011-07-01 to 2021-10-16



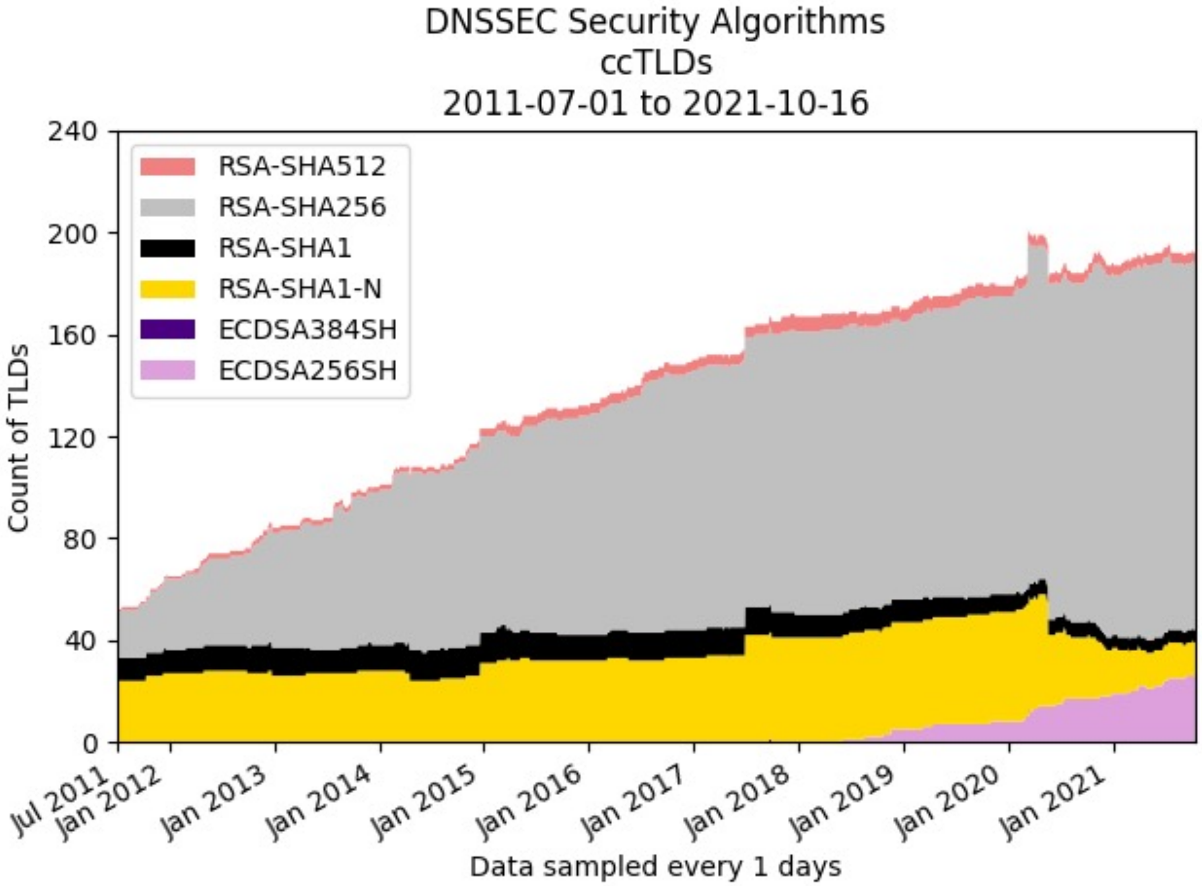
DNSSEC Security Algorithms
gTLDs
2011-07-01 to 2021-10-16



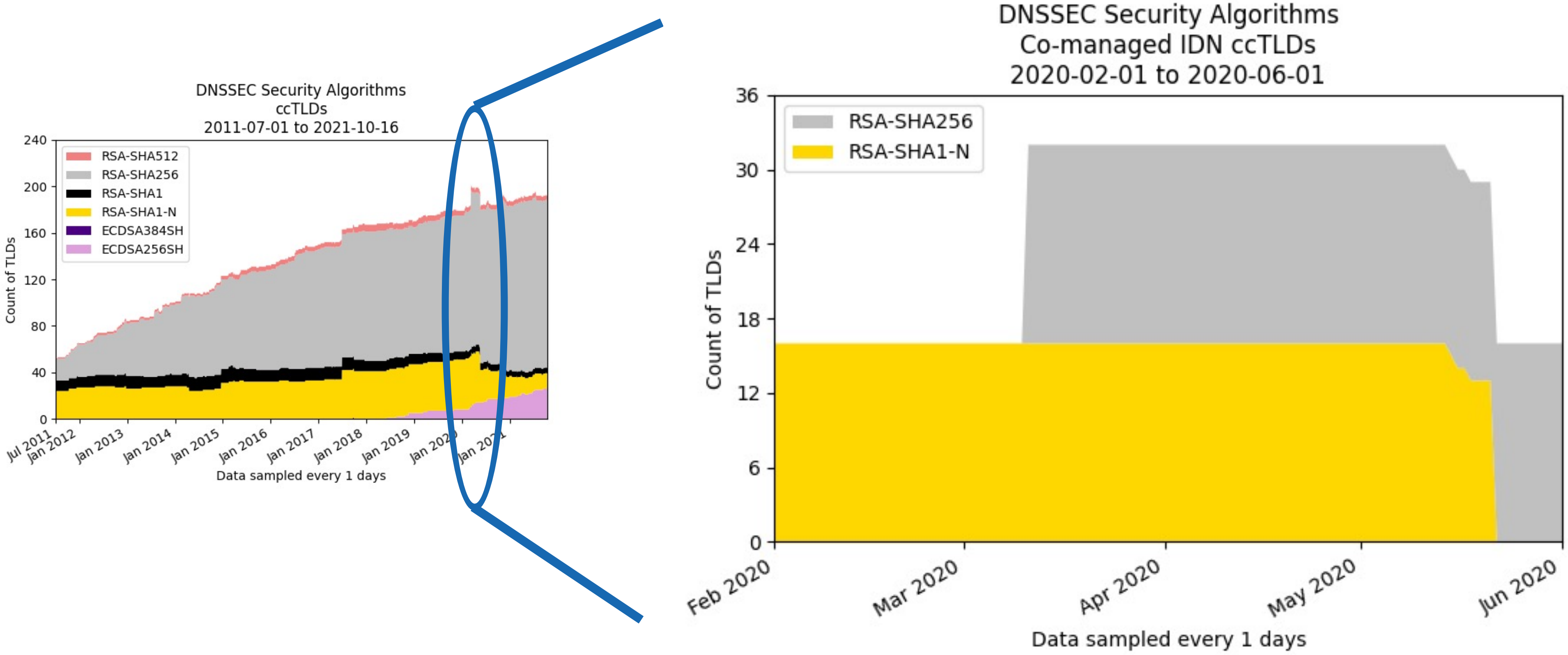
DNSSEC Security Algorithms
ccTLDs
2011-07-01 to 2021-10-16



ccTLDs


DNSSEC Security Algorithms
ccTLDs
2011-07-01 to 2021-10-16
RSA-SHA512
RSA-SHA256
RSA-SHA1
RSA-SHA1-N
ECDSA384SH
ECDSA256SH
Count of TLDs
0
40
80
120
160
200
240
Jul 2011
Jan 2012
Jan 2013
Jan 2014
Jan 2015
Jan 2016
Jan 2017
Jan 2018
Jan 2019
Jan 2020
Jan 2021
Data sampled every 1 days

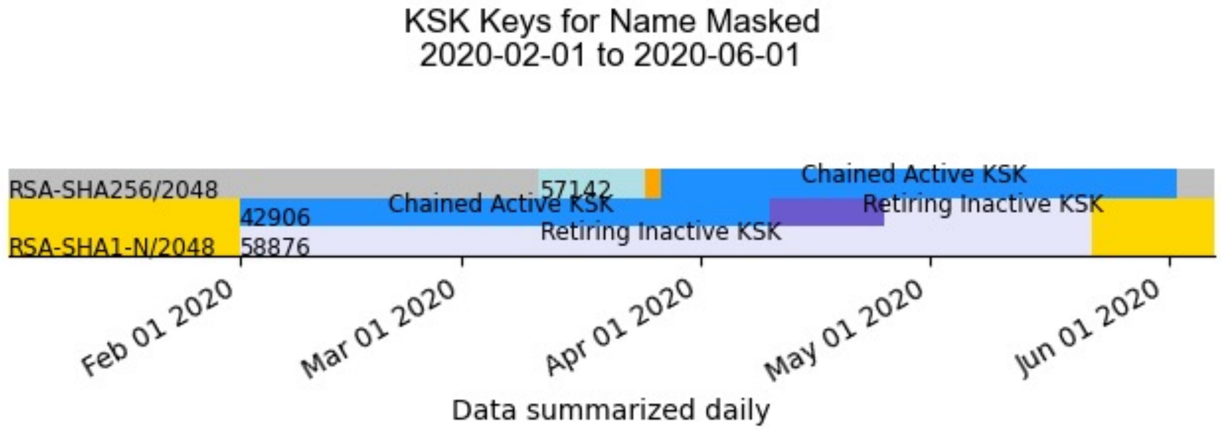
ccTLDs

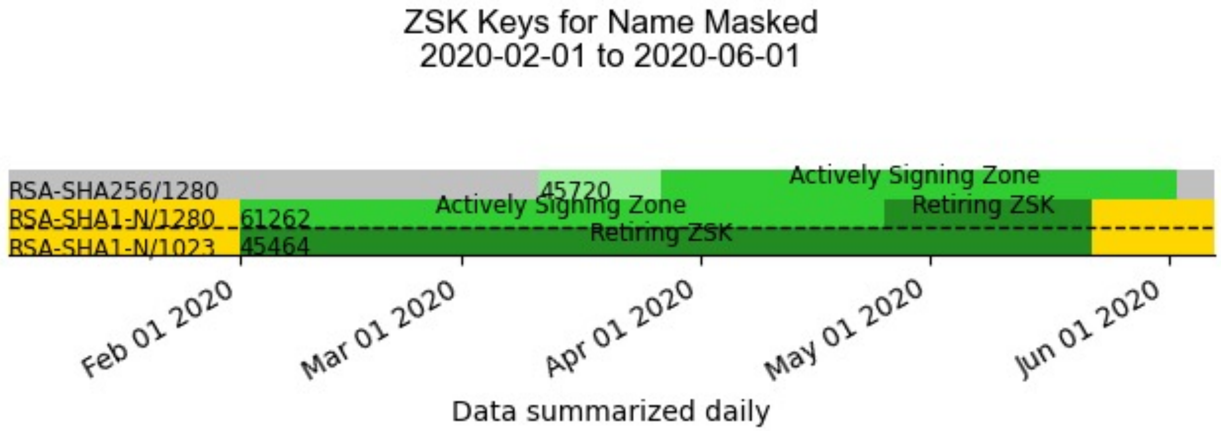


DNSSEC Security Algorithms
ccTLDs
2011-07-01 to 2021-10-16

DNSSEC Security Algorithms
Co-managed IDN ccTLDs
2020-02-01 to 2020-06-01

A deep dive – overlap in an “algorithm roll” (one of the TLDs involved)

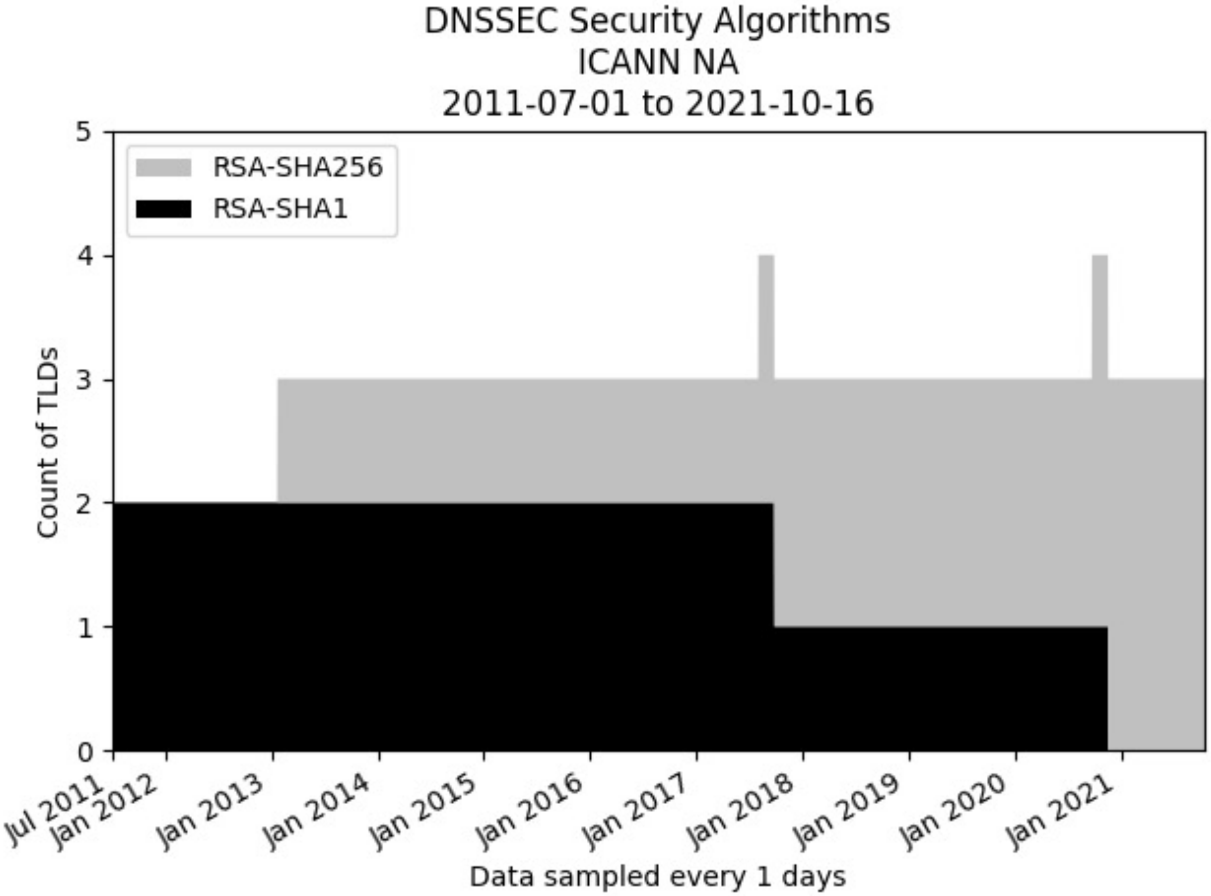




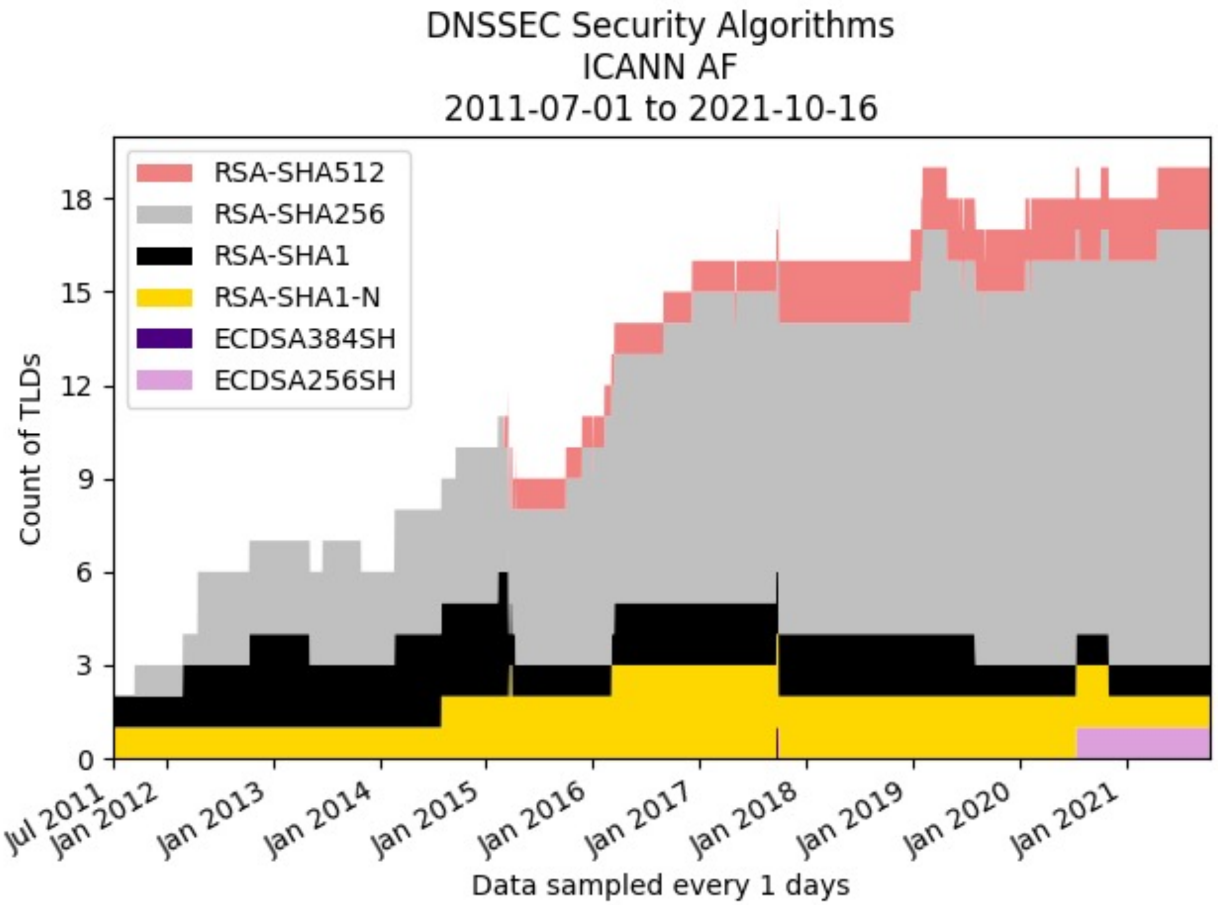
This chart visualizes the lifecycles of keys for one of the involved IDN ccTLDs

- Top chart shows Key Signing Keys, bottom shows Zone Signing Keys
- The new algorithm appears in mid-March
- From late-March to late-April, both algorithms are active
- By late-May, the old algorithm is removed
- Zones involved in the spike follow this pattern

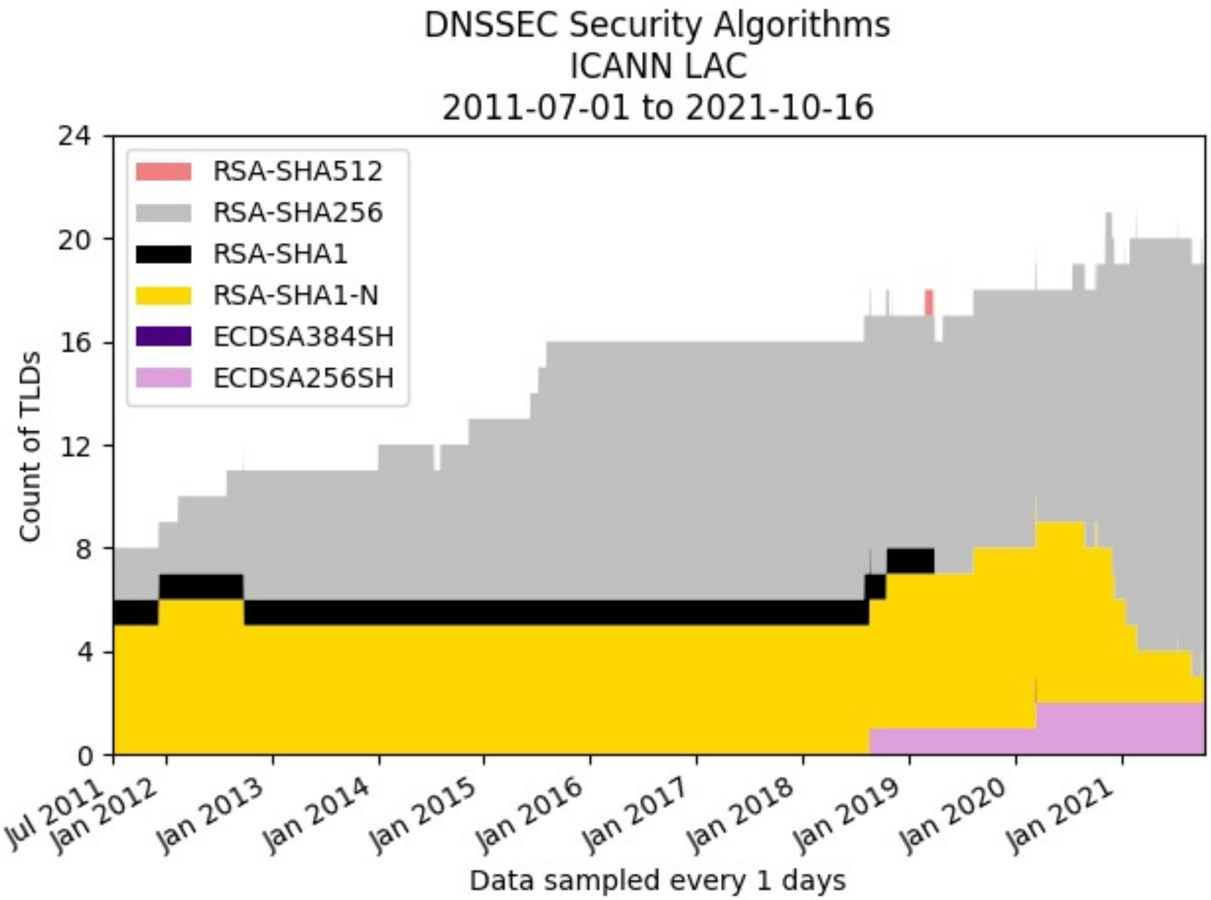
ccTLDs : ICANN North America (8 total, 3 DNSSEC)



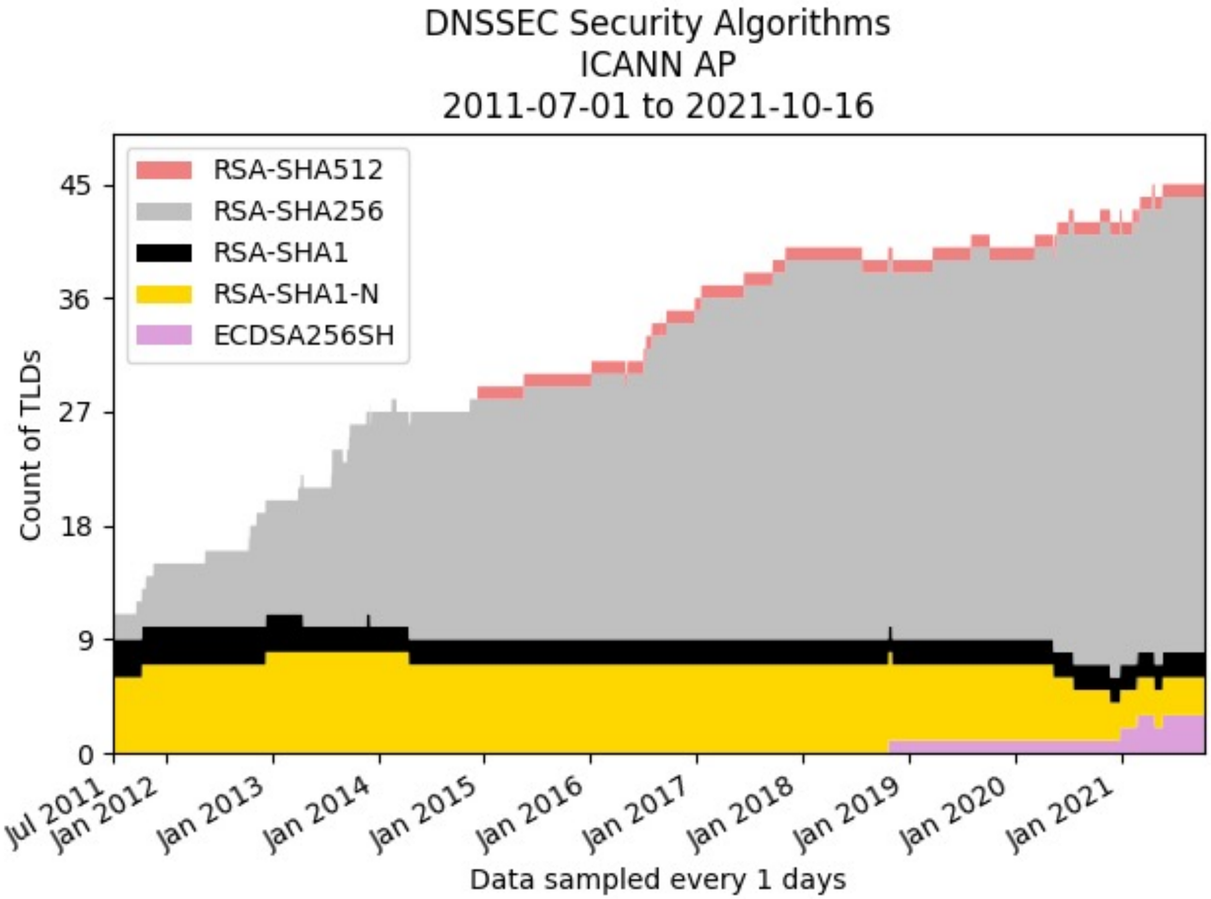
ccTLDs : ICANN Africa (55 total)



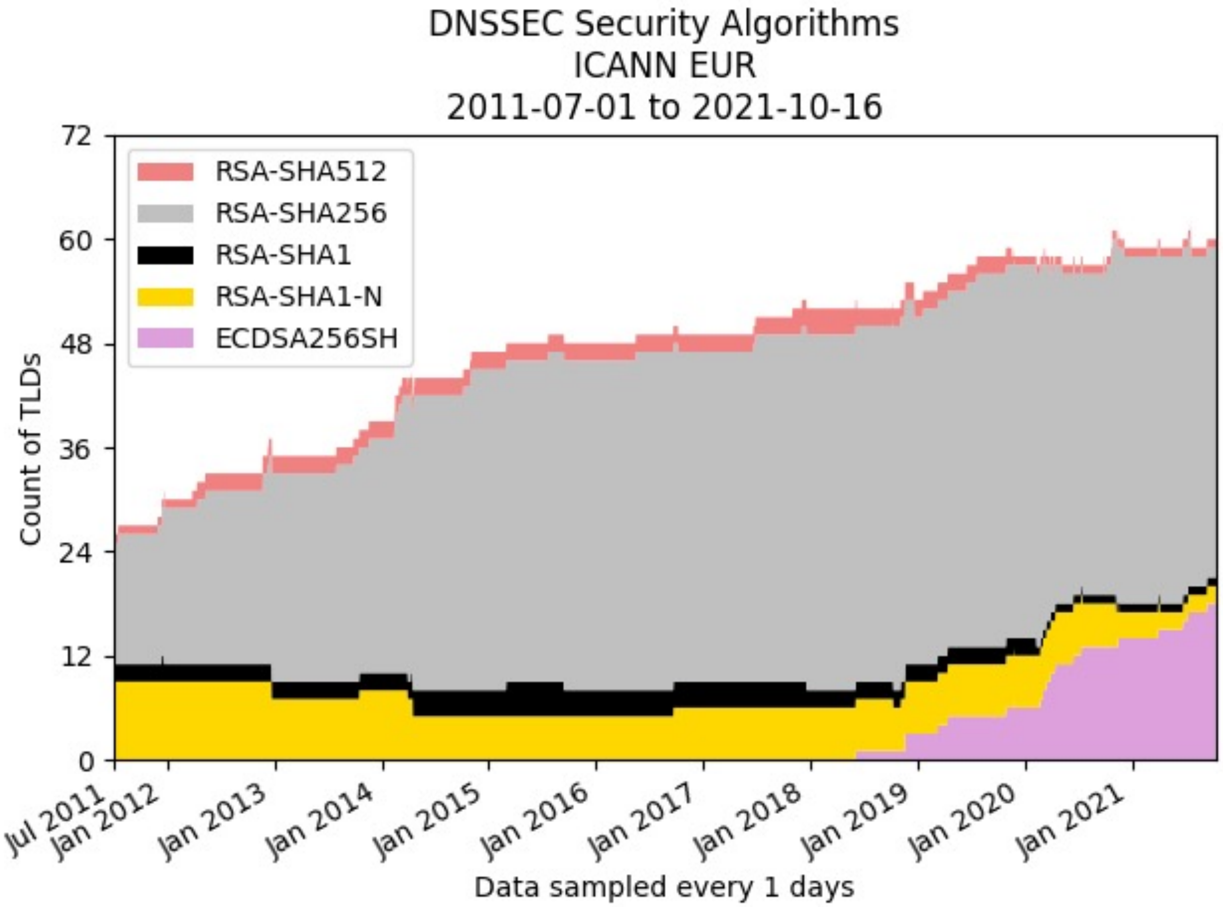
ccTLDs : ICANN Latin America/Caribbean Islands (37 total)



ccTLDs : ICANN Asia/Australia/Pacific (73 total)



ccTLDs : ICANN Europe (77 total)



Engage with ICANN

Thank You and Questions

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

- @icann
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- slideshare/icannpresentations
- soundcloud/icann
- instagram.com/icannorg