Root KSK Rollover Update
(or, We're really doing it this time)

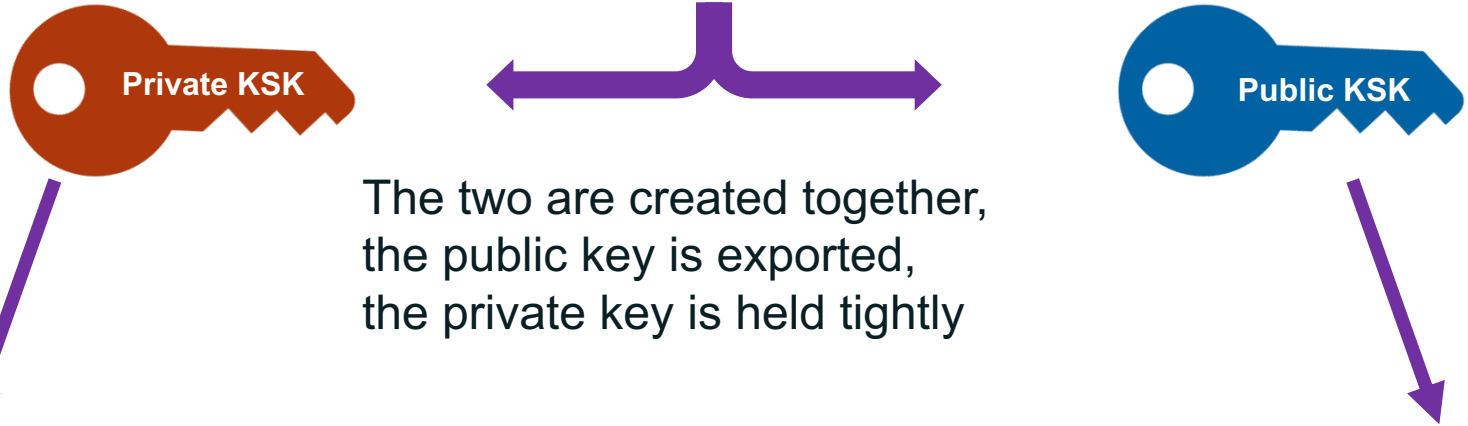
Andres Pavez
IANA

LACNIC 29 / LACNOG

4 May 2018

What is the DNSSEC KSK?

Two Components ("Keys") with a special mathematical bond



The two are created together, the public key is exported, the private key is held tightly

Held secretly in securely managed devices

Distributed widely for configuration in resolvers

What is the DNSSEC KSK?

Two Components ("Keys") with a special mathematical bond

The two are created together, the public key is exported, the private key is held tightly

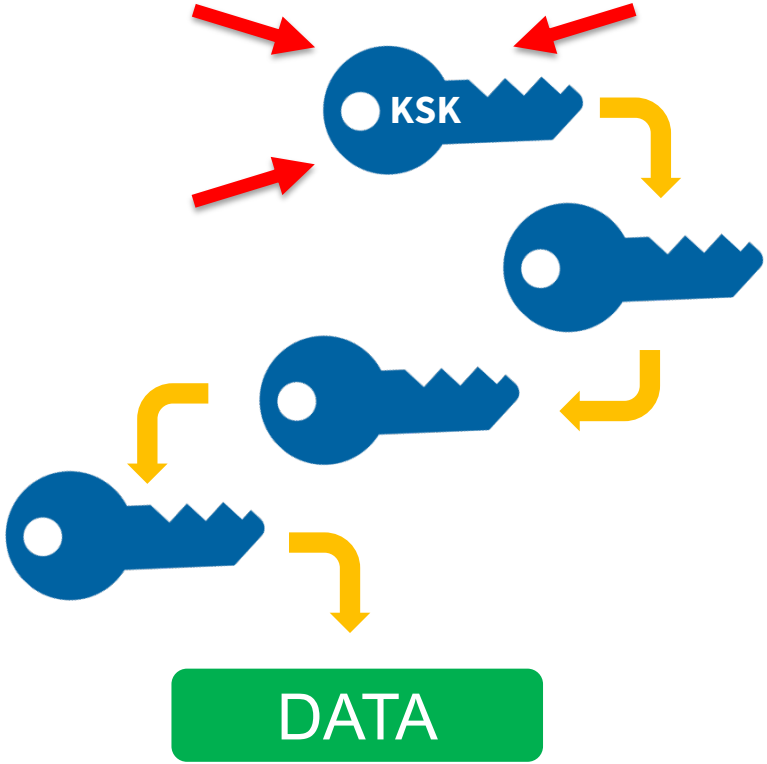
Held secretly in securely managed devices

Distributed widely for configuration in resolvers

This is the hardest part of the project

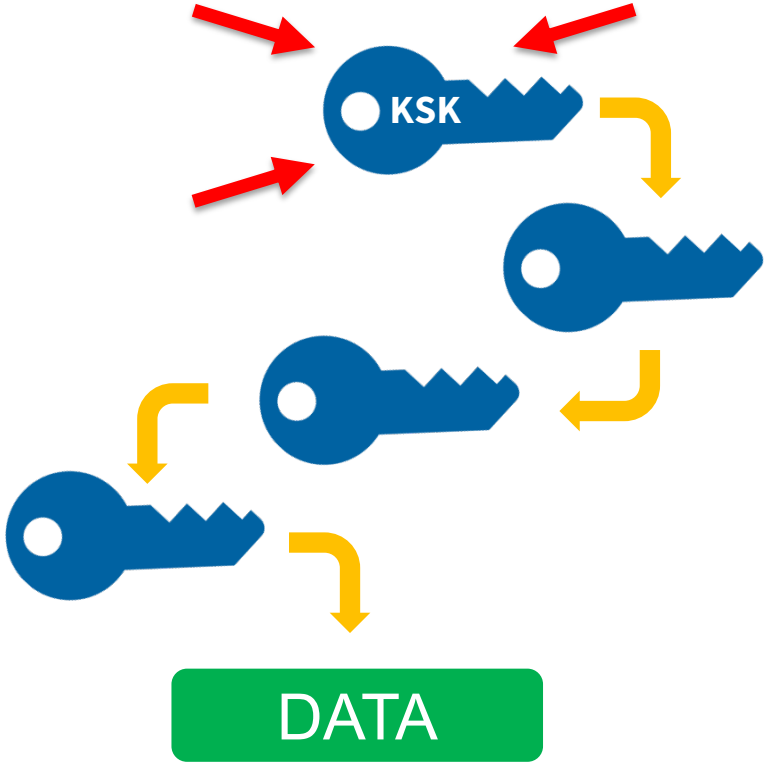
The Importance of the Root Zone DNSSEC KSK

- The Root Zone DNSSEC Key Signing Key “**KSK**” is the top most cryptographic key in the DNSSEC hierarchy
- Public portion of the KSK is a configuration parameter in DNS validating revolvers
- Everyone who wants DNSSEC protection must copy it, store it "locally"



What does it mean to Rollover the KSK?

- The Rollover means replacing, gracefully, the existing KSK with a new KSK
- Changing the Private KSK is a simple operational matter
- Changing the Public KSK involves others who anonymously choose to use DNSSEC



Previously Planned Milestones

Event	Date
Creation of KSK-2017	October 27, 2016
Production Qualified	February 2, 2017
Out-of-DNS-band Publication	February 2, 2017, onwards
Automated Updates Publication	July 11, 2017, onwards
Sign (Production Use)	**October 11, 2017,** onwards
Revoke KSK-2010	January 11, 2018
Remove KSK-2010	Dates TBD, 2018

The "Was To Be"

What's Happened to the Milestones?

Event	Date
Creation of KSK-2017	October 27, 2016
Production Qualified	February 2, 2017
Out-of-DNS-band Publication	February 2, 2017, onwards
Automated Updates Publication	July 11, 2017, onwards
Sign (Production Use)	***October 11, 2018, not confirmed***
Revoke KSK-2010	***TBD***
Remove KSK-2010	***TBD***

What Happened? Why pause?

- When the process began we established rules for "unexpected states"
  - One of the planned rules for progressing the plan included
    - If evidence of trouble ahead, pause
  - But there were no alarms available at the time

  - As the rollover process proceeded, a readiness measure was invented in the IETF
    - *Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)*
    - Commonly known as RFC 8145
      - BIND implemented in 9.9.10, 9.10.5 and 9.11.0, released 19 April 2017
      - Unbound 1.6.4, released 27 June 2017
      - Knot Resolver 1.5.0, released 2 November 2017

  - By September 2017, the readiness measure indicated "there might be problems"

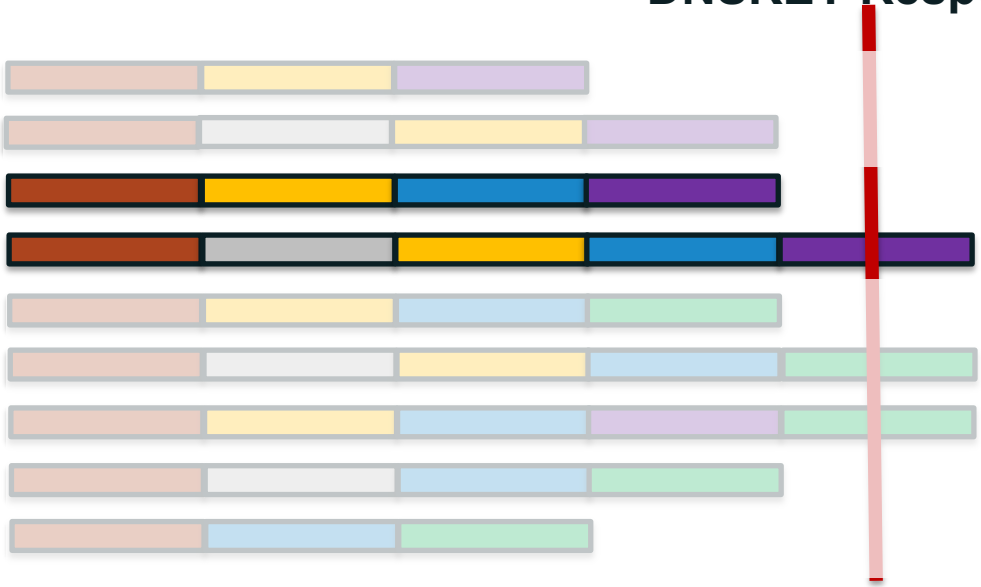
Following our Plan

- *2017 KSK Rollover Ops Implementation Plan* states:
- The ceremony in phase D, to prepare for phase E, is tentatively scheduled for the third quarter of 2017 (assuming that phase C was not extended). ... There will be four files generated:
  - D-to-E: move from publication to rollover (skr-root-2017-q4-d-to-e.xml)
  - E-to-D: back out from rollover to publication (skr-root-2017-q4-e-to-d.xml)
  - **D-to-D: extend phase D, stay in publication (skr-root-2017-q4-d-to-d.xml)**
  - C-to-C: prolong backout from phase D (skr-root-2017-q4-c-to-c.xml)
- That ceremony, held 17 August 2017 prepared us for the fall back. The ceremonies held 18 October 2017, 2 February 2018 and 11 April 2018 repeated this step, allowing us to remain in the current "Phase D" – the phase in which KSK-2017 appears in the root zone DNSKEY set.

Are We Safe? Old concern: DNSKEY Response Size

- **Visualizing Packet Sizes**

1280 Byte "Limit" for the DNSKEY Response



- 'thru' June-19 — 864 Bytes
- 2017-June-20 — 1139 Bytes
- 2017-July-11* — 1139 Bytes
- 2017-Sept-19* — 1414 Bytes
- KSK Rolls — 1139 Bytes
- Roll w/nextZSK — 1414 Bytes
- Revocation — 1424 Bytes
- New Normal — 1139 Bytes
- New Normal — 864 Bytes

- **(*) – These states are now repeated quarterly as we pause**

September 2017

- Verisign analyzed RFC8145 trust anchor report data sent to A & J root servers
  - Very small number of resolvers reporting trust anchor data (<1500 unique per day)
  - But significant percentage (~7-8%) had only KSK-2010
- ICANN OCTO analyzed B, D, F and L root traffic for entire month of September 2017
  - 11,982 unique IP addresses (IPv4 and IPv6) reporting
  - 500 reported only KSK-2010 (4.1%)
- 27 September 2017: The ICANN org postpones the root KSK roll
  - Needing to understand reasons why so many resolvers have only KSK-2010

October–December 2017

- The ICANN org attempts to contact operators of the 500 resolvers from September 2017
- Findings:
  - Tracking down operators based on just IP address is ***hard!***
  - Operators for only 20% (100 addresses) could be contacted
  - Of those:
    - 60% in address ranges known to host devices with dynamic IPs
    - 25% from resolvers forwarding queries from other resolvers
  - No single cause
  - No obvious path forward
    - E.g., bug fix by resolver vendor, new communication messages, etc.

December 2017–January 2018

- With no clear path forward, the ICANN org decided to solicit community input
- Input and discussion on acceptable criteria for proceeding with the KSK roll took place on *ksk-rollover@icann.org*
- Results of discussion:
  - Agreement there is no way to accurately measure the number of users who would be affected by rolling the root KSK
  - But a belief better measurements may become available for future KSK rollovers
  - Consensus was that the ICANN org should proceed with rolling the root zone KSK in a timely fashion
  - And continue outreach to ensure rollover news reaches as wide an audience as possible

February-April 2018

- The ICANN org published a *draft* plan to proceed with the KSK rollover:
  - Draft calls for rolling the root zone KSK on **11 October 2018**
    - No specific measureable criteria emerged during community discussion
  - Continue extensive outreach
    - We will keep publicizing the root KSK roll
  - Publish more observations for trust anchor report data
    - Now publishing monthly snapshots of the RFC 8145 trust anchor report data received from most of the root servers

- Public comment period on the draft plan closed 2 April 2018,and staff report
  - https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en
  - https://www.icann.org/en/system/files/files/report-comments-ksk-rollover-restart-23apr18-en.pdf

- Updated plans plus other information can be found
  - https://www.icann.org/resources/pages/ksk-rollover

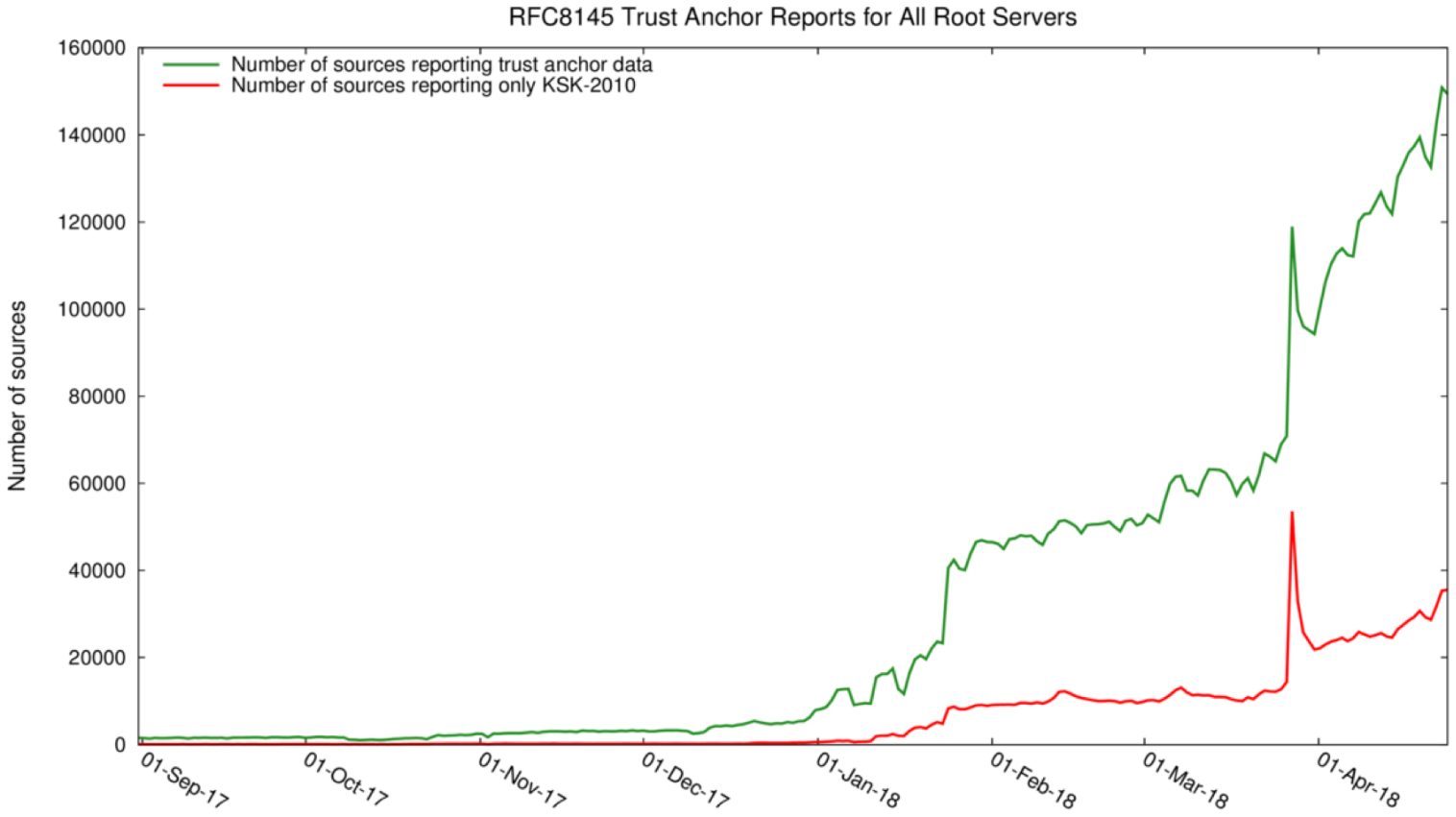
Root KSK Rollover Proposed Schedule *(draft)*

Date	Action
1 February 2018	Draft plan published, public comment opened
10-15 March (ICANN61)	Hold session for community feedback
2 April	Comment period ends; revise plan, as necessary
23 April	Publish staff report on public comment
May (ICANN Board workshop)	Request Resolution asking RSSAC & SSAC to review and comment by 1 Aug
24-28 June (ICANN62)	Hold session for community feedback
1 August	Receive RSSAC and SSAC feedback; revise plan, as necessary
Mid August	Publish final plan, with message that roll is contingent on Board resolution
September (Board workshop)	Request Resolution directing ICANN org to roll on 11 October 2018
11 October 2018	Rescheduled date for root KSK roll - ***not confirmed***

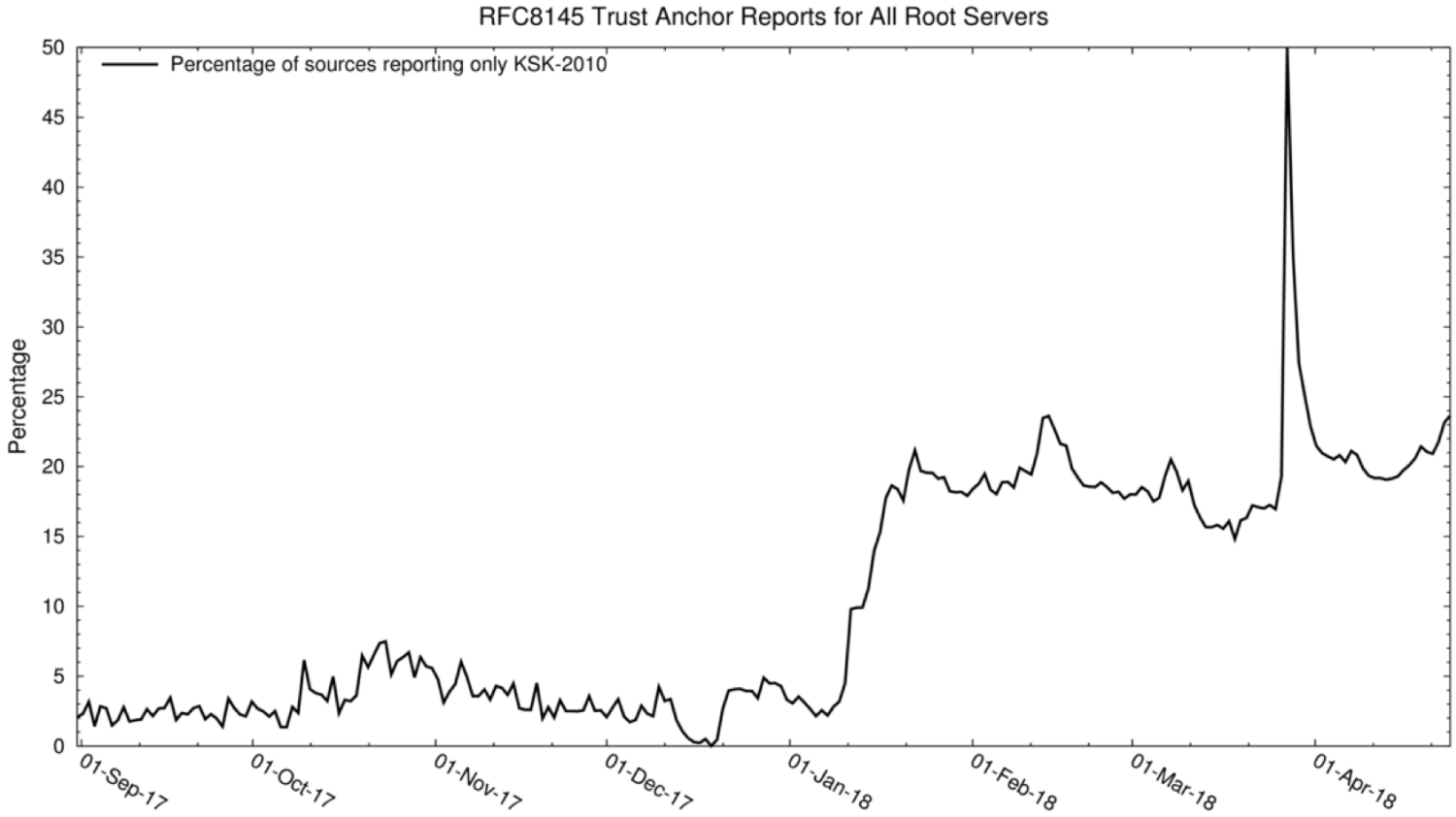
Looking at the RFC8145 Trust Anchor Reports

- ICANN OCTO has access to RFC8145 data from 11 root servers
  - A, B, C, D, E, F, I, J, K, L, M
- Initial analysis (late 2017) used pcap (packet capture) data from B, D, F
- Now using stats collected by Duane Wessels's excellent *rzkeychange* plug-in for *dnscap*
- ***Some sources reporting only having KSK-2010!***
- ***Still very confusing data!***
  - Reporting addresses may be repeating another's report, many addresses give no other evidence they perform DNSSEC validation
  - Independent investigations into buggy, non-DNS software (i.e., other than resolver vendor code)
  - DNS is not designed to be easily measured

RFC 8145 Reporting Addresses (1 Sept 2017 to 25 April 2018)



Percentage of KSK-2010 only servers



Why the Jump(s)?

- An example of a hard-to-understand event
  - This "just happens" to involve a specific implementation, *it is only an example*
- Best hypothesis: Unbound 1.6.8 released on 19 January 2018
  - *“Fix for CVE-2017-15105: vulnerability in the processing of wildcard synthesized NSEC records”*
  - Patch related to security, so perhaps many operators had a strong motivation to upgrade?
- But why no drop-off in KSK-2010 after 30 days?
  - RFC5011 support should update trust anchor store after ~30 days
  - Hypothesis: upgrade in place means *unbound-anchor* not run again, so configuration might still have only KSK-2010
- Maybe many of these are ephemeral VMs or containers?
  - They never run long enough for RFC5011 add hold-down timer to complete

Community Assistance in Understanding the Data

- We did a limited distribution of a list of IP addresses reporting only KSK-2010
  - ISPCP and RIRs willing to help track down operators
  - Two purposes:
    1. Get systems updated with KSK-2017
    2. Continue to look for root causes of non-updating and adjust outreach and actions, as necessary
- Independent researchers diving into more detailed data
  - Stakeholders have more data than is public
- Making the list more widely available still under consideration

What Can You Do?

- If you have other data, other background, you are encouraged to investigate too
  - Please let us know
  - There's a need to correlate data, hypothesis and actions
  - A little bit of data can be a dangerous thing to act upon
- Nevertheless, if you run a resolver
  - Turn on DNSSEC and configure the new KSK
  - Start here: https://www.icann.org/resources/pages/ksk-rollover
  - Refer to this: https://www.icann.org/en/system/files/files/ksk-rollover-quick-guide-prepare-systems-25apr18-en.pdf
- You don't need to wait and use *Automated Updates* (RFC 5011) to trust KSK-2017
  - KSK-2017 is a secure key, we encourage you to treat the (correct) key as "trusted"
- Join the *ksk-rollover@icann.org* mailing list to stay updated

Next Steps for the Rollover Project

- We keep investigating RFC8145 data
  - Why do some roots servers have a lower percentage reporting KSK-2010?
  - More analysis of sources at ASN level
- Contact ASNs with the most sources reporting only KSK-2010
- Encourage and assist others investigating sources reporting only KSK-2010
- Continue publicizing the root KSK roll
- We keep listening to the community

Thank You and Questions

Visit us at **icann.org**
Email: andres.pavez@iana.org
OCTO: edward.lewis@icann.org / matt.larson@icann.org

 @icann

 facebook.com/icannorg

 youtube.com/icannnews

 flickr.com/icann

 linkedin/company/icann

 slideshare/icannpresentations

 soundcloud/icann