Rolling the DNS Root Key Based on Input from Many ICANN Communities

– Or –

Rock, meet hard place…

David Conrad, CTO

IETF 101 Thursday Lunch Speaker Series
22 March 2018

Overview

- Introductions
- How we got to where we are
- Where are we?
- What's next
- Implications
- How you can help

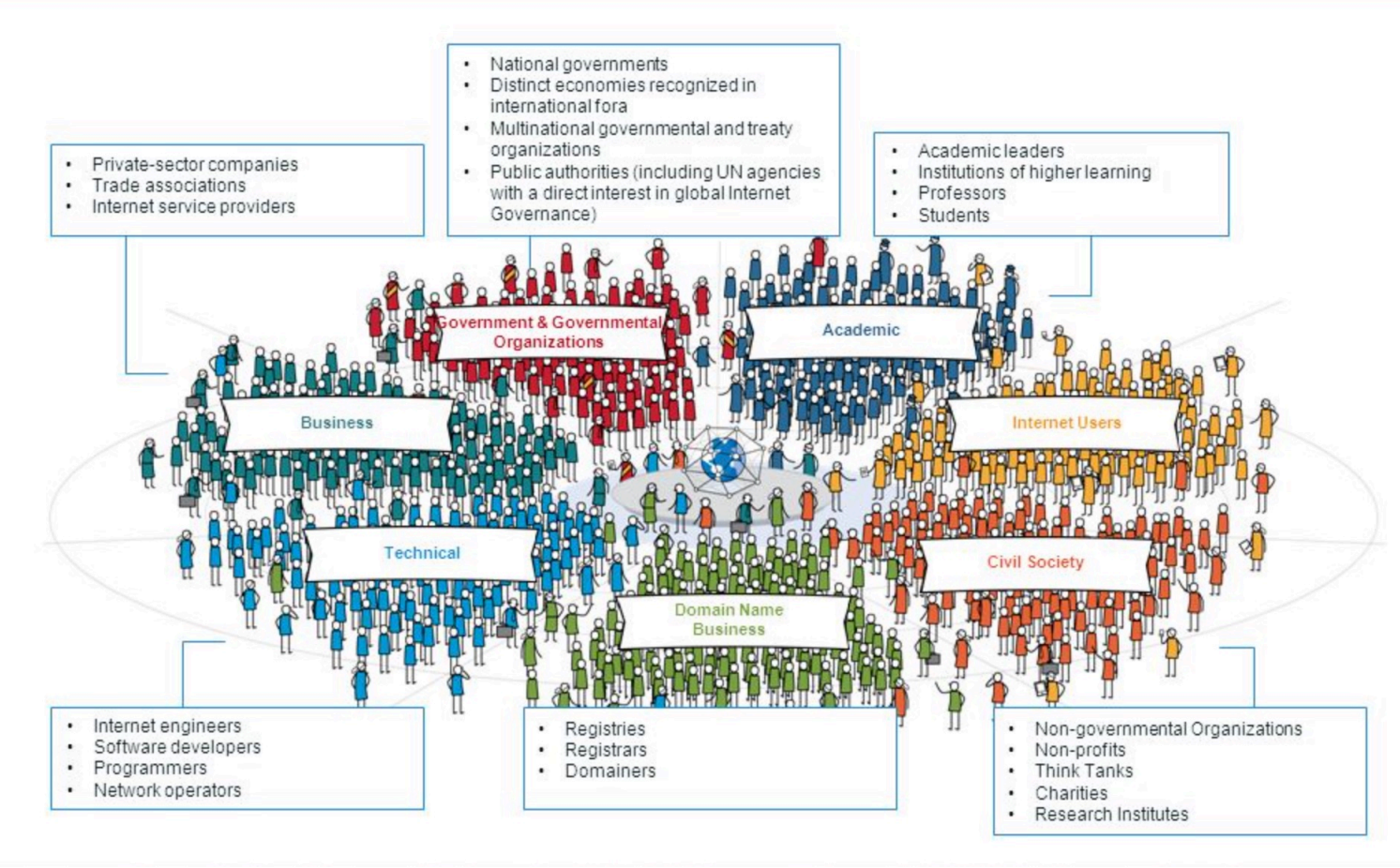

InfoWorld
FROM IDG
ICANN's DNS Apocalypse
Changes to the DNS made by ICANN's CTO David Conrad have triggered what some are calling a 'DNS Apocalypse'
ASSOCIATED PRESS
BIG STORY
TOP NEWS
SPECIAL COVERAGE
ARCHIVE
ESPAÑOL
VIDEO
RADIO
Nov 27, 4:35 PM EST
INTERNET POLL: FIRE ICANN CTO
BY JENN BRYCE
ASSOCIATED PRESS
LOS ANGELES, California. (AP) -- 43,000 netizens have
signed a petition urging the Internet Corporate
Names and Numbers
TIME
DECEMBER 12, 2016
404 ERROR
How one man managed to
LIVE
BREAKING NEWS
ICANN'S CTO BREAKS INTERNET
18:45
ELDERS OF INTERNET INCREASE BOUNTY TO $20K | PRESIDENT VOWS TO GIVE STERN

What is ICANN (for the purposes of this discussion)?

- We are a global, multi-stakeholder, bottom-up, consensus-driven organization
- We are the IANA Functions Operator
  - Rolling the root KSK is a part of the IANA Names Function
- With community and partner help:
  - We DNSSEC-signed the root in July 2010
  - We developed the KSK Rollover Plan
- We began rolling the KSK in October 2016
  - We suspended rolling the KSK in September 2017
- We do other things:
  - Create new TLDs, develop TLD policy, accredit registrars, create new RIRs, allocate blocks of numbers to the RIRs and for protocol purposes, administer the protocol parameter registries, coordinate root servers, etc.
  - Not going to talk about these

The ICANN Ecosystem

ICANN Communities



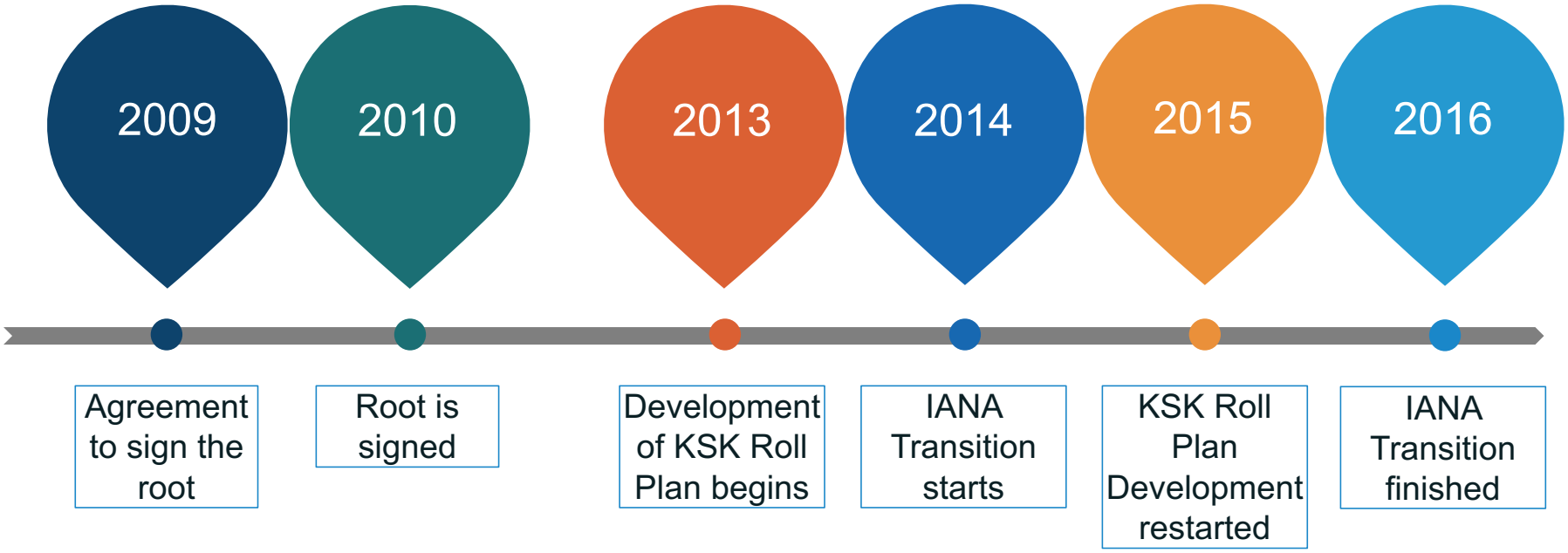
All communities get to shape ICANN's policies

- ICANN tries to describe all its policies to all its constituents so that they can participate in our policy-making
- Technical communities get to comment on:
  - Our budget
  - Our engagement with governments
  - Etc.
- Non-technical communities get to comment on:
  - Rolling the root KSK for the DNS
  - The way we manage the contents of the root zone
  - Etc.
- Predictably, this can get "interesting"
  - Diametrically opposed agendas, etc.

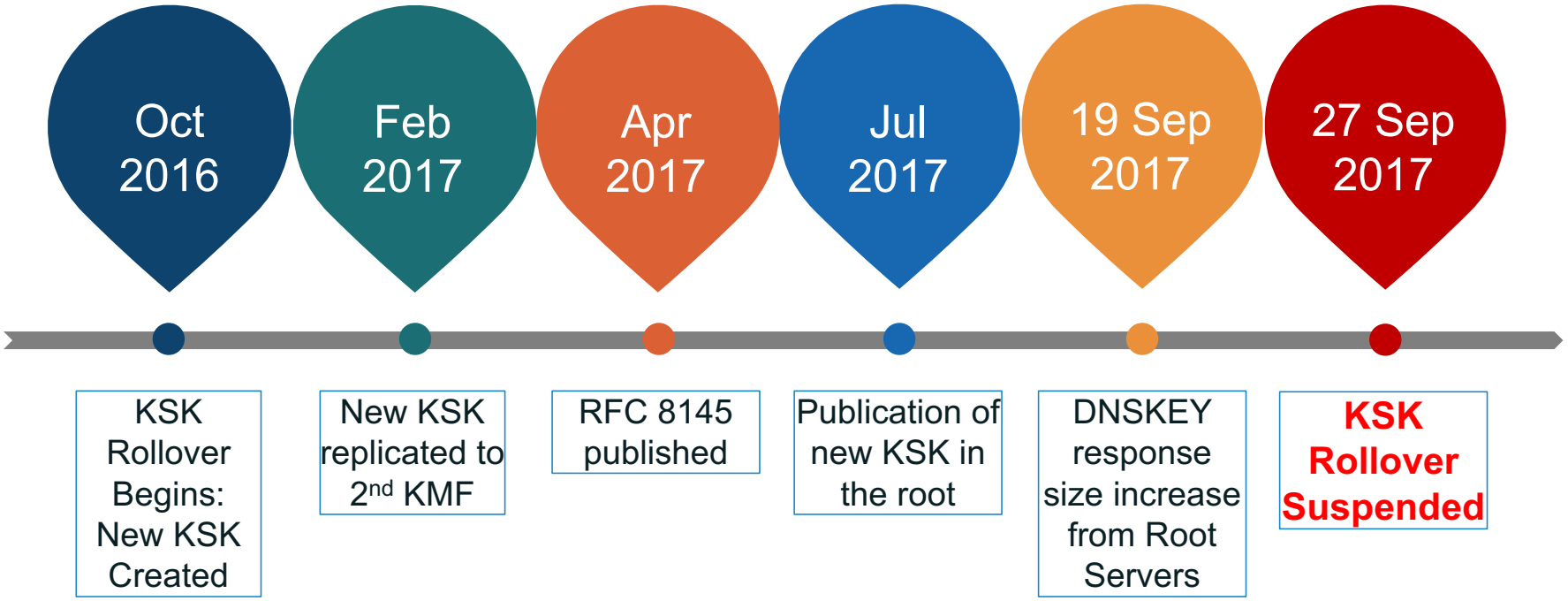
ICANN DNSSEC Work Is Community Driven

- Extensive Community input on:
  - Signing the Root
  - Development of the DNSSEC Policy Statement
  - “Trusted Community Representatives”
  - Key Ceremonies
  - Development of the KSK Rollover Plan
  - Etc.
- What is the Technical Community in this context?
  - People participating in, e.g.,
    - IETF DNSOP Working Group
    - DNS-OARC
    - DNSSEC-Deployment mailing list
    - DNSSEC-related workshops
    - ICANN Technical Advisory Committees
- Most input from the Technical Community so far

How did we get here?



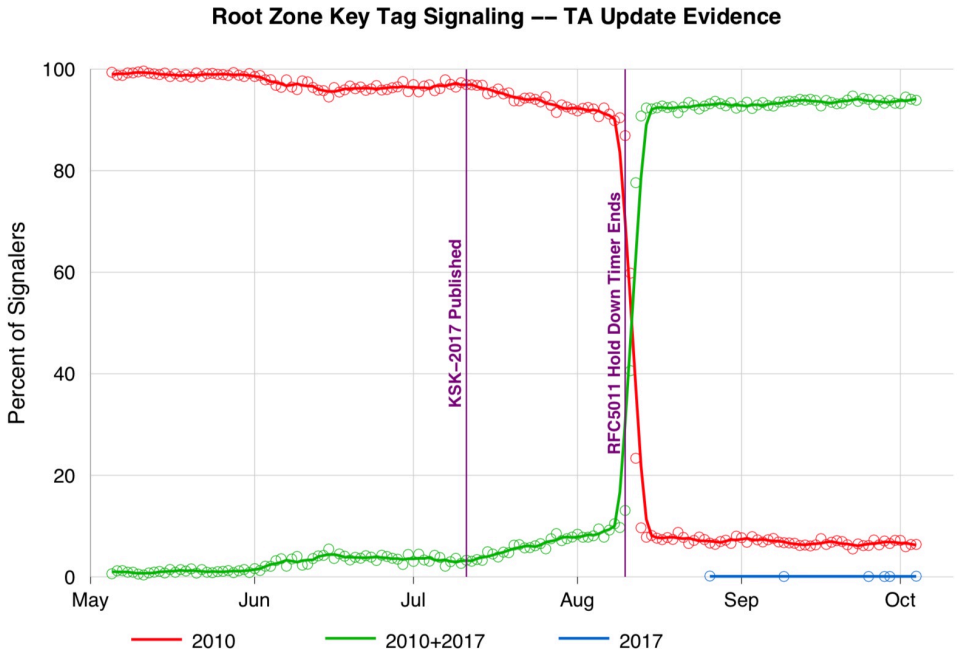
How did we get here?



So What Happened?

- **Duane Wessels of Verisign publishes RFC 8145**
- **People implement it**
- **People turn it on**
- **Duane notices something odd…**

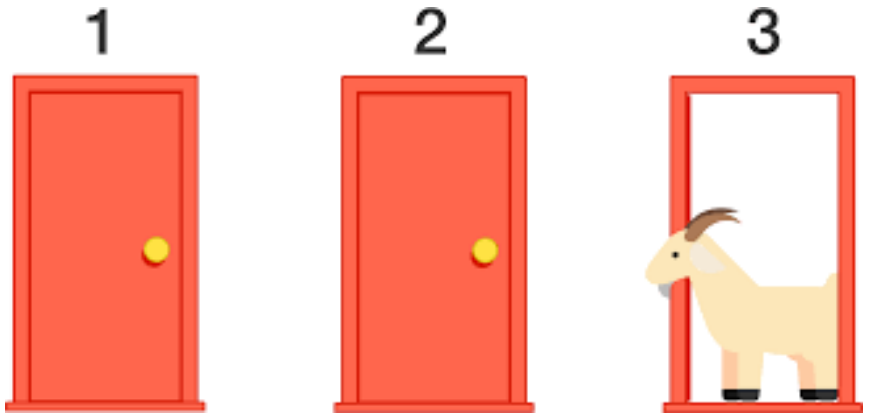
When	What
2015 December	draft-ietf-dnsop-edns-key-tag-00
2016 July	First implementation in BIND
2017 February	draft-ietf-dnsop-edns-key-tag-05
2017 April	RFC 8145
2017 April	First implementation in Unbound
2017 May	Start collecting data



Courtesy: Verisign (https://www.icann.org/en/system/files/files/rfc-8145-trust-anchor-signaling-ksk-rollover-11oct17-en.pdf)

When Faced With The Unknown…

- Possible Options
  1. Run around with hair on fire
  2. Stay the course
  3. Try to figure out what's going on



Postpone The Rollover!

- Do NOT sign the root zone with KSK-2017 yet
  - Do not remove KSK-2017
- Try to further replicate Duane's results
- Try to understand why so many resolvers have KSK-2010 only
- Figure out what to do:
  - Informally consult with the community
  - Develop a new plan
  - Formally ask for input on new plan
  - Publish new plan
- Get approval to move forward with new plan
- Roll the $#(*$&(#$ KSK

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 is *hard*
  - 20% (100 addresses) could be contacted
    - 60% in address ranges known to be dynamic IPs
    - 25% from resolvers forwarding from other resolvers
  - No “smoking gun” single cause
  - No obvious path forward
    - E.g., bug fix by resolver vendor, new communication messages, etc.

December 2017–January 2018

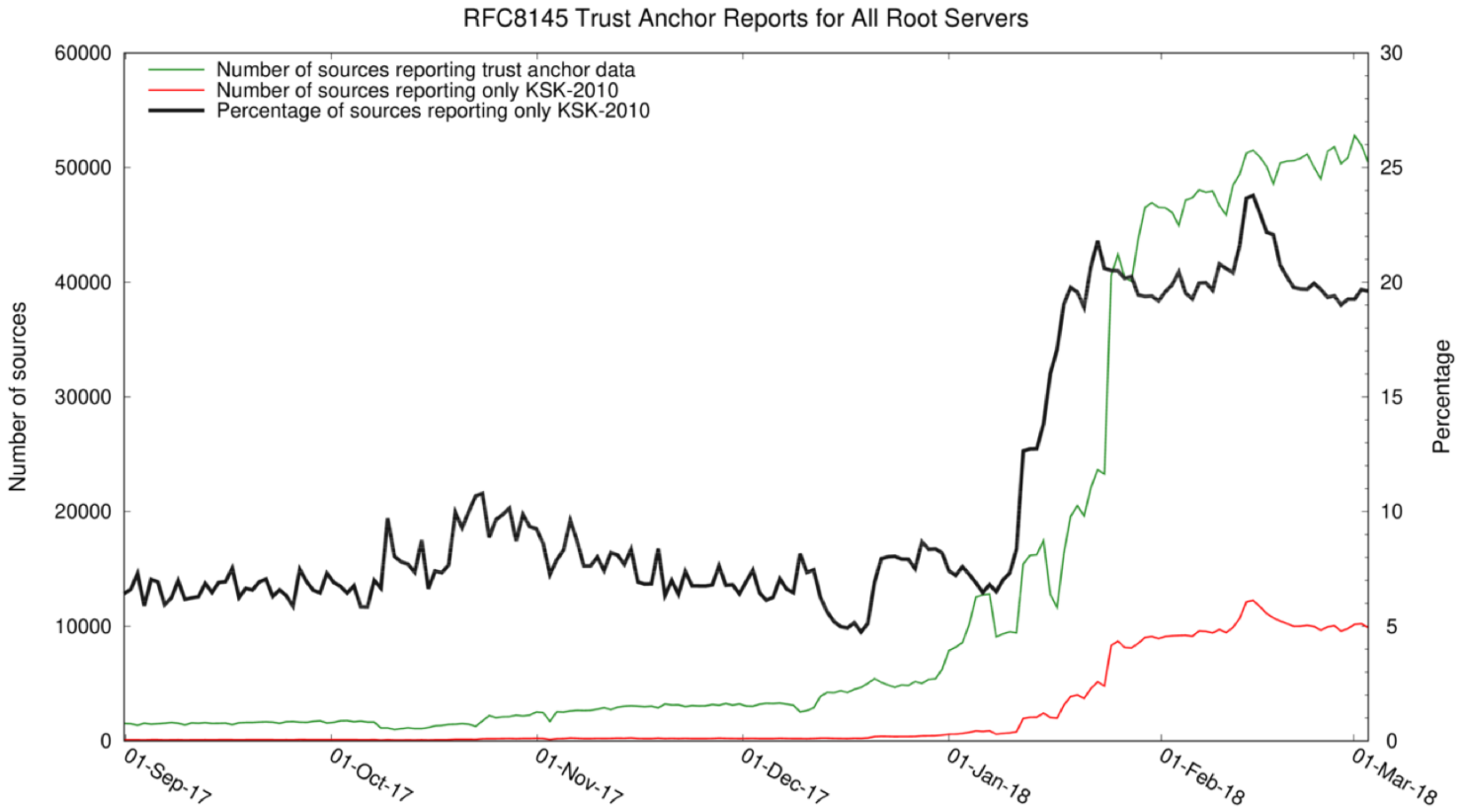
- With no clear path forward, the ICANN org decided to solicit community input
- Input and discussion on acceptable criteria for proceeding with the KSK roll took place on *ksk-rollover@icann.org*
- Results of discussion:
  - Agreement there is no way to accurately measure the number of users who would 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
- Continue collecting data

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 data from B, D, F
- Now using stats collected by Duane Wessels's excellent *rzkeychange* plug-in for *dnscap*
- Plug-in reports every 60 seconds via DNS query
  - Timestamp, resolver source IP, configured trust anchors and node ID encoded in QNAME
  - Destination is a zone operated by ICANN OCTO

```
1520174596.109-169-54-6.1._ta-4a5c-4f66.meb01.l-root.[ZONE-NAME]
1520174596.109-169-54-7.1._ta-4a5c-4f66.meb01.l-root.[ZONE-NAME]
1520174596.116-206-41-6.1._ta-4a5c.meb01.l-root.[ZONE-NAME]
1520174596.49-213-19-144.1._ta-4a5c-4f66.meb01.l-root.[ZONE-NAME]
```

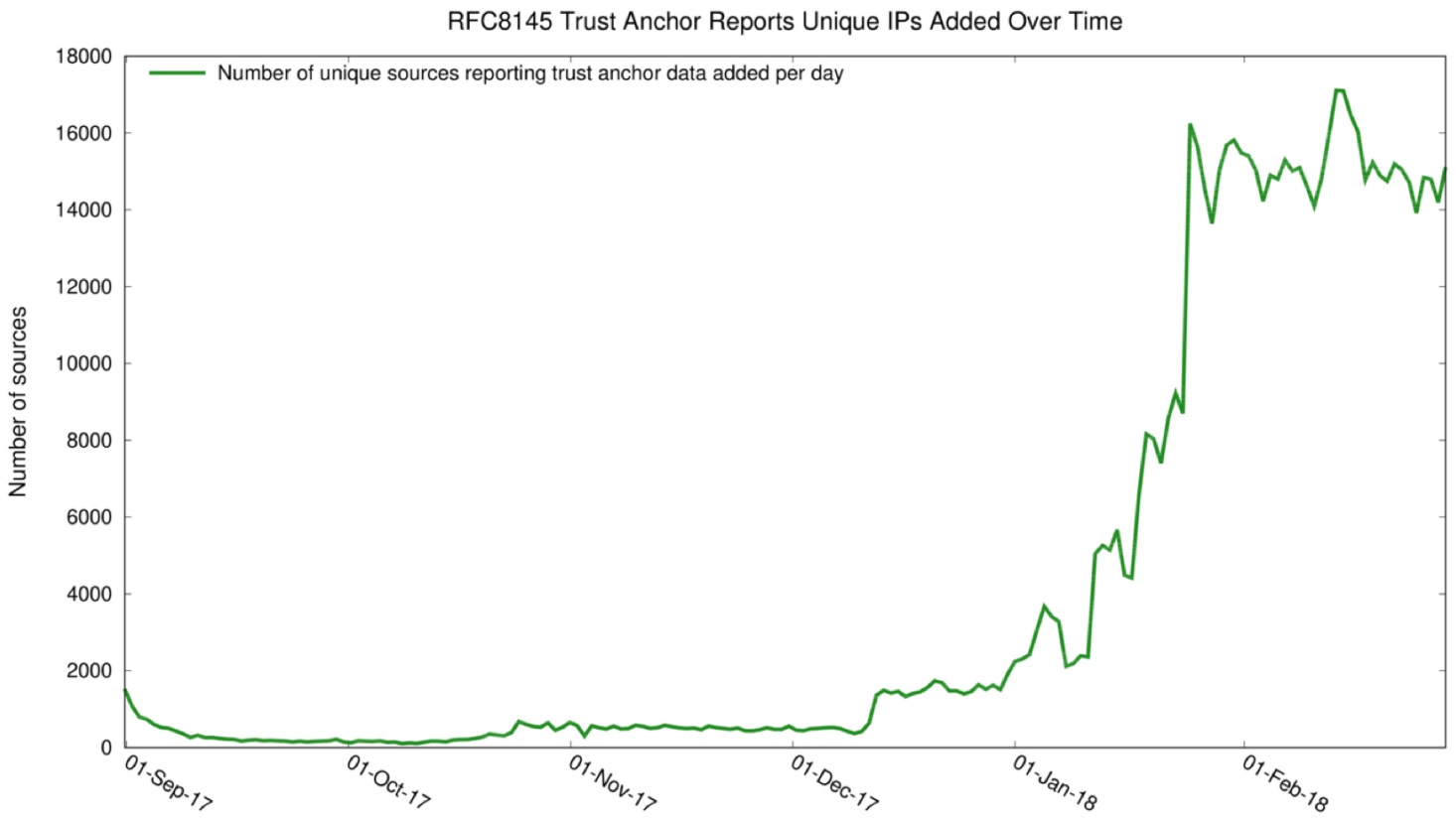
RFC8145 Data For All Root Servers



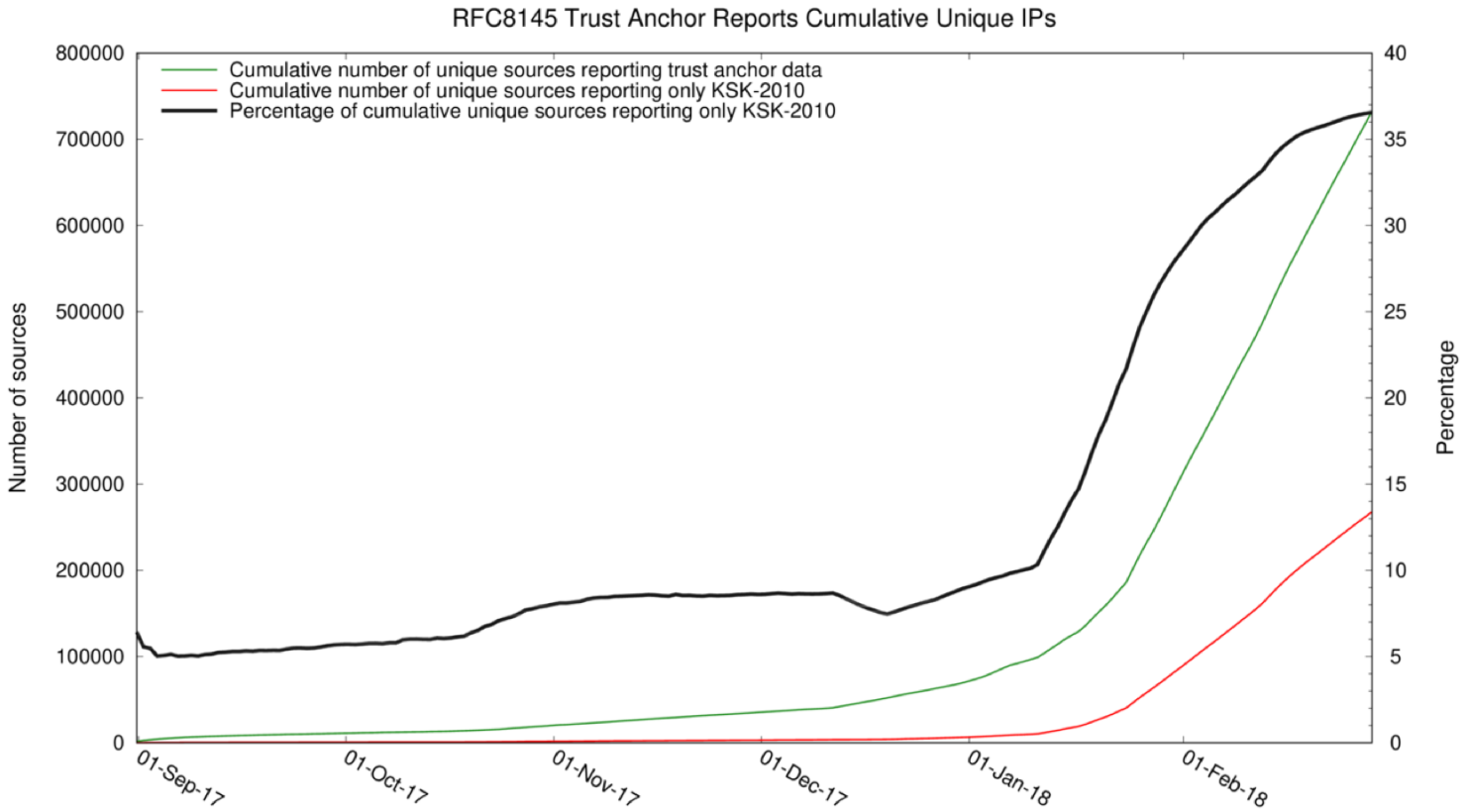
Why the Jump in January?

- 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 strong motivation to upgrade?
- But why no drop-off in KSK-2010 after 30 days?
  - Upgrade in place means *unbound-anchor* not run, so configuration might still have only KSK-2010
  - But RFC5011 support should update trust anchor store after ~30 days
- Maybe many of these are ephemeral VMs or containers?
  - They never run long enough for RFC5011 add hold-down timer to complete

Unique IPs Added Per Day



Cumulative Unique IPs Over Time

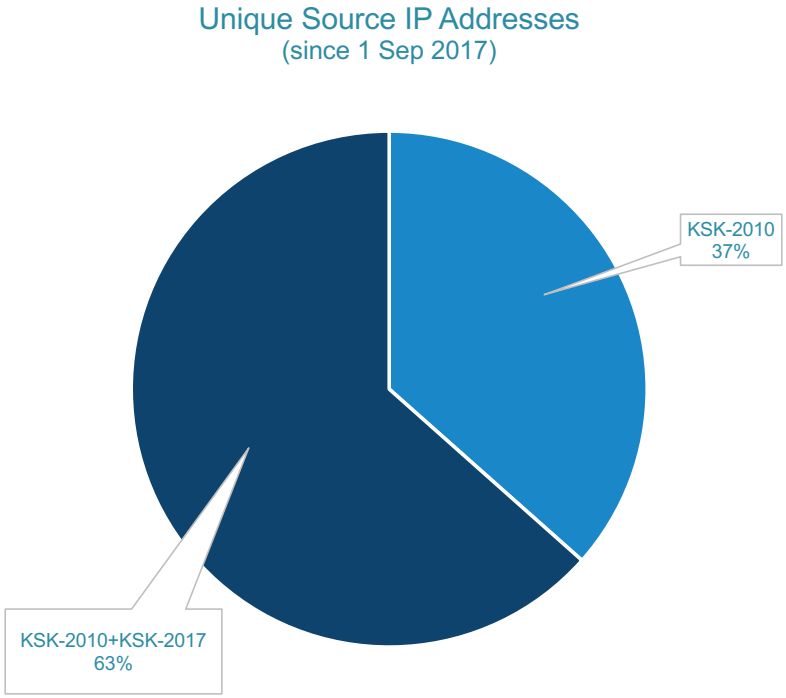


That's a Lot of Addresses

- Since 1 September 2017:

IPs reporting KSK-2010	267,815
IPs reporting KSK-2010+KSK-2017	464,701
Total	**732,516**
Total unique IPs	**730,957**
Difference	**1,559**

- Over time, some IPs report both KSK-2010 only and KSK-2010+KSK-2017
  - Forwarders?
  - Started with only KSK-2010 but then changed configuration to add KSK-2017?



Top 30 ASNs Sending RFC8145 Data

Number of sources	ASN	AS description	Country
41,462	55836	RELIANCEJIO-IN Reliance Jio Infocomm Limited	IN
22,279	3320	DTAG Internet service provider operations	DE
16,084	35819	MOBILY-AS Etihad Etisalat Company (Mobily)	SA
9,808	45609	BHARTI-MOBILITY-AS-AP Bharti Airtel Ltd. AS for GPRS Service	IN
9,761	25019	SAUDINETSTC-AS	SA
9,099	39891	ALJAWWALSTC-AS	SA
9,054	7922	COMCAST-7922 - Comcast Cable Communications, LLC	US
7,981	28885	OMANTEL-NAP-AS OmanTel NAP	OM
7,344	22394	CELLCO - Cellco Partnership DBA Verizon Wireless	US
6,858	16135	TURKCELL-AS Turkcell A.S.	TR
6,593	21928	T-MOBILE-AS21928 - T-Mobile USA, Inc.	US
6,587	43766	MTC-KSA-AS	SA
6,410	6830	LGI-UPC formerly known as UPC Broadband Holding B.V.	AT
6,142	6805	TDDE-ASN1	DE
6,042	3209	VODANET International IP-Backbone of Vodafone	DE
5,883	45595	PKTELECOM-AS-PK Pakistan Telecom Company Limited	PK
5,802	26599	TELEF√ìNICA BRASIL S.A	BR
5,211	9121	TTNET	TR
5,129	3215	AS3215	FR
5,049	50010	NAWRAS-AS Sultanate of Oman	OM
4,945	8452	TE-AS TE-AS	EG
4,704	36873	VNL1-AS	NG
4,502	20057	ATT-MOBILITY-LLC-AS20057 - AT&T Mobility LLC	US
3,996	45271	ICLNET-AS-AP Idea Cellular Limited	IN
3,886	4761	INDOSAT-INP-AP INDOSAT Internet Network Provider	ID
3,734	5384	EMIRATES-INTERNET Emirates Internet	AE
3,685	29256	INT-PDN-STE-AS STE PDN Internal AS	SY
3,678	2856	BT-UK-AS BTnet UK Regional network	GB
3,657	7303	Telecom Argentina S.A.	AR
3,619	9829	BSNL-NIB National Internet Backbone	IN

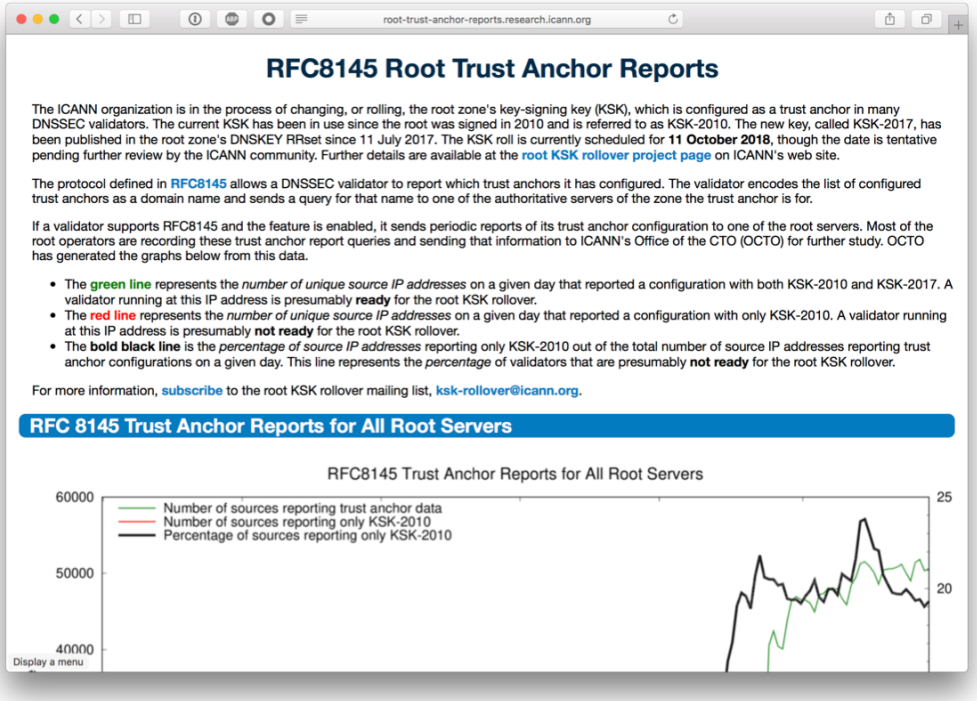
What's Next

- Continue to try to figure out what's going on
  - Given data we have
  - Ask community for (more) help
- Revise plan, based on:
  - Community input
  - The data we have
- Get formal advice from ICANN advisory committees
  - Security and Stability
  - Root Server System
- Request final approval from ICANN Board
  - Provide briefing, including formal advice from ACs

"I THINK OUR ONLY CHOICE AT THIS POINT IS TO TAKE THE NEXT BIG STEP."

Community Assistance

- http://root-trust-anchor-reports.research.icann.org
  - Updated weekly
- We have distributed a list of IP addresses reporting only KSK-2010
  - ICANN 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
- Making the list more widely available still under consideration



Moving Forward

- The ICANN org published a *draft* plan to proceed with the KSK rollover:
  - Roll 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 currently open**
  - Closes 2 April 2018
  - https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en

Root KSK Rollover Proposed Schedule *(draft)*

Date	Action
1 February	*Draft plan published, public comment opened*
10-15 March (ICANN61)	*Hold session for community feedback*
2 April	Comment period ends; revise plan, as necessary
Mid-April	Publish staff report on public comment and revised plan
10 May	Request Board resolution to ask SSAC to review and comment on the plan by 1 August
24-28 June (ICANN62)	Hold another session for community feedback
1 August	Receive SSAC feedback; revise plan, as necessary
Mid-August	Publish final plan, with message that roll is contingent on Board resolution
14 September	Request Board resolution directing ICANN org to roll the root KSK on **11 October 2018**
11 October	Rescheduled date for root KSK roll

Implications

- On 11 Oct 2018 we **know** we will break some *resolvers*
  - Currently between 20-30% as reported by RFC 8145 announcements
  - We do NOT know how many users make use of those resolvers
    - We do NOT know how many users make use of ONLY those resolvers
    - We do NOT know how many users will lose resolution service
- We **believe** most validation is done by large resolvers
  - Google Public DNS, Comcast, etc.
    - Not worried about these folks
- Measurement in operational protocols would be **very nice**
  - Measuring what we care about (e.g., users vs. resolvers)
    - **Won't happen soon**
- Final decision by ICANN Board will be non-technical
  - Without data cost/benefit analysis is hard

How You Can Help

- Turn on DNSSEC validation
  - Making sure you manage your trust anchor correctly
- Tell your network operator friends:
  - Turn on DNSSEC validation
  - Make sure they manage their trust anchor correctly
- **Provide input during the public comment per**iod
  - Closes 2 April 2018
    - 11 days
  - As of noon today (22 March)
    - 7 (seven) comments

https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: email@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann