Root KSK Rollover Update

Matt Larson
VP of Research, Office of the CTO, ICANN

ICANN 61
COMMUNITY FORUM

SAN JUAN
10–15 March 2018

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 (8,908 IPv4 and 3,078 IPv6) reporting
  - 500 reported only KSK-2010 (4.1%)
- 27 September 2017: The ICANN org postpones the root KSK roll
  - Need 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 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 “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

1 February 2018

- 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)*

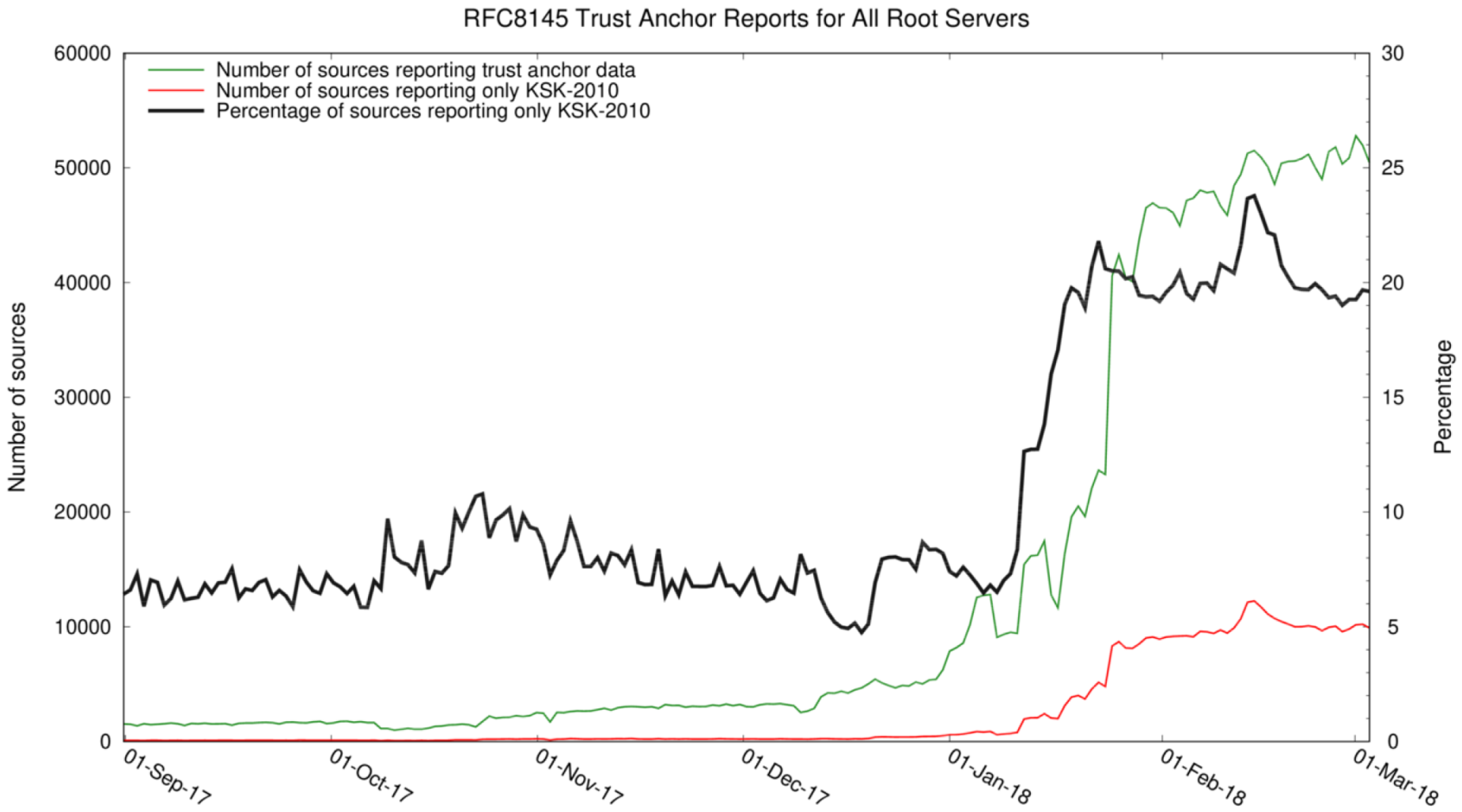
Date	Action
1 February 2018	Draft plan published, public comment opened
10-15 March (ICANN61)	Hold session for community feedback
2 April	Comment period ends; revise plan, as necessary
Mid April	Publish staff report on public comment and revised plan
10 May (Board workshop)	Request Board resolution to 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 (Board workshop)	Request Board resolution directing ICANN org to roll the root KSK on 11 October 2018
11 October 2018	Rescheduled date for root KSK roll

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]
```

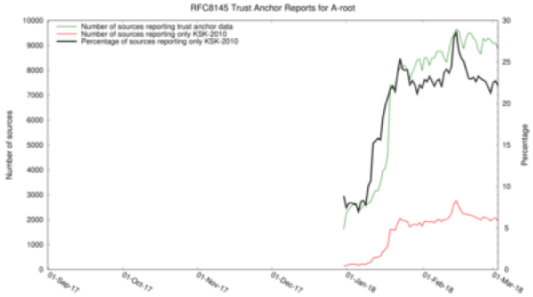
RFC8145 Data For All Root Servers

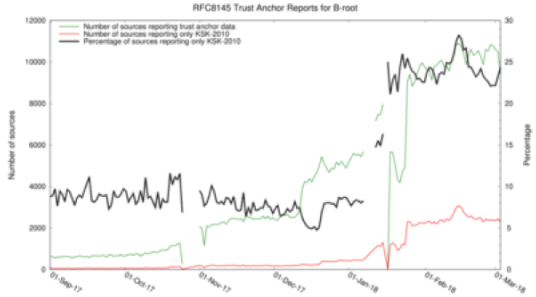


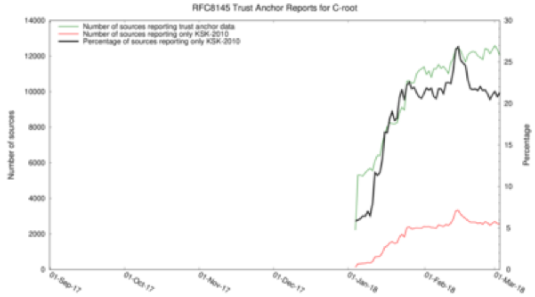
Why the Jump in January?

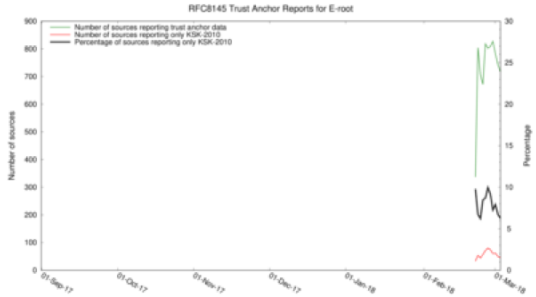
- Best hypothesis: Unbound 1.6.8 released on 19 January 2018
  - *“Fix for CVE-2017-15105: vulnerability in the processing of wildcard synthesized NSEC records”*
- Patch related to security, so perhaps strong motivation to upgrade?
- But why no drop-off in KSK-2010 after 30 days?
  - Upgrade in place 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

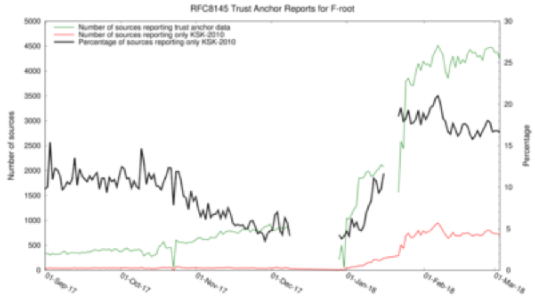
RFC8145 Data For Individual Root Servers

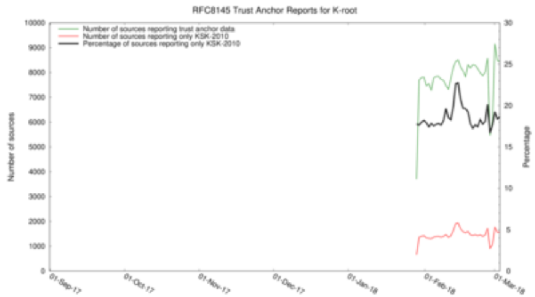




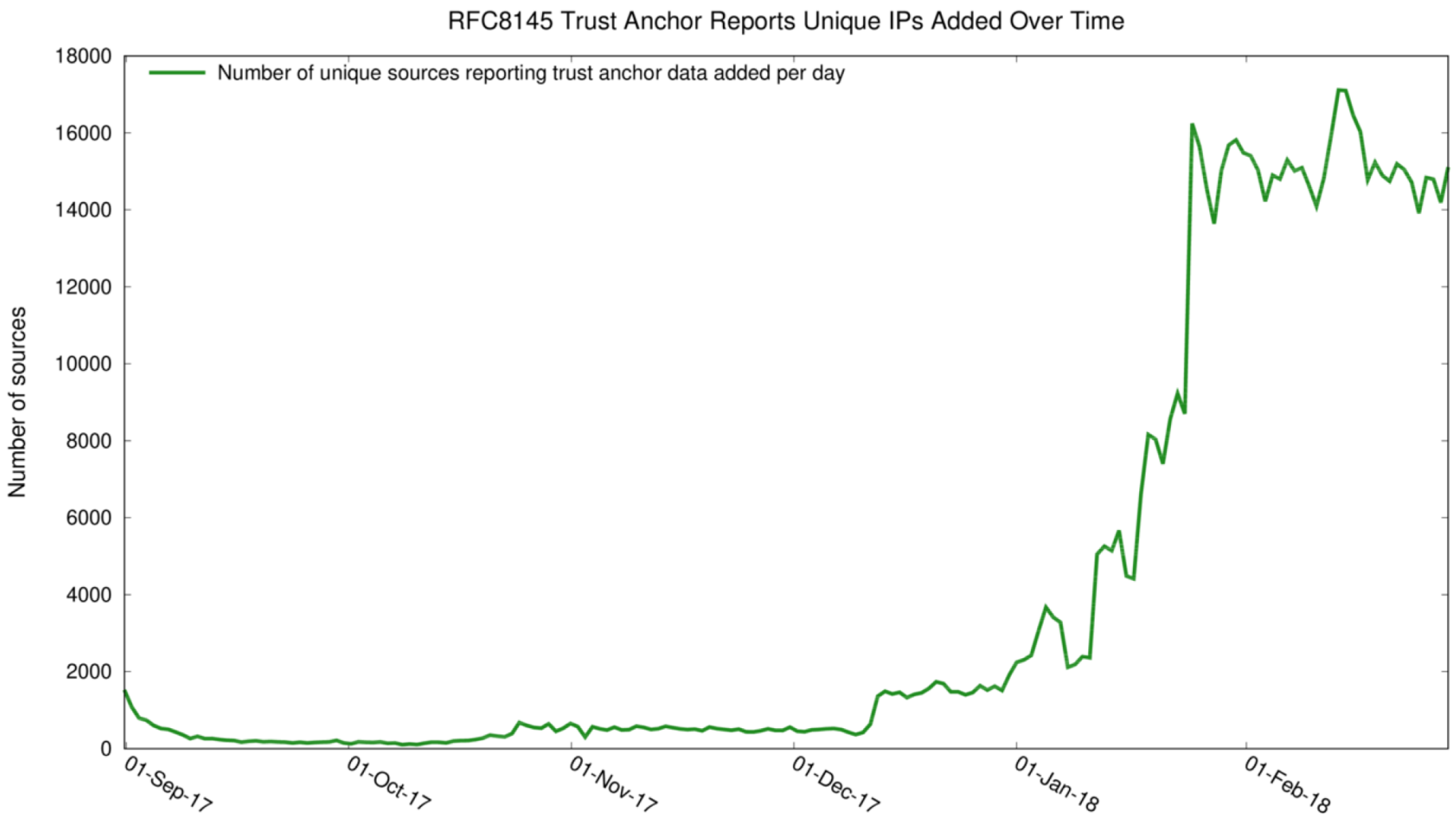




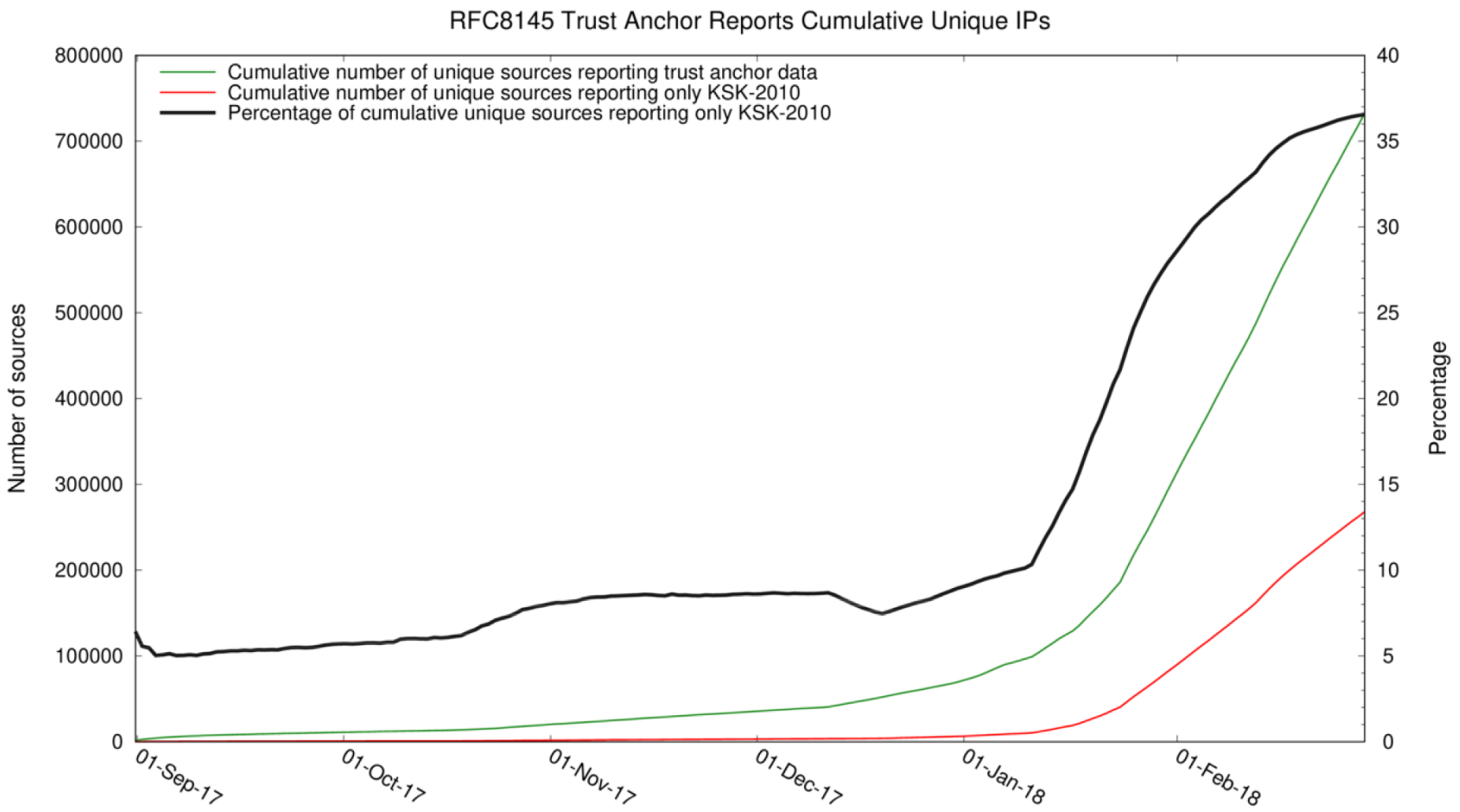




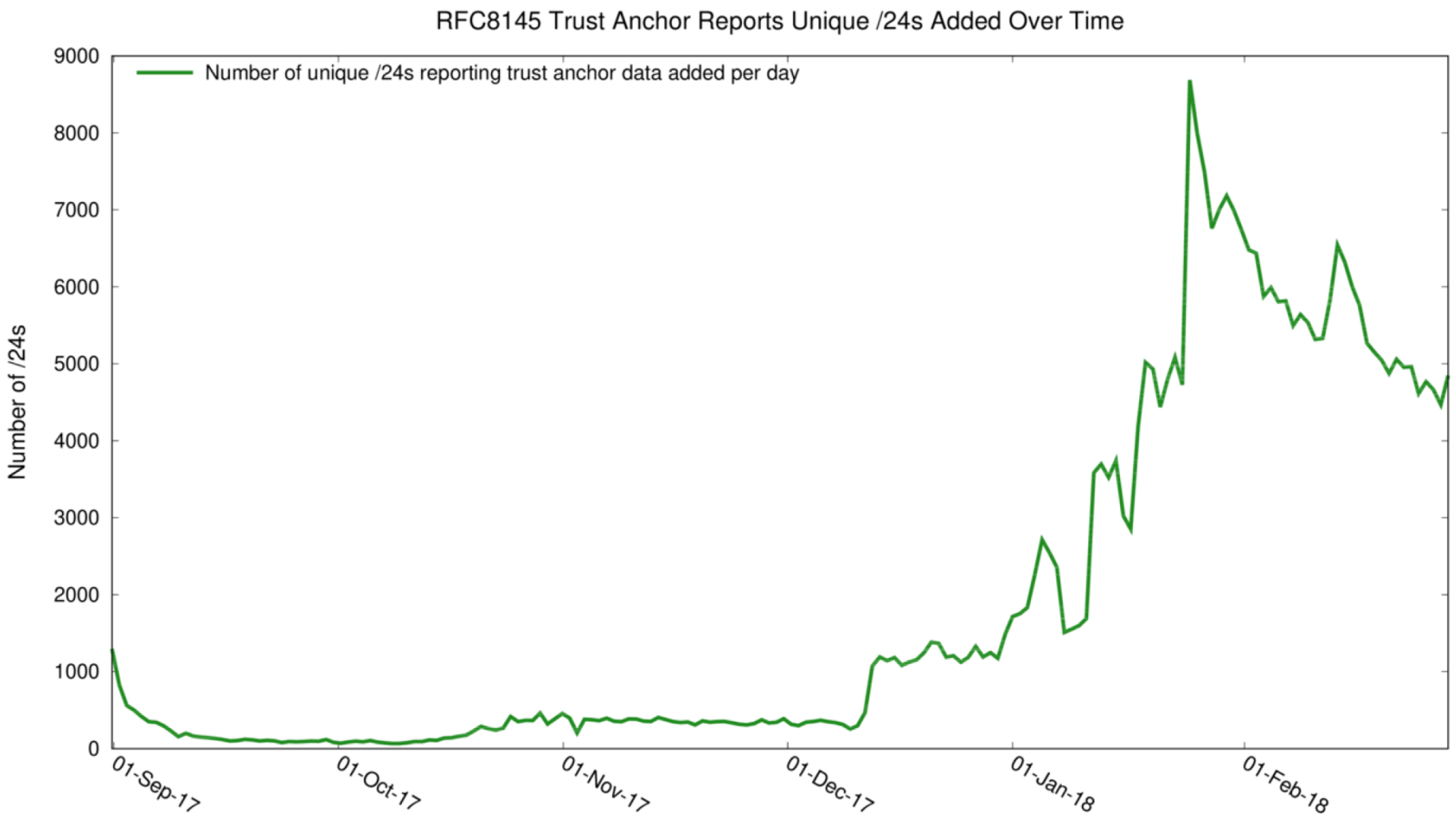
Unique IPs Added Per Day



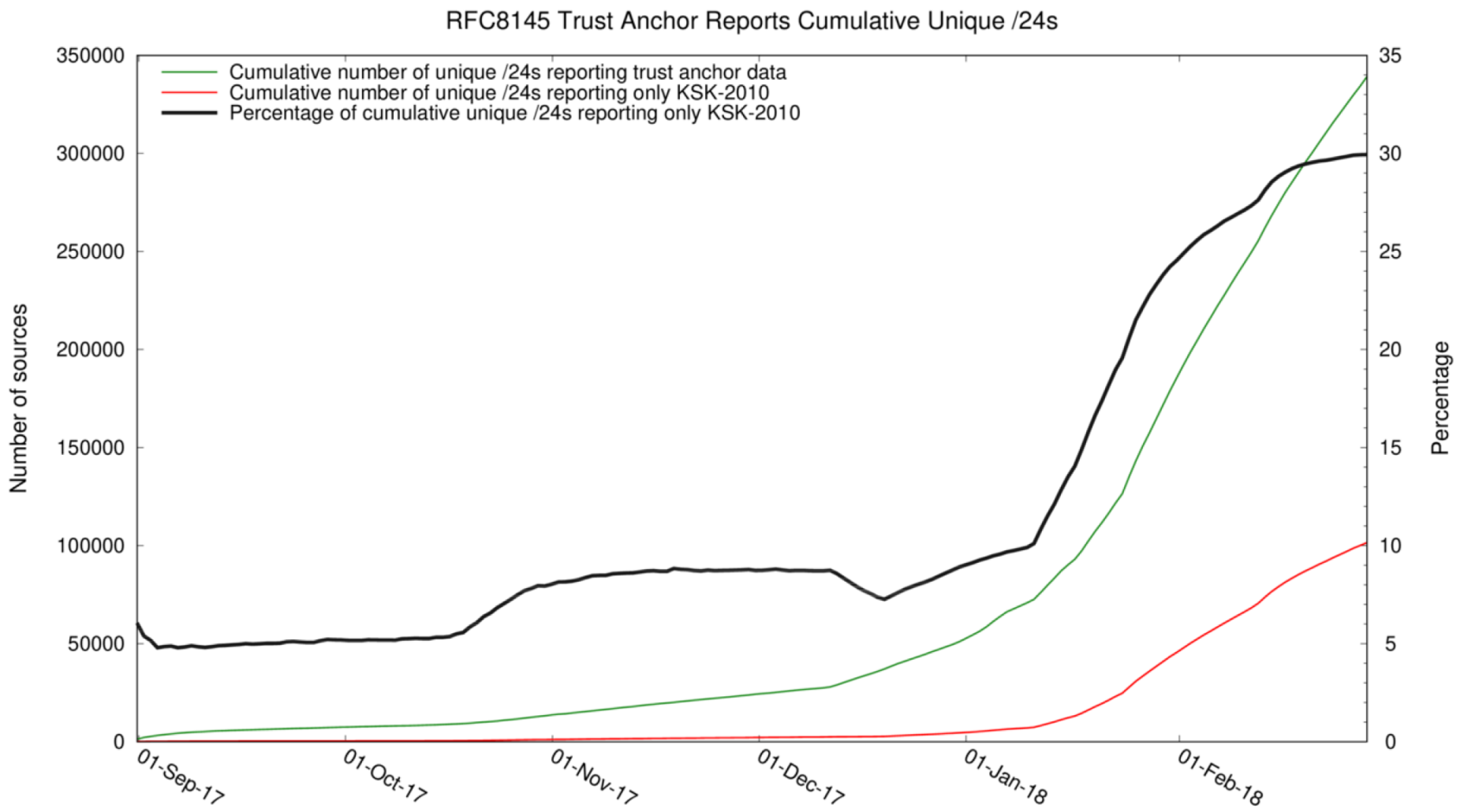
Cumulative Unique IPs Over Time



Unique /24s Added Per Day



Cumulative Unique /24s Over Time



That's a Lot of Addresses

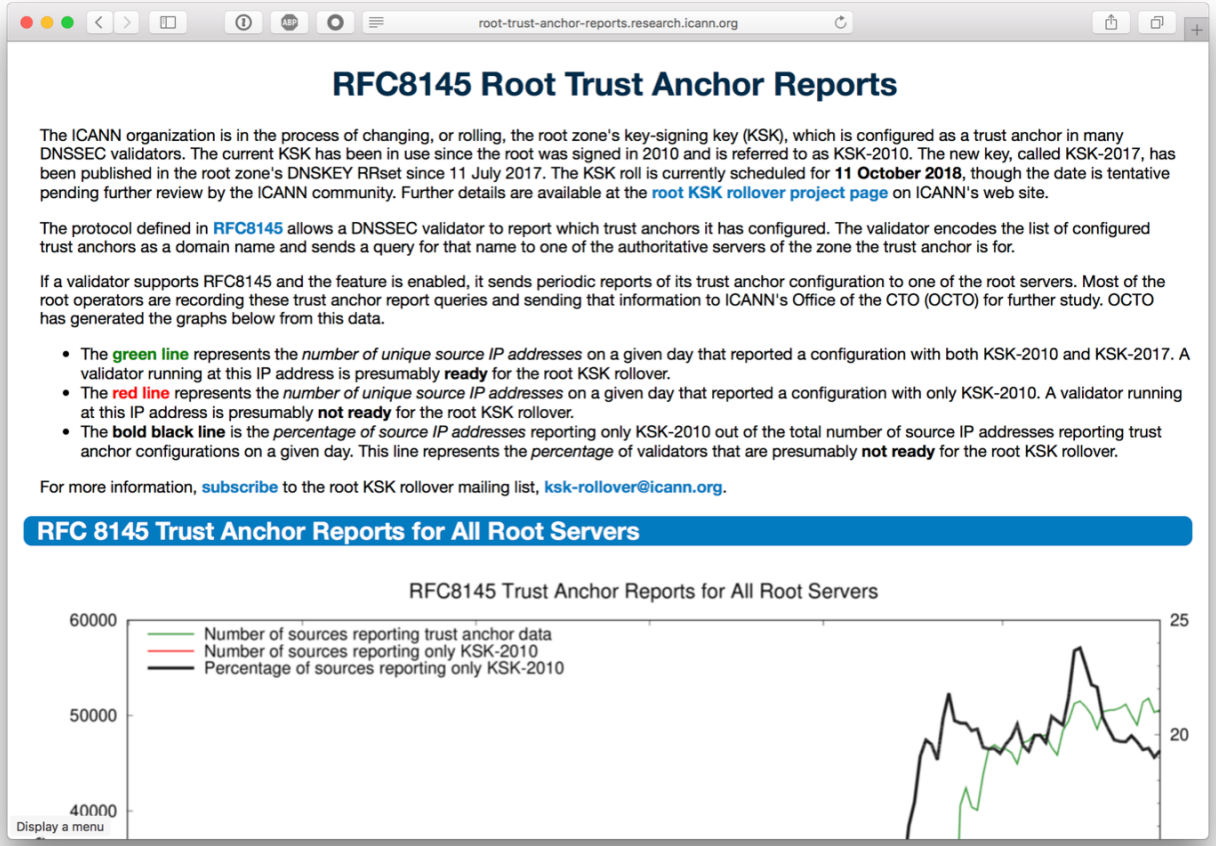
- Since 1 September 2017:

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**

- There's a difference because some IPs report both KSK-2010 and KSK-2010+KSK-2017
  - Forwarders?
  - Started with only KSK-2010 but then changed configuration to add KSK-2017?

RFC8145 Graphs Now Published

- http://root-trust-anchor-reports.research.icann.org
  - Updated weekly



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

Community Assistance

- We have distributed 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
- Making the list more widely available still under consideration

Next Steps

- Keep investigating RFC8145 data
  - Why do some roots (E, J) 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
- Keep listening to the community

How You Can Help

- Comment on the plan through the ICANN public comment process
  - Closes 2 April 2018
  - https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en
- Join the *ksk-rollover@icann.org* mailing list to stay updated

Thank You and Questions

Visit us at **icann.org**
Email: matt.larson@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann