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
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

- Community
- Organization
- Board
ICANN Communities

- Private-sector companies
  - Trade associations
  - Internet service providers

- National governments
  - Distinct economies recognized in international fora
  - Multinational governmental and treaty organizations
  - Public authorities (including UN agencies with a direct interest in global Internet Governance)

- Academic leaders
  - Institutions of higher learning
  - Professors
  - Students

- Internet users

- Business
- Technical
- Civil Society
- Domain Names
- Academic

- Domain Name Business

- Internet engineers
  - Software developers
  - Programmers
  - Network operators

- Registries
  - Registrars
  - Domainers

- Non-governmental Organizations
  - Non-profits
  - Think Tanks
  - Charities
  - Research Institutes
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?

2009
Agreement to sign the root

2010
Root is signed

2013
Development of KSK Roll Plan begins

2014
IANA Transition starts

2015
KSK Roll Plan Development restarted

2016
IANA Transition finished
How did we get here?

- **Oct 2016**: KSK Rollover Begins: New KSK Created
- **Feb 2017**: New KSK replicated to 2nd KMF
- **Apr 2017**: RFC 8145 published
- **Jul 2017**: Publication of new KSK in the root
- **19 Sep 2017**: DNSKEY response size increase from Root Servers
- **27 Sep 2017**: KSK Rollover Suspended
So What Happened?

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

<table>
<thead>
<tr>
<th>When</th>
<th>What</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015 December</td>
<td>draft-ietf-dnsop-edns-key-tag-00</td>
</tr>
<tr>
<td>2016 July</td>
<td>First implementation in BIND</td>
</tr>
<tr>
<td>2017 February</td>
<td>draft-ietf-dnsop-edns-key-tag-05</td>
</tr>
<tr>
<td>2017 April</td>
<td>RFC 8145</td>
</tr>
<tr>
<td>2017 April</td>
<td>First implementation in Unbound</td>
</tr>
<tr>
<td>2017 May</td>
<td>Start collecting data</td>
</tr>
</tbody>
</table>

Root Zone Key Tag Signaling — TA Update Evidence

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.
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

RFC8145 Trust Anchor Reports for All Root Servers

Number of sources reporting trust anchor data
Number of sources reporting only KSK-2010
Percentage of sources reporting only KSK-2010

Number of sources
Percentage
01-Sep-17 01-Oct-17 01-Nov-17 01-Dec-17 01-Jan-18 01-Feb-18 01-Mar-18
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

RFC8145 Trust Anchor Reports Unique IPs Added Over Time

Number of unique sources reporting trust anchor data added per day

Number of sources

01-Sep-17  01-Oct-17  01-Nov-17  01-Dec-17  01-Jan-18  01-Feb-18
Cumulative Unique IPs Over Time

RFC8145 Trust Anchor Reports Cumulative Unique IPs

- Cumulative number of unique sources reporting trust anchor data
- Cumulative number of unique sources reporting only KSK-2010
- Percentage of cumulative unique sources reporting only KSK-2010

Number of sources

0 100000 200000 300000 400000 500000 600000 700000 800000

01-Sep-17 01-Oct-17 01-Nov-17 01-Dec-17 01-Jan-18 01-Feb-18

Percentage

0 5 10 15 20 25 30 35 40
That’s a Lot of Addresses

- Since 1 September 2017:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IPs reporting KSK-2010</td>
<td>267,815</td>
</tr>
<tr>
<td>IPs reporting KSK-2010+KSK-2017</td>
<td>464,701</td>
</tr>
<tr>
<td>Total</td>
<td>732,516</td>
</tr>
<tr>
<td>Total unique IPs</td>
<td>730,957</td>
</tr>
<tr>
<td>Difference</td>
<td>1,559</td>
</tr>
</tbody>
</table>

- 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

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 February</td>
<td><em>Draft plan published, public comment opened</em></td>
</tr>
<tr>
<td>10-15 March (ICANN61)</td>
<td><em>Hold session for community feedback</em></td>
</tr>
<tr>
<td>2 April</td>
<td>Comment period ends; revise plan, as necessary</td>
</tr>
<tr>
<td>Mid-April</td>
<td>Publish staff report on public comment and revised plan</td>
</tr>
<tr>
<td>10 May</td>
<td>Request Board resolution to ask SSAC to review and comment on the plan by 1 August</td>
</tr>
<tr>
<td>24-28 June (ICANN62)</td>
<td>Hold another session for community feedback</td>
</tr>
<tr>
<td>1 August</td>
<td>Receive SSAC feedback; revise plan, as necessary</td>
</tr>
<tr>
<td>Mid-August</td>
<td>Publish final plan, with message that roll is contingent on Board resolution</td>
</tr>
<tr>
<td>14 September</td>
<td>Request Board resolution directing ICANN org to roll the root KSK on <strong>11 October 2018</strong></td>
</tr>
<tr>
<td>11 October</td>
<td>Rescheduled date for root KSK roll</td>
</tr>
</tbody>
</table>
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 period
  - Closes 2 April 2018
    - 11 days
  - As of noon today (22 March)
    - 7 (seven) comments

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