Root Zone DNSSEC Key Signing Key Rollover

Champika Wijayatunga | APTLD71 | Ho Chi Minh City | Mar 2, 2017
What is the purpose of this talk?

1. To publicize the new Root Zone DNSSEC KSK
2. Provide status, upcoming events, and contact information
3. Provide helpful resources on the KSK roll
What is 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 configuration parameter in DNS validating revolvers.
DNSSEC Key Management in the Root Zone

- Multi-stakeholder, bottom-up trust model* /w 21 crypto officers from around the world
- Broadcast Key Ceremonies and public docs
- SysTrust audited

*Managed by technical community+ICANN
Why Change the KSK?

• Primary reason – Operational Preparedness
  – KSK has no expiration date, currently no weakness
  – No key should live forever: bad crypto practice
  – DNSSEC Practice Statement states the key will be rolled
  – Prefer to exercise process in normal conditions
    • As opposed to abnormal, such as key compromise

• Big challenge
  – Involves countless/uncountable participants
  – No test environment can cover all possibilities
What are the rollover’s milestones?

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation of KSK-2017</td>
<td>October 27, 2016</td>
</tr>
<tr>
<td>Production Qualified</td>
<td>February 2, 2017</td>
</tr>
<tr>
<td>Out-of-DNS-band Publication</td>
<td>Now, onwards</td>
</tr>
<tr>
<td>In-band <em>(Automated Updates)</em> Publication</td>
<td>July 11, 2017 onwards</td>
</tr>
<tr>
<td>Sign (Production Use)</td>
<td>October 11, 2017 onwards</td>
</tr>
<tr>
<td>Revoke KSK-2010</td>
<td>January 11, 2018</td>
</tr>
<tr>
<td>Remove KSK-2010 from systems</td>
<td>Dates TBD, 2018</td>
</tr>
</tbody>
</table>
Bottom Line

• Changing the root KSK will impact just about all DNSSEC validations (15% worldwide)
• If the trust anchor is "misconfigured" (i.e., the wrong key) DNSSEC will reject legitimate responses
• To anyone or any process relying on DNS, it will appear that the desired data is unavailable, website is unreachable, "the Internet is down"
What You Need to Know

- **Manage Your Trust Anchors**
  - Be aware of your software tools for managing trust anchors
  - Be aware of the new KSK

- **When Events Happen**
  - Keep an eye on dates
  - Be mindful of when changes are scheduled and monitor appropriately
To help ensure trouble-free Internet access for their users, Internet service providers, enterprise network operators and others who have enabled DNSSEC validation must update their systems with the public part of the new KSK (the root “trust anchor”)

- Available from https://www.iana.org/dnssec/files

Key dates of the process when end users may experience interruption in Internet services:

- **19 September, 2017**
  Size increase for DNSKEY response from root name servers

- **11 October, 2017 – Most important date**
  New KSK used for signing for the first time

- **11 January, 2018**
  The old KSK is revoked
How can you engage with ICANN?

Thank You and Questions

Join the ksk-rollover@icann.org mailing list
Archives: https://mm.icann.org/listinfo/ksk-rollover
KSK-Roll Website: https://www.icann.org/kskroll

Twitter: twitter.com/icann
Facebook: facebook.com/icannorg
YouTube: youtube.com/user/icannnews
LinkedIn: linkedin.com/company/icann

Soundcloud: soundcloud.com/icann
Weibo: weibo.com/ICANNorg
Flickr: flickr.com/photos/icann
Slideshare: slideshare.net/icannpresentations

Follow #Keyroll