Rolling the Root Zone DNSSEC Key Signing Key *Lightning Talk*

Roy Arends | RIPE 73 | October 2016

Motivation for this talk

- ICANN is about to change an important configuration parameter in DNSSEC
- Plan documents are available for your information
- This is an update to KSK roll presentations given in the DNS WG meetings of RIPE 70, 71, and 72

DNSSEC in the Root Zone

- DNSSEC in the Root Zone is managed by:
  - ICANN, responsible for operating the root KSK
    - "signs the KSK & ZSK”
  - Verisign, responsible for operating the root ZSK
    - "signs the root zone”

- The current root KSK was created in 2010
  - A 2048 bits, RSASHA256 key
    - These parameters do not change

Why change the current Root KSK?

- Good cryptographic hygiene
  - Secrets don't remain secret forever
- Good operational hygiene
  - Have a plan, complete enough to execute
  - Exercise the plan under normal circumstances
- Promised to do so in a policy statement in 2010
  - “Each RZ KSK will be scheduled to be rolled over through a key ceremony as required, or after 5 years of operation.”

The KSK Roll Plan Documents

- Available at: https://www.icann.org/kskroll
  - 2017 KSK Rollover Operational Implementation Plan
  - 2017 KSK Rollover Monitoring Plan
  - 2017 KSK Rollover Back Out Plan
  - 2017 KSK Rollover Systems Test Plan
  - 2017 KSK Rollover External Test Plan

- We encourage interested folks to given them a read

Dates to Watch

- September 19, 2017
  - The root zone DNSKEY set will increase to 1414 bytes for 20 days, prior to that date 1139 bytes has been the high water mark

- **October 11, 2017**
  - The root zone DNSKEY set will *only* be signed by the new KSK
  - If preparations haven't been made, trouble will ensue

- January 11, 2018
  - The root zone DNSKEY set will increase to 1425 bytes for 20 days

Tools & Testbeds

- We are working with DNS software and tool developers and distributors
  - Management/troubleshooting aids
  - Updates of bundled keys
- Testbeds for Code Developers
  - Automated updates: *http://keyroll.systems/*
  - Root zone model: *https://www.toot-servers.net/*
- Testbeds for Service Operators
  - I.e., using "off-the-shelf" parameters
  - Planned for end-of-2016

For More Information

- Join the ksk-rollover@icann.org mailing list:
  - https://mm.icann.org/listinfo/ksk-rollover

- Follow on Twitter
  - @ICANN
  - Hashtag: #KeyRoll

- Visit the web page:
  - https://www.icann.org/kskroll

Engage with ICANN

Thank You and Questions

Reach me at:
Email: ksk-rollover@icann.org
Website: icann.org/kskroll

twitter.com/icann

gplus.to/icann

facebook.com/icannorg

weibo.com/ICANNorg

linkedin.com/company/icann

flickr.com/photos/icann

youtube.com/user/icannnews

slideshare.net/icannpresentations