Rolling the Root Zone DNSSEC Key Signing Key
Dr. Richard Lamb | November 2016 richard.lamb@icann.org
Motivation for this talk

• ICANN is about to change an important configuration parameter in DNSSEC

• For a network operator, this may create a need for action

• This discussion is meant to inform: Why this is happening, what is happening, and when
  • Highlighting: the availability of project plan documents
Do Class Exercise Here
Current Root KSK

- The current root KSK was created in 2010
  - Stored in Hardware Security Modules in two Key Management Facilities
  - The operations surrounding the key is an entirely different talk (21 trusted community representatives, multi-person controls, key ceremonies, 3rd party audit.)
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.”

* [https://www.iana.org/dnssec/icann-dps.txt](https://www.iana.org/dnssec/icann-dps.txt) Section 6.5
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"
• The KSK Rollover Plan Documents

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

• We encourage interested folks to given them a read
Overview of Project Plans

• The new KSK was created on October 27, 2016
• Expect new KSK to be install on backup site Feb 2017
Upcoming 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**
  • On this date the root zone DNSKEY set will be signed only by the new KSK

• **January 11, 2018**
  • The root zone DNSKEY set will increase to 1425 bytes for 20 days
Operational Implementation Plan Timeline

Phase A - Generation
Phase B - Replication
Phase C - First SKR
Phase D - Publication
Phase E - Rollover
Phase F - Revocation

- 2016 Q4
- 2017 Q1
- 2017 Q2
- 2017 Q3
- 2017 Q4
- 2018 Q1

Slot 1.9  Slot 1.9  Slot 1  Slot 2.8  Slot 9  Slot 1  Slot 2.8  Slot 9  Slot 1  Slot 2.8  Slot 9

... normal ZSK publishing ...
ZSK-earlier
ZSK-q1  ZSK-q1  ZSK-q1
post-publish

ZSK-q2
pre-publish
ZSK-q2  ZSK-q2  ZSK-q2
post-publish

ZSK-q3
pre-publish
ZSK-q3  ZSK-q3  ZSK-q3

... normal KSK-2010 publishing and signing ...

KSK-2010 publish+sign  KSK-2010 publish+sign  KSK-2010 publish+sign  KSK-2010 publish+sign  KSK-2010 publish+sign  KSK-2010 publish+sign  KSK-2010 publish+sign  KSK-2010 publish+sign

KSK-2010 publish+sign  KSK-2010 publish+sign  KSK-2010 publish+sign  KSK-2010 publish+sign  KSK-2010 publish+sign  KSK-2010 publish+sign  KSK-2010 publish+sign  KSK-2010 publish+sign


First SKR with KSK-2017 signed
First packet size increase
Second packet size increase
Rollover
Delayed revocation of KSK-2010

KSK-2017 created in 1st KMF
KSK-2017 replicated to 2nd KMF
Trust Anchor Management

• How do you trust and configure?
  • Are trust anchors subject to configuration control?
  • Rely on embedded data in software?
  • Are DNSSEC validation failures monitored?

• Automated Updates of DNSSEC Trust Anchors
  • Most direct, reliable means for getting the key

• Negative Trust Anchor management – RFC 7646
  • Protects against errors made by others
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
facebook.com/icannorg
linkedin.com/company/icann
youtube.com/user/icannnews

gplus.to/icann
weibo.com/ICANNorg
flickr.com/photos/icann
slideshare.net/icannpresentations

Engage with ICANN