KSK Rollover

Andrea Beccalli
Stakeholder Engagement Director

ESNOG
10 April 2018

SK Rollover: An Overview

ICANN is in the process of performing a Root Zone DNS Security Extensions (DNSSEC) Key Signing Key (KSK) rollover

- The Root Zone DNSSEC Key Signing Key "**KSK**" is the top most cryptographic key in the DNSSEC hierarchy
- The KSK is a cryptographic public-private key pair:
  - Public part: trusted starting point for DNSSEC validation
  - Private part: signs the Zone Signing Key (ZSK)
- Builds a "chain of trust" of successive keys and signatures to validate the authenticity of any DNSSEC signed data

Watch video:

Why is ICANN Rolling the KSK?

- As with passwords, the cryptographic keys used in DNSSEC-signing DNS data should be changed periodically
  - Ensures infrastructure can support key change in case of emergency
- This type of change has never before occurred at the root level
  - There has been one functional, operational Root Zone DNSSEC KSK since 2010
- The KSK rollover must be widely and carefully coordinated to ensure that it does not interfere with normal operations

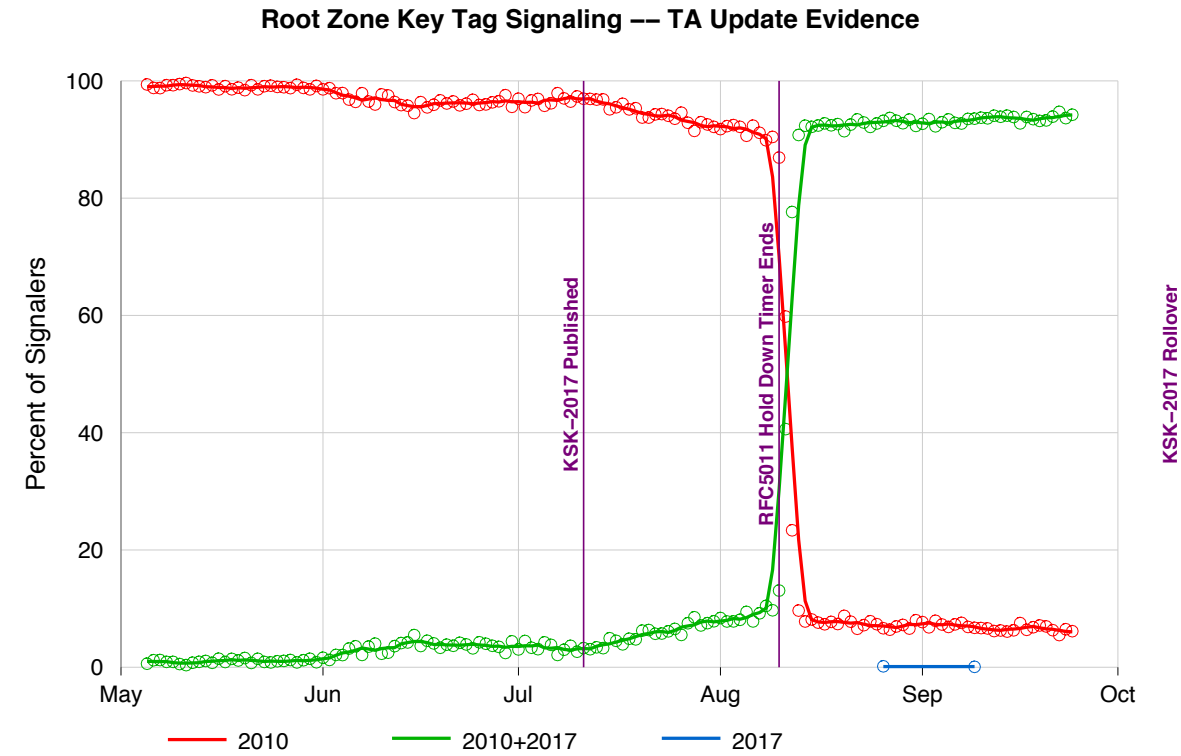
Background

- When you validate DNSSEC signed DNS records, you need a Trust Anchor.
  - A Trust Anchor is a Public Key.
- Public Keys should not live forever.
- These Trust Anchors probably should be periodically renewed (rolled).
  - You can do this automatically or manually.
- However, there was no way for us (ICANN) to check if you have the right key configured.
- Therefore, a multi-year design and outreach effort ensued:
  - Design-team, blogs, outreach, presentations in various venues, plans, vendors and governments were contacted, etc., etc.

he Process

- **11 July 2017**: Introduce the new KSK-2017.
  - Monitor if there are fundamental changes in root-server traffic
  - If not, continue, else fall back.
- **10 August 2017**: “30 day hold-down period ends”
  - Monitor if there are fundamental changes in root-server traffic.
  - If not, continue, else fall back.
- **19 September 2017**: DNSKEY Response size increased due to standard ZSK roll
  - Monitor if there are fundamental changes in root-server traffic.
  - If not, continue, else fall back.

The timeline in a graph



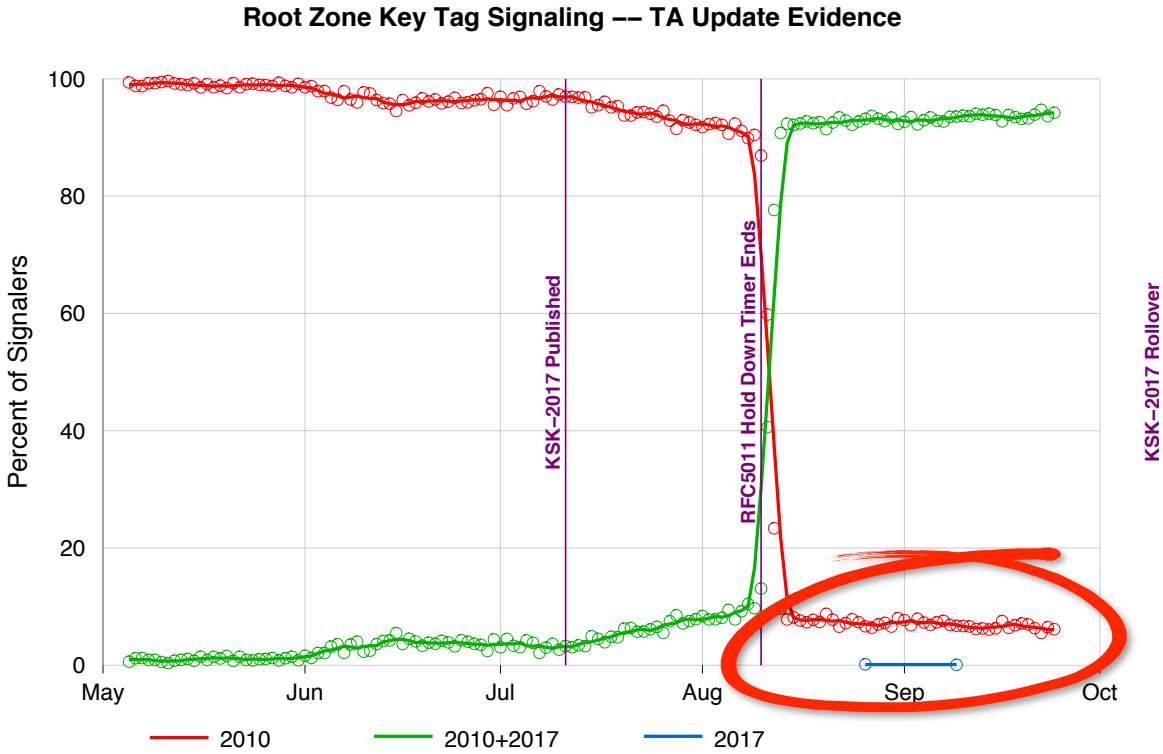
Who has KSK-2017 configured as a trust anchor?

- Until very recently, there was no way to know which trust anchors validators have configured
- *Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)* is a recent protocol extension that can provide that information
  - Reports trust anchor key tags via EDNS option or DNS query
  - Published as RFC 8145 (April 2017)
- Implementations
  - BIND 9.11 starting with 9.11.0b3 (28 July 2016)
  - BIND 9.10 starting with 9.10.5b1 (11 January 2017)
  - Unbound 1.6.4 (27 June 2017)
  - On by default in BIND (since 28 July 2016) and in Unbound since version 1.6.7 (10 October 2017)
  - No other known implementations

ooking for key tag signaling

- RFC 8145 is so new and validator support so limited that the root KSK roll project team did not expect to get enough data to help with the first root KSK Roll.
  - On average, there are 4.2 Million unique addresses sending queries to root-servers.
  - Given typical deployment curves, it was assumed the dataset would be too small to statistically represent all validating resolvers.
- However…
  - Before the introduction of KSK-2017, RFC8145-able resolvers would send KSK-2010 only.
  - After the hold down period of 30 days, RFC8145-able resolvers would send both KSK-2010 and KSK-2017.
  - Duane Wessels (Verisign, co-author of 8145) started looking at A & J root traffic for this signaling

Hey! There's data! Wait. What?



urther analysis by OCTO Research

- ICANN OCTO Research did an analysis similar to Duane's
  - Analyzed query data from B, D, F and L root servers
  - For the entire month of September and October (until the 24th)
- Results:
  - Total number of unique addresses reporting key tag data: **27,084** (out of 4.2 million, 0.57%)
  - Total number that only ever reports KSK-2010: **1631**
  - **6.02% of reporting validators were not ready for the KSK roll on 11 October 2017**
  - Non-zero percentage of reporting validators were announcing **only** KSK-2017 (?!)
- Analysis is complicated
  - Dynamic resolver IPs make the situation look worse by inflating true number of sources
  - Resolvers behind forwarders make the situation look better as they obscure multiple validators behind the forwarder

Why do validators report just KSK-2010?

- Multiple reasons suspected or confirmed:
  1. BIND reports trust anchors even if not validating
  2. Old configurations pre-dating automatic update support
     - E.g., BIND's *trusted-keys* instead of *managed-keys* or *dnssec-validation auto*
  3. Bugs in automatic update or key tag signaling support
     - E.g., announce key tags even if DNSSEC not enabled (DO=0)
  4. Operator error
     - E.g., Docker container keeps booting up with only KSK-2010 and starts 5011 all over again
- We always knew old configurations would be an issue but never had objective data until now
- We worried bugs and operator error were possible but didn't have evidence until now
- Analysis is ongoing
  - Hired a contractor to try to figure out reasons for misconfiguration

ack to the plan and process

- 19 September 2017: DNSKEY Response size increased due to standard ZSK roll
  - Monitor if there are fundamental changes in root-server traffic.
  - If not, continue, else fall back.
- We had received Verisign's report and corroborated it with our own data.
- From the Operational Plan:

  "*The Root Zone Management Partners might also decide to extend any phase for additional quarters. For example, if new information indicates that the next phase may lead to complications, the current phase would be prolonged. This is referred to as an extend scenario.*"
- 27 September 2017: "Extend" scenario kicks in
  - ICANN Announces that the root KSK Rollover is delayed

ssues

- We do not know how representative the set of validators reporting key tag data is compared to the set of all validators
- Validators != end users (or “end systems”), and the impact on end users is what is most important
  - The design team recognized this
- Determining number of end users/systems for a given resolver is hard
  - APNIC’s Google Ad experiment platform-based data will help
- Mitigation is hard
  - We’ve already had a multi-year campaign to reach operators
  - Implementation-specific problems don’t make the problem easier

ey roll

- We postponed the root KSK rollover in September 2017 until we could gather more information and understand the situation better
- Study & Analysis conducted August 2017-February 2018
- Public comment period launched on 1 February 2018 through 1 April 2018 on revised date (11 October 2018)
- Comments have been limited but few respondents in favor of going forward with key roll

Who Will Be Impacted?

DNS Software Developers & Distributors

System Integrators

Network Operators

Root Server Operators

Internet Service Providers

End Users
(if no action taken by resolver operators)

Why You Need to Prepare

If you have enabled DNSSEC validation, you must update your systems with the new KSK to help ensure trouble-free Internet access for users

- Currently, 25 percent of global Internet users, or **750 million people**, use DNSSEC-validating resolvers that could be affected by the KSK rollover
- If these validating resolvers do not have the new key when the KSK is rolled, end users relying on those resolvers will encounter errors and be **unable to access the Internet**

What Do Operators Need to Do?

Be aware whether DNSSEC is enabled in your servers

Be aware of how trust is evaluated in your operations

Test/verify your set ups

Inspect configuration files, are they (also) up to date?

If DNSSEC validation is enabled or planned in your system

- Have a plan for participating in the KSK rollover
- Know the dates, know the symptoms, solutions

ow To Update Your System

If your software supports automated updates of DNSSEC trust anchors (RFC 5011):

- The KSK will be updated automatically at the appropriate time
- You do not need to take additional action
  - Devices that are offline during the rollover will have to be updated manually if they are brought online after the rollover is finished

If your software does not support automated updates of DNSSEC trust anchors (RFC 5011) or is not configured to use it:

- The software's trust anchor file must be manually updated
- The new root zone KSK is now available here after March 2017:

Root Anchors ▶

data.iana.org/ root-anchors/

heck to See If Your Systems Are Ready

Text in the
box isn't co
check

ICANN is offering a **test bed** for operators or any interested parties to confirm that their systems handle the automated update process correctly.

Check to make sure your systems are ready by visiting:
go.icann.org/KSKtest

Automated Trust Anchor Update Testbed

The root zone Key Signing Key (KSK) is changing, or rolling, on 11 October 2017. Operators of recursive resolvers with DNSSEC validation enabled will need to ensure that their systems are updated with the new root zone KSK configured as a trust anchor before that date. If a recursive resolver supports RFC 5011, "Automated Updates of DNS Security (DNSSEC) Trust Anchors", and this feature is properly configured, the new KSK should automatically be installed as a trust anchor and DNSSEC validation should continue without problems.

If a validating resolver's implementation or configuration of the RFC 5011 automated trust anchor update protocol is incorrect for any reason, then its configuration might not be properly updated during the root zone KSK roll and resolution would fail after 11 October 2017.

This testbed allows operators of validating resolvers to test their implementation and confirm its ability to properly follow a KSK roll and update its trust anchor configuration.

This test protocol assumes that you understand **the upcoming KSK change**, and at least some about **RFC 5011**.

Purpose of This Testbed

The test system described here allows the operator of a validating recursive resolver to test its support for the RFC 5011 automated trust anchor update protocol and therefore its readiness for the root zone KSK roll. The test operates in real time and should not affect the resolver's normal operation. The testbed works by starting a KSK roll in a new zone each week. These test zones are not used for any other purpose. For example, the current zone name is 2017-03-26.automated-ksk-test.research.icann.org. Because this zone is used only for the testbed and contains no names any

hree Steps to Recovery

If your DNSSEC validation fails after the key role:

Stop the tickets

It's OK to turn off DNSSEC validation while you fix (but remember to turn it back on!)

Debug

If the problem is the trust anchor, find out why it isn't correct

- Did RFC 5011 fail? Did configuration tools fail to update the key?
- If the problem is fragmentation related, make sure TCP is enabled and/or make other transport adjustments

Test the recovery

Make sure your fixes take hold

or More Information

Join the conversation online

- Use the hashtag #KeyRoll
- Sign up to the mailing list https://mm.icann.org/listinfo/ksk-rollover

Ask a question to globalsupport@icann.org

- Subject line: “KSK Rollover”

Attend an event

- Visit https://features.icann.org/calendar to find upcoming KSK rollover presentations in your region

Learn more ▶

https://icann.org/kskroll

One World, One Internet

Visit us at **icann.org**


@icann


facebook.com/icannorg

youtube.com/icannnews


flickr.com/icann


linkedin/company/icann


slideshare/icannpresentations


soundcloud/icann