KSK Rollover Update

David Conrad, CTO

ICANN 59 – ccNSO Members Meeting
26 June 2017

KSK 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

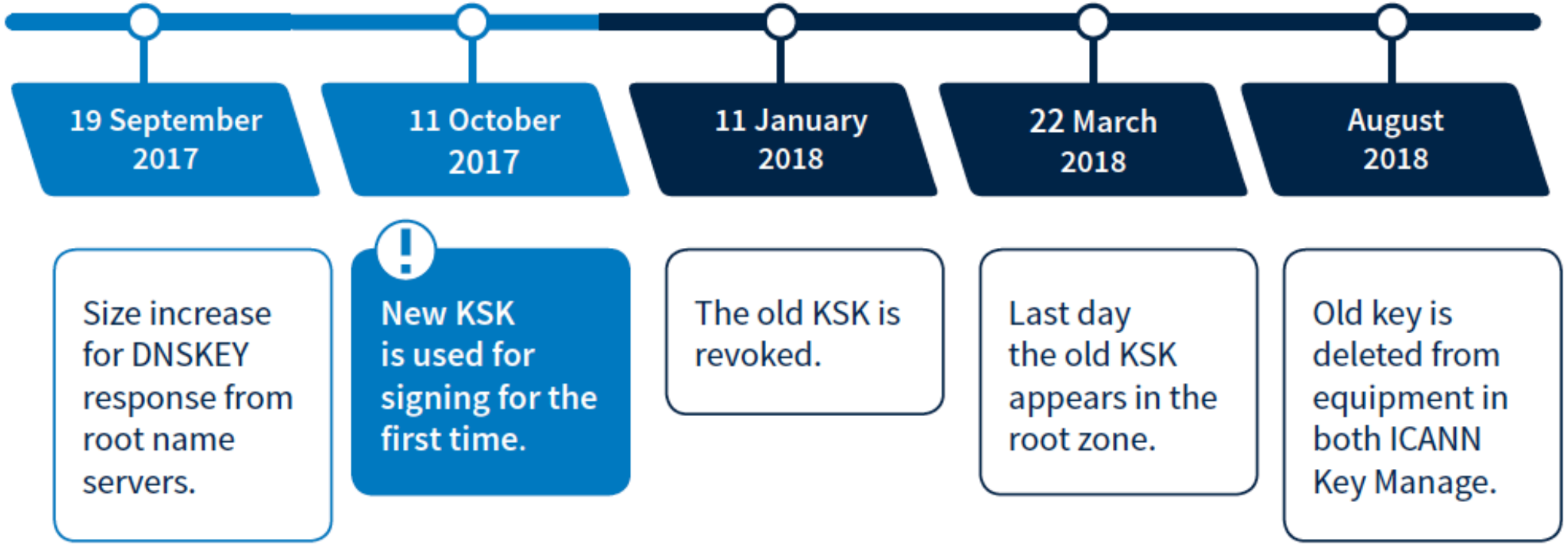
Why is ICANN Rolling the KSK?

- 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

When Does the Rollover Take Place?

The KSK rollover is a process, not a single event

The following dates are key milestones in the process when end users may experience interruption in Internet services:



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 Resolver 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

- Make sure trust anchor can be changed

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

How 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 <u>not</u> 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:

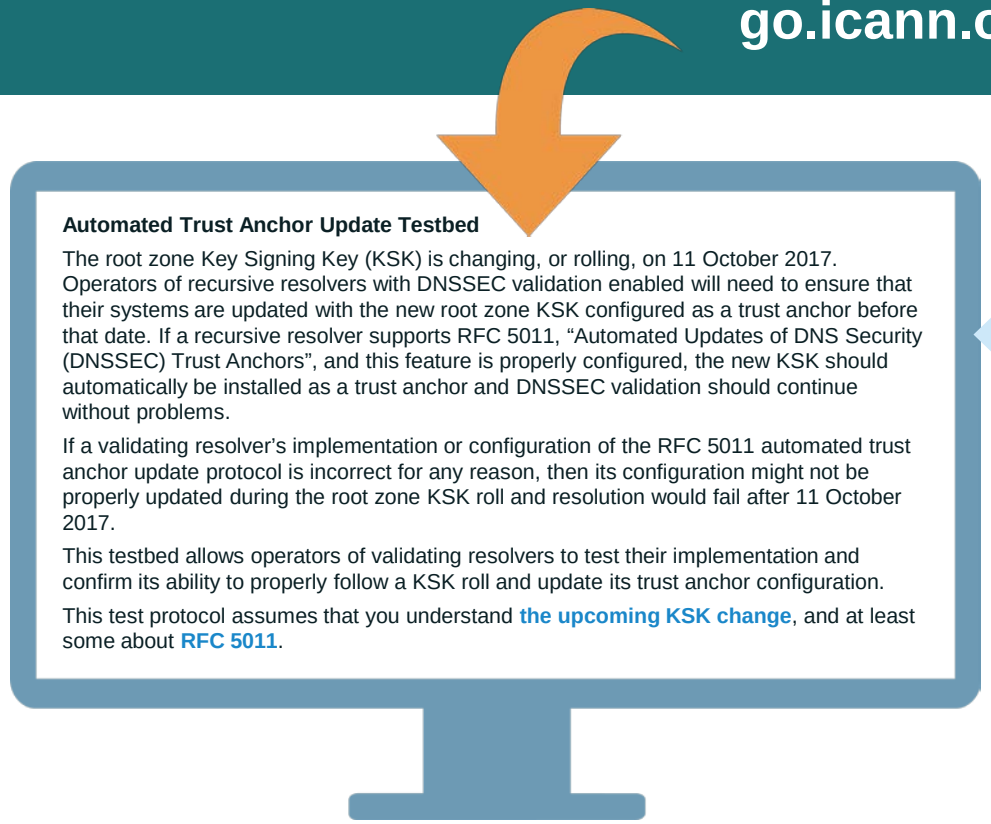
Root Anchors ▶

data.iana.org/ root-anchors/

Check to See If Your Systems Are Ready

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



Purpose of This Testbed

- Allow resolver operator to test RFC 5011 support
  - Operates in real time.
  - Should not affect the resolver's normal operation.

The testbed starts a KSK roll in a new zone each week. For example, the current zone name is 2017-06-25.automated-ksk-test.research.icann.org.

Three 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

Our “Ask” of you

- Use ICANN’s testing platform to confirm that your validating infrastructure supports the ability to handle the rollover without manual intervention.
  - Platform at go.icann.org/KSKtest
- Help us increase awareness of the key change throughout your communities.
  - Awareness will assure the roll goes smoothly

For 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

Engage with ICANN – Thank You and Questions

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