



# **DNSSEC: Important Update**

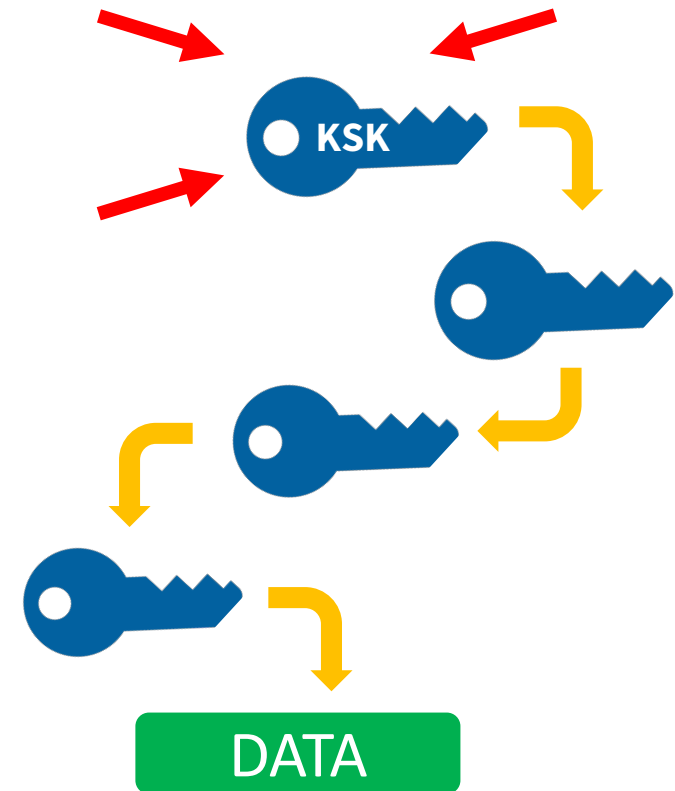
## ***Root Zone DNSSEC KSK Rollover***

Edward Lewis, Senior Technologist, ICANN  
22 May 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?

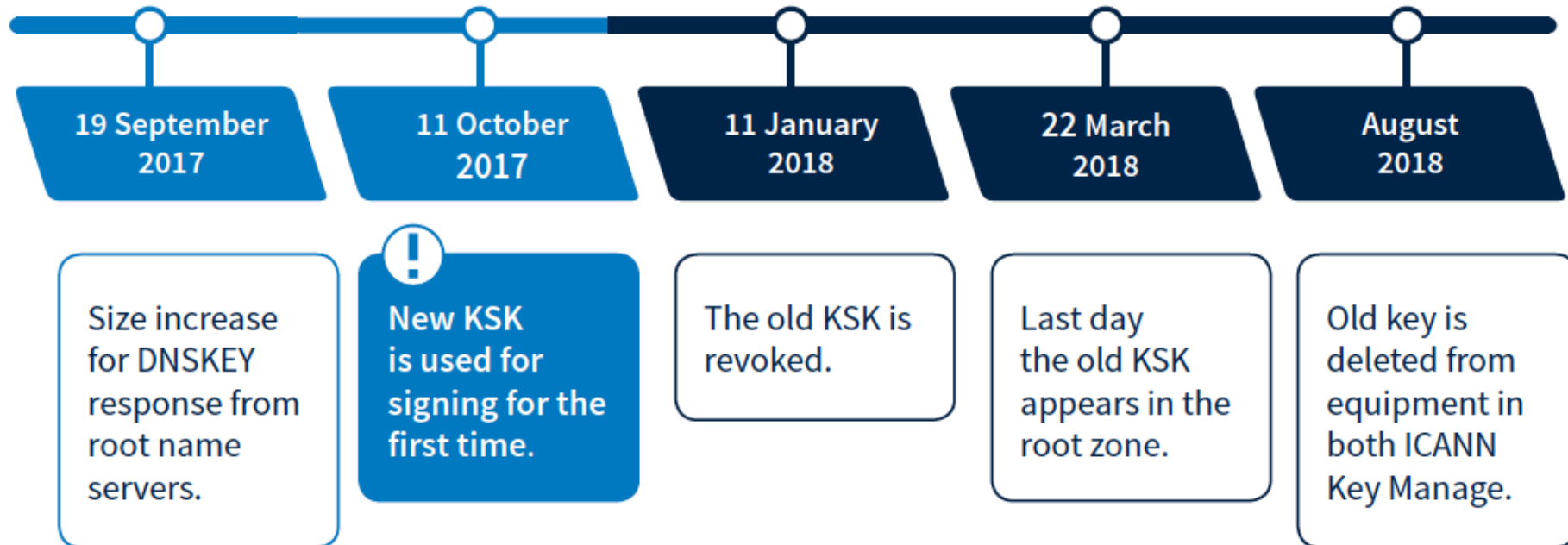
- ⦿ As with passwords, the cryptographic keys used in DNSSEC-signing DNS data should be changed periodically
  - Ensures infrastructure can support key change in case of emergency
- ⦿ This type of change has never before occurred at the root level
  - There has been one functional, operational Root Zone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

# DNSSEC

# 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**



# For More Information

1

**Visit <https://icann.org/kskroll>**

2

**Join the conversation online**

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

3

**Ask a question to [globalsupport@icann.org](mailto:globalsupport@icann.org)**

- Subject line: “KSK Rollover”

4

**Attend an event**

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

