



KSK Rollover

Tech Day | Office of the CTO | 5 November 2016

KSK Rollover: An Overview

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

- ⦿ 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

KSK Rollover: An Overview

- ⦿ 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
- ⦿ The KSK rollover must be widely and carefully coordinated to ensure that it does not interfere with normal operations

DNSSEC

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)

Don't Get Locked Out!

- To help ensure trouble-free Internet access for their users, Internet service providers, enterprise network operators and others who have enabled DNSSEC validation **must update their systems with the public part of the new KSK (the root “trust anchor”)**
 - Available from <https://www.iana.org/dnssec/files>
- Key dates of the process when end users may experience interruption in Internet services:
 - **19 September, 2017**
Size increase for DNSKEY response from root name servers
 - **11 October, 2017 – Most important date**
New KSK used for signing for the first time
 - **11 January, 2018**
The old KSK is revoked



For More Information

- ⦿ Visit <https://icann.org/kskroll>
 - Share this resource with others
- ⦿ 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”
- ⦿ Visit <https://features.icann.org/calendar> to find upcoming KSK rollover presentations