Quick Guide:
Prepare Your Systems for the Root KSK Rollover

What Is the Root KSK Rollover?

The Internet Corporation for Assigned Names and Numbers (ICANN) is planning to roll, or change, the "top" pair of cryptographic keys used in the Domain Name System Security Extensions (DNSSEC) protocol, commonly known as the root zone key signing key (KSK). This will be the first time the KSK has been changed since it was initially generated in 2010. It is considered an important security step, in much the same way that regularly changing passwords is considered a prudent practice by any Internet user.

Changing the key involves generating a new cryptographic key pair and distributing the new public component to DNSSEC-validating resolvers. As every Internet query using DNSSEC depends on the root zone KSK to validate the destination, this will be a significant change. Now that the new key has been generated, operators, such as ISPs, will need to update their systems with the new key so that when a user attempts to visit a website, it can validate it against the new KSK.

Why You Need to Prepare

Currently, about a quarter of global Internet users access the Internet through 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.

If you don't use DNSSEC, your system will not be affected by the rollover. However, you should know that DNSSEC is an important part of preventing domain name hijacking.

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: **https://go.icann.org/KSKtest**.

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

Designed by ICANN Communications | March 2018

What You Need To Do

Your systems can be updated at any time prior to the rollover using the new root zone KSK that was published in 11 July 2017 and some may already have automated updates in place. The action you need to take depends on the following.

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

The KSK should have been updated automatically at the appropriate time. You do not need to take additional action.

Of note, devices that are offline during the rollover will have to be updated manually if they are brought online after the rollover is finished.

ICANN started offering a test bed in March 2017, for operators or any interested parties to confirm that their systems handle the automated update process correctly. More information is available at **https://icann.org/kskroll.**

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 at: **https://go.icann.org/2DOB7zn**.

When Does the KSK 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:

11 October 2018

Proposed date for the new KSK being used for signing for the first time.

11 January 2019

Proposed date for the old KSK being revoked.

More information about the rollover, including resources to help you prepare for the upcoming change, can be found at **https://icann.org/kskroll**.

You can also send an email to **globalsupport@icann.org** with "KSK Rollover" in the subject line, or join the conversation on Twitter using #KeyRoll.

Designed by ICANN Communications | March 2018