Root Zone Key Signing Key (KSK) Rollover

KSK rollover at a glance

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 KSK. This will be the first time the KSK has been changed since it was initially generated in 2010.

Changing these DNSSEC keys is an important security step, in much the same way that regularly changing passwords is considered a prudent practice by any Internet user.

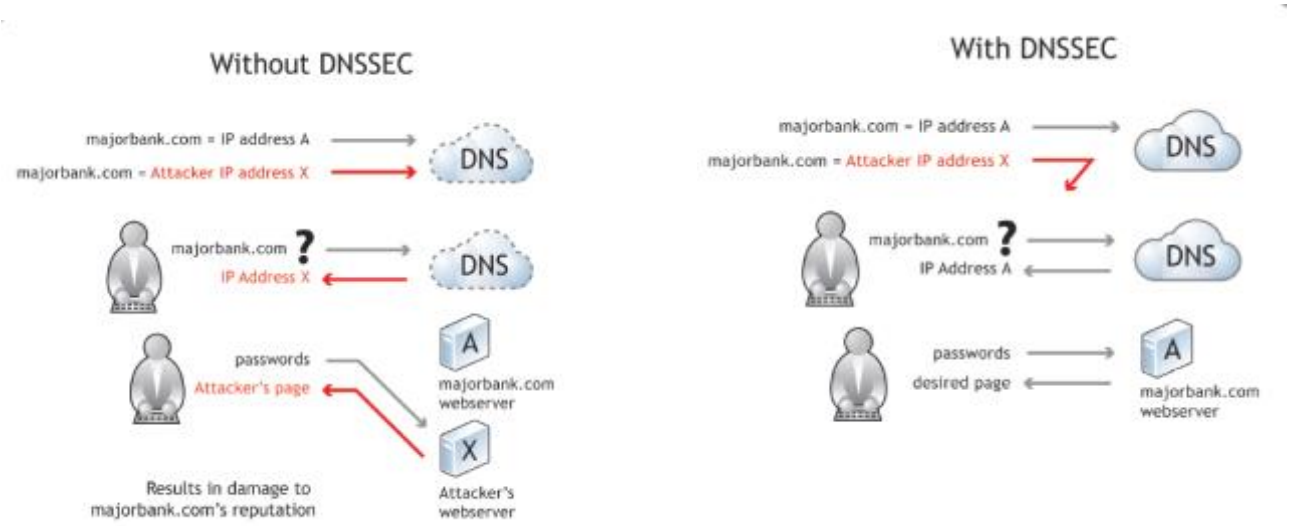
The root zone KSK consists of a private key and a public key. The private component is securely stored by ICANN, but the public component is widely distributed and configured in a large number of devices, possibly numbering in the millions. The multi-step KSK rollover process basically involves generating a new cryptographic key pair and then distributing the new public key.

Internet service providers, enterprise network operators and others performing DNSSEC validation must ensure their systems are updated with the public part of the new KSK in order to assure trouble-free Internet access for their users.

The KSK is an essential component of DNSSEC, a security technology that authenticates the integrity of information within the Domain Name System (DNS), which is the Internet's global phone book. This type of change has never before occurred at the root level, so the rollover must be widely and carefully coordinated to ensure that it does not interfere with normal operations. For this reason, ICANN is informing the Internet operator and user communities about the changes now, before the rollover actually occurs.

What role does the KSK play in DNSSEC?

The KSK plays an important role in protecting Internet users from domain name hijacking by validating DNS data. As the phrase implies, domain name hijacking is taking control of a domain name, often by those with malicious intent who may be seeking illicit financial gain. For example, attempts to access bank account information may result in redirecting users to a site that steals identification and passwords.



Why the KSK rollover matters

The KSK has been widely distributed to every operator performing DNSSEC validation. If the validating resolvers using DNSSEC 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.

The root zone KSK is the first key in a chain of public keys that a validating resolver uses to confirm the authenticity of DNS data. Each key in the chain vouches for the validity of the next key, starting with the root KSK at the beginning of the chain. If the root zone KSK changes and the resolver's configuration is not updated, the first key in the chain will be wrong, making the entire chain invalid. As a result, DNSSEC validation will fail and the resulting error will keep users from accessing the Internet.

When will the rollover take place?

The KSK rollover is a process, not a single event, expected to be completed in March 2018. The new public key is tentatively scheduled to be published at http://data.iana.org/root-anchors/ in February 2017, and will appear in the DNS for the first time on July 11, 2017.

Here are some other milestones in the rollover process. Please note that these dates are subject to change because of operational considerations:

- **October 2016:** Generation of new KSK
- **February 2017:** Publication of new KSK on the IANA web site
- **July 2017:** Publication of new KSK in DNS
- **October 2017:** New KSK used for signing (the actual rollover event itself)

- **January 2018:** Revocation of old KSK
- **March 2018:** Secure destruction of the old KSK and completion of KSK rollover process

How many people could be affected?

An estimated one-in-four global Internet users, or 750 million people, could be affected by the KSK rollover. That figure is based on the estimated number of Internet users who use DNSSEC-validating resolvers.

Who needs to take action?

Developers of software supporting DNSSEC validation are strongly encouraged to support the RFC 5011 automatic trust anchor update protocol. Software developers and distributors who include the root zone KSK in code or configuration files should ensure that the new root zone KSK is used, ideally as soon as possible after the new KSK is published in February 2017.

Operators relying on the RFC 5011 automatic trust anchor update protocol should ensure that their DNSSEC-enabled resolvers are configured to automatically update the root zone trust anchor when the rollover occurs. Operators who update DNSSEC-enabled resolver trust anchor configuration manually should ensure that the new root zone KSK is configured before October 11, 2017.

Anyone who writes, integrates, distributes or operates software supporting DNSSEC validation that correctly follows the RFC 5011 automatic trust anchor protocol does not need to take any action.

Resources

Ask a question

To submit a question, please send an email to globalsupport@icann.org with "KSK Rollover" in the subject line.

Learn more about the KSK Rollover

https://www.icann.org/kskroll

Join the conversation

Use the hashtag #KeyRoll: https://twitter.com/icann