What To Expect During the Root KSK Rollover

ICANN Office of the CTO

Updated on 17 September 2018

Executive Summary

After the root KSK rollover begins (currently planned for 11 October 2018), a very small percentage of Internet users are expected to see problems in resolving some domain names. There are currently a small number of Domain Name System Security Extensions (DNSSEC) validating recursive resolvers that are misconfigured, and some of the users relying on these resolvers will experience problems. This document describes which users will see problems and, among them, what kinds of issues they will see at various times.

- Users who rely on a resolver that does not perform DNSSEC validation will not see any effect from the rollover.
- Users who rely on a resolver that has the new KSK will not see any effect from the rollover.
- If all of a users' resolvers do not have the new KSK in their trust anchor configuration, the user will likely start seeing the effects at some point in the 48 hours after the rollover happens.
- It is impossible to predict when the operators of affected resolvers will notice that validation is failing for them.
- Data analysis suggests that more than 99% of users whose resolvers are validating will be unaffected by the KSK rollover.

1. Introduction

The ICANN organization has publicized the upcoming rollover of the DNS root zone KSK for many years.[1] During the recent public comment for the revised rollover plans,[2] many members of the community asked for more details on the rollover process. The ICANN org agreed to publish more materials to help prepare for the rollover.[3] This document is part of that effort.

There has been some confusion in various communities about what will (and will not) be seen once the rollover happens. This document gives details about what is expected starting from the moment that the rollover takes place.

This document has many audiences. Three primary ones are:

- Operators of validating resolvers who want to know what to look for once the rollover happens

[1] http://www.icann.org/kskroll
[2] https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en
[3] https://www.icann.org/en/system/files/files/report-comments-ksk-rollover-restart-23apr18-en.pdf

- Non-technical press and others who intend to write about the rollover before and as it happens
- Researchers who will be monitoring the DNS for indications of resolver failure after the rollover happens

We should note that this document is probably of little interest to those who use at least one resolver that is ready for the rollover. After the rollover occurs, these users will see no change in their use of the DNS or the Internet in general. The same is true for users whose resolvers do not perform DNSSEC validation at all. Current estimates are that about two thirds of users are behind resolvers that do not yet perform DNSSEC validation.

The rollover is currently planned to take place on 11 October 2018 at 1600 UTC. The rollover was originally planned for 11 October *2017*, but it was postponed due to unclear data received just before the rollover.[4]

Sections 2 and 3 of this document describe what will happen after the rollover to validating resolvers that are prepared for the rollover, and to those that are not. Section 4 describes what might be seen by researchers who are monitoring traffic to the DNS root server system. Throughout this document there are non-deterministic phrases used to describe will happen after the rollover. This wording is used because there is no way for anyone other than a resolver's operator to accurately tell which software is run by the resolver, and no way to tell whether a resolver is even configured correctly for the rollover.

Important Note To Resolver Operators: All operators of validating resolvers reading this document should immediately verify whether they are prepared for the rollover by checking their current trust anchors.[5] If operators are not ready, they should update to the latest trust anchors at their earliest opportunity.[6] Operators of resolvers that are not doing DNSSEC validation are already prepared for the rollover.

1.1 Definition of the Root KSK Rollover

The DNS root zone was signed with DNSSEC in 2010. The DNS root zone has two types of keys; zone-signing keys (ZSKs) that sign the main data in the root zone, and key-signing keys (KSKs) that sign just the root key set (both ZSKs and KSKs) in the root zone. Every three months, a new ZSK is published. Each new ZSK is signed by a longer-lived KSK.

The rollover occurs when the root KSK is changed and the new KSK starts signing the root key set for the zone. At the time of the rollover, the original KSK will be retired and the new KSK will be used. The first KSK is called KSK-2010 (still in use today). The new KSK is called KSK-2017. After the rollover, KSK-2010 will no longer be signing the root key set: instead, KSK-2017 will be signing the root key set.

[4] https://www.icann.org/news/announcement-2017-09-27-en
[5] https://www.icann.org/dns-resolvers-checking-current-trust-anchors
[6] https://www.icann.org/dns-resolvers-updating-latest-trust-anchor

1.2 Trust Anchors

In order to understand how the rollover will happen, it is also important to understand how the validating resolver trusts the root KSK. Each validating resolver is configured with a set of *trust anchors*, which are copies of the keys or key identifiers that match the root KSK. Trust anchors are typically configured automatically by software vendors, or by the resolvers which are configured to automatically update the trust anchors using the process described in RFC 5011,[7] or by the resolver operator who manually adds a new KSK to the resolver's trust anchor store.

Before KSK-2017 existed, all validating resolvers only had the KSK-2010 configured as a trust anchor. After KSK-2017 was created and published, most resolver operators either manually added KSK-2017 to their resolver's trust anchor configuration, or the change was made for them by their software (such as through the RFC 5011 automated update process) or by their software vendor. However, some resolver operators did not update their configuration, and are now unprepared for the rollover because they still only have KSK-2010 as a trust anchor. When the rollover happens, these resolver operators will have no valid trust anchors.

2. Resolvers that are Prepared for the Rollover

Resolvers that are prepared for the rollover already have KSK-2017 configured as a trust anchor. When the rollover happens, these resolvers will continue to work just as they did before the rollover because the new root KSK is already trusted to sign the root key set. Some resolver software might note in the operational logs that a rollover happened, but those log entries (if they even exist) are unlikely to be seen unless the operator is specifically looking for them.

Users of resolvers that are prepared for the rollover will see no difference when the rollover happens. The responses they get to normal queries will be identical before and after the rollover. According to recent research by APNIC,[8] more than 99% of users whose resolvers perform DNSSEC validation are using resolvers that are prepared for the rollover.

Most Internet users have more than one DNS resolver configured. If any of the resolvers that a user has configured is prepared for the rollover, the user's software should find that resolver after the rollover and continue to use it. This might slow down DNS resolution as their system keeps trying the resolver that is not prepared before switching to the resolver that is prepared, but the user will still get DNS resolution.

3. Resolvers that are Unprepared for the Rollover

If a resolver has only the KSK-2010 key configured as a trust anchor, after the rollover, the resolver will start to fail to validate the answers it gets from authoritative servers. However, the time at which that failure starts to happen is not predictable.

Although publication in the DNS is an instantaneous action there can be a time lag for a resolver to see a newly published record. Each record in the DNS has a "time to live" (usually called the *TTL*) during which a resolver will not try to get a newer version of the record. After the moment

[7] https://datatracker.ietf.org/doc/rfc5011/

[8] http://www.potaroo.net/ispcol/2018-04/ksk.html

of the rollover, a resolver will likely still have a cached version of the signature made by KSK-2010 and will therefore continue to validate successfully, at least for a while.

3.1 Failure Starts When The ZSK Cannot be Validated

Every time a validating resolver gets a response from an authoritative name server, it checks the signature on that response. It saves the validation status of the signature on each name in its cache. To validate the signature on a name like “www.example.com”, the resolver needs to validate the signatures on the root, on “.com”, on “example.com”, and "www.example.com”. Resolvers typically cache these validations so they don’t perform them for each name. Most resolvers only perform validations when the validation status might have changed.

The TTL for the KSK and ZSK records is 48 hours. If a resolver obtains the root key set and validates it *just* before the rollover happens, that resolver won’t know about the rollover for almost two days, because the resolver will not fetch a new KSK until it gets the first query after the TTL of root key set has expired. In a normal resolver with only a few users, that triggering query will happen within a few minutes (or even seconds) after the DNSKEY records’ TTL has expired. On a resolver with a single user, the time before the first query could be hours, or even days, after the root key set’s TTL has expired.

Note that this description is a bit simpler than what really happens. For example, some resolvers enforce a maximum length on TTLs, which could make those resolvers see the key rollover in a shorter period of time. Other configuration choices can also affect when the resolver first sees the rollover.

3.2 What Users Will See When All of Their Resolvers Fail

At some point within 48 hours after the time of the rollover, some users’ DNS queries will begin to fail because they will cause the resolver to get root key set again. As explained above, one cannot predict when the first results will fail during that 48-hour period.

When this failure happens, if the user has multiple resolvers configured (as most users do), their system software will try the other resolvers that the user has configured. This might slow down DNS resolution as their system keeps trying the resolver that is not prepared before switching to the resolver that is prepared, but the user will still get DNS resolution and might not even notice the slowdown. However, if all of the user’s resolvers are not prepared for the rollover (such as if they are all managed by one organization and that organization has not made any of their resolvers ready), the user will start seeing failure sometime in the 48 hours after the rollover.

Users will see different symptoms of failure depending on what program they are running and how that program reacts to failed DNS lookups. In browsers, it is likely that a web page will become unavailable (or possibly only images on an already displayed web page might fail to appear). In email programs, the user might not be able to get new mail, or parts of message bodies may show errors. The failures will cascade until no program is able to show new information from the Internet.

Note that the term “users” here does not just indicate humans. Automated systems that are also using unprepared resolvers for their DNS resolution will start to fail, possibly catastrophically.

After the operator of the resolver fixes the inability to validate (either by adding KSK-2017 as a trust anchor, or by turning validation off), the users' Internet experience should go back to normal almost immediately.

3.3 How Resolver Operators Will Know About the Failure

An operator of a resolver who has configured their system monitoring software to look for significant errors will be alerted immediately after the resolver fetches a new copy of the root key set and it is unable to be validated. Such monitoring offers the operator the best chance of quickly detecting and recovering from the failure.

If the operator is not actively monitoring for significant errors, they will probably not know about the failing validation until automated systems that rely on the resolver start failing, or users start calling them about outages. If the operator is also only using resolvers with incorrect trust anchor configurations, they may be unable to get email messages that are being sent to them, and might only hear about the problems by phone calls.

3.4 Recovering from Being Unprepared

As soon as operators discover that their resolver's DNSSEC validation is failing, they should change their resolver configuration to temporarily disable DNSSEC validation. This should cause the problems to immediately stop.

After that, the operator should install, as soon as possible, the KSK-2017 as a trust anchor and turn on DNSSEC validation again. ICANN org provides instructions for updating the trust anchors for common resolver software.[9]

4. What Root Server Operators Will See

After the rollover, root server operators will start to see significantly more queries from resolvers that are unprepared for the rollover. Those queries will most likely be for the DNSKEY of the root (./IN/DNSKEY), and will also likely include queries for the DS record of the .net zone (.net/IN/DS). Additionally, since the responses can't be validated correctly, they will not be cached, which will lead to increased traffic overall from these validating resolvers. Similarly, operators of resolvers that allow other resolvers to forward through them will likely start seeing increased counts of these requests after the rollover.

Researchers are already monitoring root server traffic for root DNSKEY requests in order to get a baseline of how many queries per minute are typical. These statistics are reported to ICANN in near real time (once per minute) by 11 of the 12 root server organisations. ICANN will continue to monitor those statistics after the rollover begins and will report the results to the root server operators and the rest of the DNS technical community.

[9] https://www.icann.org/dns-resolvers-updating-latest-trust-anchor

Appendix A. Where to Find Out More About the Rollover

The primary source for information about the rollover is:

http://www.icann.org/kskroll

That page has a KSK Rollover Quick Guide, an extensive set of resources about DNSSEC, why the community chose to have a rollover, and the plans for the rollover. It is available in English, Spanish, French, Russian, Arabic, Chinese, Portuguese, Korean and Japanese.

Subscribe to this mailing list for discussion about the rollover:

https://mm.icann.org/listinfo/ksk-rollover

Appendix B. Glossary

DNSSEC – Extensions to DNS that allow an authoritative server to cryptographically sign DNS records so that a resolver can be assured that the data in the records was not altered.[10]

KSK – Key Signing Key, the key that is used to sign all the keys in a zone.

Rollover – Changing a Key Signing Key in a zone from an existing key to a newer one.

TTL – The "Time To Live" for a set of records in the DNS. When a resolver gets a set of records from an authoritative server, it usually keeps those records in its cache for the number of seconds indicated in the TTL.

Validation – Validating the signatures on the records in a zone that is protected by DNSSEC. Resolvers perform validation in order to be sure that the records they receive from an authoritative server are correct.

ZSK – Zone Signing Key, the key that is used to sign all the records in a zone other than keys (which are signed by the Key Signing Key).

[10] https://meetings.icann.org/en/marrakech55/schedule/sun-dnssec-everybody