Review of the 2018 DNSSEC KSK Rollover

ICANN Office of the CTO
4 March 2019

TABLE OF CONTENTS

1. Executive Summary

Objective

Modern use of the Domain Name System Security Extensions (DNSSEC) protocol relies on validating resolvers to all have the same trust anchor, which is a representation of the key used for signing the other keys in the root zone. That key, commonly called the root key signing key (KSK), was first introduced to the root zone in 2010.

At the time, the community agreed that the key should be changed periodically to make sure that all DNSSEC validating software was capable of making changes when needed. Other reasons given at the time were to encourage the design of a rollover plan that could be reused in an emergency, and to show that the DNSSEC ecosystem was flexible enough to handle such changes.

Method

ICANN org asked the community to help define the KSK rollover process and in 2015 a KSK roll design team from the technical community produced a draft plan with a target rollover date of October 2017. ICANN's communications outreach was aimed at helping change the KSK with little or no disruption to the Internet. Because the validating resolvers are managed only by their operators, there was no means to measure or control all of the elements involved in the rollover. The strategy focused on publicizing the broad message that the root zone KSK is changing, with more detailed supporting documents for those who would need it.

The initial rollover was scheduled for 11 October 2017 but was postponed because some last-minute data showed that a significant number of resolvers used by Internet Service Providers (ISPs) and Network Operators were not yet ready for the Key Rollover. The availability of the new data was due to a new DNS protocol feature that added the ability for a resolver to report back to the root servers which keys it has configured.

Findings

The Root KSK Operator published a root zone with DNSKEY record set signed by KSK-2017 for the first time on 11 October 2018. The number of queries for the root DNSKEY records increased, indicating that some resolvers were still unprepared for the rollover when it happened. However, there were no significant outages. On 11 January 2019, the old KSK was revoked, and the number of queries for the root DNSKEY records increased again, indicating that that some resolvers either are based on software with significant programming errors or bad configurations.

Conclusions

The result of the rollover process was the KSK being changed with only a very small amount of disruption visible to Internet users. Thus, the most significant conclusion to be drawn from the process for this first rollover was that it was an overwhelming success. Even with that, two companion conclusions are that it is impossible to predict how resolvers will react to KSK changes, and that a long rollover process can have negative consequences for the community.

2. Introduction

The DNS is used to easily identify resources on the Internet. Increased computing and networking sophistication since the DNS's design in 1983 have made this database of names vulnerable to attacks. Specifically, it is possible for attackers to falsify responses to DNS queries, which gives them the ability to redirect end users to Internet sites under their control without notice.

DNSSEC is the widely implemented protocol that uses digital-signature cryptography to help thwart such attacks. In order for DNSSEC to work effectively, all users must have a single root of trust, and that trust must be based on cryptographic keys that are shared outside the DNS itself. The main cryptographic key for DNSSEC was changed on 11 October 2018. It was replaced by another KSK after a thorough process of community consultations and technical steps needed to minimize unwanted side effects of the change.

This document describes the entire process of the change of the KSK. It is meant to be helpful in planning future rollovers.

The process of changing the KSK had many components. One of the most significant components was informing the public about the change and potential impacts. In this document, the communications effort is described near the end in its own section.

Readers interested in following the KSK discussion are encouraged to join the "ksk-rollover" mailing list.[1]

Definitions

DNSSEC – DNS Security Extensions, the set of protocols used to give assurance that data received in a DNS response is the same as the data entered in a zone by the zone's manager, or more specifically, the holder of the zone's signing key. DNSSEC is defined by many different RFCs, and also in ICANN's *Acronyms and Terms* pages.[2]

KSK – A key signing key, a key that is used to sign the set of keys (but not the other records) in a zone.

KSK-2010 – The KSK for the DNS root zone that was created in 2010 when the root zone was first signed with DNSSEC. This key was used as the trust anchor for the DNS until the rollover in 2018.

KSK-2017 – The KSK for the DNS root zone that was created in 2017. At the time this document is published, this is the current trust anchor for the DNS, and was first used to sign the root zone on 11 October 2018.

resource record set (RRset) – A set of resource records in a zone that has the same domain name, class, and type. The KSKs and ZSKs for a zone have the same resource type (DNSKEY), and thus are grouped as an RRset.

[1] See https://mm.icann.org/listinfo/ksk-rollover

[2] See https://www.icann.org/icann-acronyms-and-terms/en/G0253

rollover – The process of changing the KSK or ZSK of a zone. This process is more than just the specific change: it involves all the preparation for and follow-up to the change.

Root KSK Operator – A role that is performed by the IANA Naming Functions Operator. During this rollover, it was fulfilled by Public Technical Identifiers (PTI)[3], an affiliate of ICANN that performs the IANA functions.

Root ZSK Operator – A role that is performed by the Root Zone Maintainer. During this rollover, it was fulfilled by Verisign.

Root Zone Partners – PTI and Verisign, who fulfill the Root KSK Operator and the Root ZSK Operator roles respectively.

ZSK – A zone-signing key, the key that is used to sign the records in a zone other than the keys themselves

Two other documents have good lists of terminology that relate to the DNS. *DNS Terminology*, RFC 8499[4], covers terminology for all parts of the DNS. Also, the *RSSAC Lexicon*[5] mostly relates to the root servers, which are an important part of the KSK rollover process.

3. DNSSEC Overview

The KSK was deployed in the root zone in 2010 as part of the DNSSEC implementation. Because the KSK had not been changed in the first years after DNSSEC deployment, the concepts related to the change were not widely discussed at that time. Further, as the ICANN organization discovered when it began soliciting community input on the process of changing the key, many different opinions exist on how to change the DNS root KSK.

For more detail and background on DNS and DNSSEC, please see *DNSSEC Basics*[6] from The Internet Society for an introduction to the topics.

General Description of the Root Key Rollover

The *DNSSEC Practice Statement for the Root Zone KSK Operator*[7] states, “Each [root zone] KSK will be scheduled to be rolled over through a key ceremony as required, or after 5 years of operation”.

The high-level steps for a rollover are:

1. Create a new cryptographic key that will become the new KSK.
2. Include the new KSK in the DNSKEY RRset for the zone.
3. Begin to tell the technical community about the new KSK so that it can be trusted before it is used for signing.
4. Start signing the DNSKEY set with the new KSK.
5. Remove the old KSK from the DNSKEY set.

[3] See https://pti.icann.org/
[4] See https://tools.ietf.org/html/rfc8499
[5] See https://www.icann.org/en/system/files/files/rssac-026-14mar17-en.pdf
[6] See https://www.internetsociety.org/deploy360/dnssec/basics/
[7] See https://www.iana.org/dnssec/icann-dps.txt

Note: the actual process of rolling the KSK for the DNS root involves many more steps, as well as sub-steps within the steps above.

Trust Anchors

A validating resolver or other system doing DNSSEC validation needs a *trust anchor* that matches the key that begins the chain of trust for validating. A trust anchor can be in one of two forms - either a copy of a public key, or a cryptographic hash of a public key - and it needs to be retrieved and configured using something other than the DNS.

Since 2010, validators that have a trust anchor configured for the root know that the DNS root is signed and can be validated. All zones below the root are either signed and can be validated, or can be proved to be not signed.

The two most common ways that trust anchors are published and distributed are:

- Hash of the public key, retrieved as a file from the Root KSK Operator.[8] This file contains the current trust anchor(s), and may also contain copies of older trust anchors with markings that those are no longer valid. The Root KSK Operator also publishes a digital signature of that file that can be used by those who have a copy of the Root KSK Operator's public signing key.[9]
- Hash of the public key or the entire public key, received from a software vendor as part of its resolver software. Different vendors have different file formats, some of which include the entire key (sometimes as a DNS resource record), others as a hash of the key.

Defining When the Rollover is Complete

In the discussions for the rollover plan, there were at least four different views of when the rollover would be complete:

- When the new key is signing the DNSKEY data set – In this view, a rollover consists of changing the key used in the RRSIG records that apply to the DNSKEY records. The rules for what RRSIG records must be present are given in Section 2.2 of *Protocol Modifications for DNSSEC* (RFC 4035).[10] If the old key is later used to sign again due to a back out because the rollover process was reversed, that is classified as a separate rollover event.

- When the old key is revoked – If a validating resolver that follows *Automated Updates of DNSSEC Trust Anchors* (RFC 5011)[11] sees the old key with the revoke bit set, that resolver will never trust the old key again. Therefore, the old key should never be used again.

- When the old key is removed from the root zone – Some validating resolvers do not follow RFC 5011, so the old key with the revoke bit set will not change the validators' behavior. Only after the old key is removed from the root zone can the rollover be

[8] See http://data.iana.org/root-anchors/root-anchors.xml
[9] See http://data.iana.org/root-anchors/root-anchors.p7s
[10] See https://tools.ietf.org/html/rfc4035
[11] See https://tools.ietf.org/html/rfc5011

considered complete.

- When the Root KSK Operator can no longer sign with the old key – After the private keys are deleted from secure storage, they can no longer be used to sign again.

Note: this document does not specify any of these four as the "official" definition of when the rollover is complete.

4. Current Operation of the DNS Root KSK

ICANN has overarching responsibility for the root of the DNS, and the Root KSK Operator is responsible for maintaining the DNSSEC KSK for the root. Operations of the root zone KSK are done in a transparent manner to instill broad trust in the proper operation, including engaging with the general public for feedback on operation and improvement.

The base documents that describe the operations of the root keys are called "DNSSEC Practice Statements", commonly shortened to "DPSs". There are two DPSs for the root zone: one for the KSK (maintained by the Root KSK Operator)[12] and one for the ZSK (maintained by the Root ZSK Operator). They are the agreements that the Root KSK Operator and the Root ZSK Operator promise to follow.

The Root KSK Operator stores the key material in four hardware security modules (HSMs) that are kept in two different, highly secure key management facilities (KMFs) thousands of miles apart. Between the design of the HSM and the physical infrastructure of the KMF, the keys are protected by many layers of physical security designed to guard against surreptitious access.[13] When the KSK is needed for signing the DNSKEY RRset (that is, signing the set of KSKs and ZSKs for the root zone), one of the HSMs in one of the facilities must be used.

The *DNSSEC Practice Statement for the Root Zone KSK Operator* requires that the Root KSK Operator perform all key signing using a public process under the oversight of members of the DNS community; these activities are called "key signing ceremonies".[14] The Root KSK Operator holds key signing ceremonies four times per year, usually at least a month before the results of the ceremonies are introduced into the root zone. The new ZSKs are created in advance by the Root ZSK Operator. The main activity at a key signing ceremony is signing the new ZSKs.

DNSSEC changes for the root zone are managed on a quarterly basis. To allow for flexibility, the results of the KSK ceremonies divide the quarter into 10-to-12 day slots. The first slot and last slot in a quarter are reserved for maintenance of the ZSK. An artifact of this setup is that changes to the KSK to the root zone are constrained to only 11 January, 11 April, 11 July, or 11 October.

The five steps listed earlier for the KSK rollover all happen during key signing ceremonies.

[12] See https://www.iana.org/dnssec/dps
[13] See https://go.icann.org/2Hw7wQr
[14] See https://kimdavies.com/key-ceremony-primer/

5. Decision to Roll Over the KSK

When the first DNS KSK was created in 2010, the DNS technical community discussed whether to have a planned KSK rollover or wait until the KSK needed to be changed because it had been compromised. After some debate, it was decided by consensus to roll over the KSK after five years. The relevant text from the KSK DPS says that the root zone KSK "will be scheduled to be rolled over through a key ceremony as required, or after 5 years of operation".

Some in the community maintained that rollovers were only needed if the KSK had been compromised, for example, by a cryptographic attack. The main reason given for having a planned rollover was to make sure that all DNSSEC validating software was capable of making changes when needed. Other reasons given for scheduling the rollover: to push ICANN to design a rollover plan that could be reused in an emergency, and to show the DNSSEC ecosystem was flexible enough to handle such changes.

In 2013, ICANN org asked the community to help define the KSK rollover process.[15] The result was a set of recommendations for how the Root Zone Partners should proceed. Also in 2013, the ICANN Stability and Security Advisory Committee (SSAC) published *SSAC Advisory on DNSSEC Key Rollover in the Root Zone* (SAC063),[16] which had additional recommendations.

This phase of the KSK rollover project began in 2015 when the Root Zone Partners assembled a KSK roll design team from the technical community to discuss and produce recommendations for rollover plans. A draft plan was produced in August 2015, and a final report document published in March 2016.[17] Following this effort, ICANN org developed a set of specific operational plans that were made public in July 2016; those operational plans had a target date for the rollover in October 2017. From July 2016 until October 2017, ICANN org initiated a series of outreach efforts to prepare for the rollover. Those planned events were adjusted due to the postponement of the rollover to October 2018. The reasons for the postponement are described later in this document.

A fuller history of the KSK rollover design development is given in Section 2 of the *Root Zone KSK Rollover Plan* from March 2016 from the design team.

Technical Recommendations in the Design Team Report

The report started with 17 recommendations, many of which are about ICANN org reaching out to various communities as the rollover progresses. Six of those recommendations, however, were technical and thus led to specific requirements for the eventual operational plans:

- *Recommendation 1: The Root Zone KSK rollover should follow the procedures described in RFC 5011 to update the trust anchors during KSK rollover.*
  The standard *Automated Updates of DNSSEC Trust Anchors* (RFC 5011)[18] describes a mechanism that is implemented in and enabled by many validating resolvers to automatically update trust anchors. At a high level, the mechanism requires the new KSK to be in the root zone for at least 30 days before it can be configured as a trust anchor. The mechanism also allows the old KSK to be marked as "revoked", causing

[15] See https://www.icann.org/public-comments/root-zone-consultation-2013-03-08-en
[16] See https://www.icann.org/en/system/files/files/sac-063-en.pdf
[17] See https://www.iana.org/reports/2016/root-ksk-rollover-design-20160307.pdf
[18] See https://tools.ietf.org/html/rfc5011

validating resolvers to remove the key as a trust anchor. The old KSK is then removed from the root zone. The Root KSK Operator followed this recommendation, and ICANN org heavily promoted the use of RFC 5011 in its communications about the rollover.

- *Recommendation 6: All changes to the root zone DNSKEY RRsets must be aligned with the 10-day slots described in the KSK Operator's DPS.*
  The *DNSSEC Practice Statement for the Root Zone KSK Operator* defines how new signatures made by the ZSKs are published in the root zone every 10 days. This recommendation states that the addition of a new KSK to the root zone, and the removal of the old KSK from the root zone, should be done at the same time as the ZSK signatures are being changed. The operational plans followed this recommendation.

- *Recommendation 7: The existing algorithm and key size for the incoming KSK for the first Root Zone KSK rollover should be maintained.*
  This recommendation means that the new KSK should use the RSA signing algorithm with the SHA-256 hash algorithm, with a key size of 2048 bits (the same as the old KSK). The operational plans followed this recommendation.

- *Recommendation 14: To support a number of potential operational contingencies that may require rollback of changes to the root zone during each phase of the KSK key roll, SKRs using the incumbent KSK, SKRs using both the incumbent and the incoming KSK, and SKRs using the incoming KSK should be generated. The Design Team also recommends that the double-signing approach is the preferred mechanism to respond to a requirement to perform a rollback in Quarter 2 of the key roll procedure.*
  This recommendation states that it should be possible to revert to keys that are known to be good if a significant problem is encountered during the rollover. The operational plans followed the first part of this recommendation, but chose not to follow the second part because double-signing causes more RRSIG records to be returned to queries for the DNSKEY RRset.

- *Recommendation 17: It is recommended that the KSK rollover process should begin on 1 April 2016... [followed by many specific dates].*
  The operational plans followed the cadence of the dates in the recommendation, but did not start as early as the report proposed. Also, the original expected dates were postponed by a year.

Issues with Creating the Rollover Report

The process of creating an initial rollover report took more than a year for a variety of reasons. The DNS community had conflicting opinions about when the first rollover should occur, such as what needed to happen before ICANN scheduled the rollover. The community also had disagreements about the steps that needed to be taken during the rollover, with different proposed designs having different side effects on the DNS.

Planning for the rollover began before the IANA transition in October 2016, but it quickly became clear that some milestones would extend past the IANA transition date. This situation caused uncertainty and made it impossible to set solid dates for specific project activities. Instead, the first high-level descriptions of the rollover were defined in terms of phases without dates, which caused some confusion in the community. In addition, this uncertainty delayed the start of communications, which were a critical aspect of the project.

However, the biggest difficulty to creating the design team report was that much of the community agreed that it was impossible to estimate the impact that the rollover would have on validating resolvers. As the report was being created, there was no way to query validating resolvers to see if they were prepared for the rollover. Further, there was no reliable way to determine how many users were using each resolver, so it was impossible to even guess the impact on users. After significant debate, the design report ended up with the following recommendation:

> *Recommendation 16: Rollback of any step in the key roll process should be initiated if the measurement program indicated that a minimum of 0.5% of the estimated Internet end-user population has been negatively impacted by the change 72 hours after each change has been deployed into the root zone.*

6. Plan to Roll Over the KSK in 2017

ICANN org published the design team's *Root Zone KSK Rollover Plan* report and then began developing the specific operational plans for implementing the general plan developed by the community described in the report. ICANN org published the operational plans in July 2016.[19]

Plan Documents

The *2017 KSK Rollover Operational Implementation Plan*[20] describes the timing of the steps needed to do the rollover. The steps listed include:

1. Generating KSK-2017 in one of the Root KSK Operator's secure facilities
2. Copying KSK-2017 to the second of the Root KSK Operator's secure facilities
3. Signing the DNSKEY records before putting them into the root zone
4. Inclusion of the KSK-2017 in the root zone in preparation for the rollover
5. Signing the DNSKEY records with KSK-2017 (the main event of the rollover)
6. Revoking KSK-2010 in the root zone
7. Deleting KSK-2010 from the secure facilities

In order to accommodate Recommendation 6 from the design team report, the plan required fitting the KSK changes to the quarterly cadence of signature refresh "slots". To allow signatures made with root KSK to have a reasonably short validity period, each calendar quarter is divided into nine slots. A new signature over the root's DNSKEY RRset made by the KSK is published every ten days at the beginning of a slot. The graphical representation of the timing in the plan is shown in Figure 1.

[19] See https://www.icann.org/resources/pages/ksk-rollover-operational-plans
[20] See https://go.icann.org/2J8iWMX

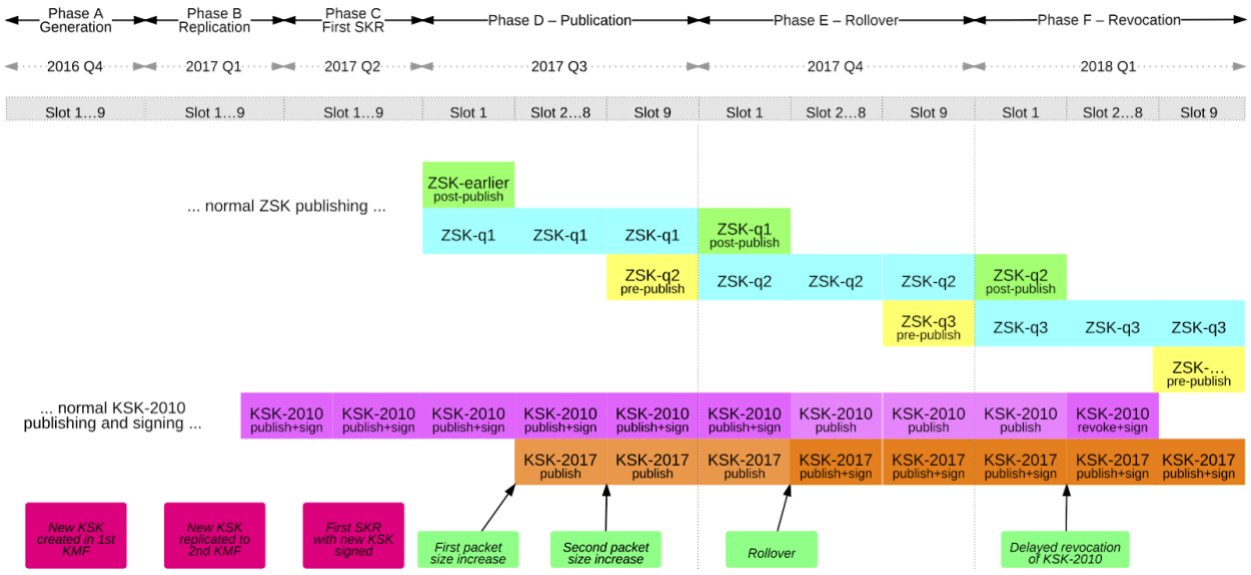

Figure 1. Timing of steps for the rollover

Many of these steps require changes to the normal procedures that the Root Zone Partners use every three months as part of a root key ceremony. After those changes were defined, the *2017 KSK Rollover Systems Test Plan*[21] described how to test those changes before they were needed for the rollover process. This helped assure the technical community that there would be no surprises during the key ceremonies that were part of the rollover.

A major feature of the operational plans was the ability to back out of a step if it was causing negative impact to a large number of users. The *2017 KSK Rollover Back Out Plan*[22] contains a description of how a backout would be executed and lists the response size for the root's DNSKEY for each step. ICANN org also had a crisis communications plan in place in case any of the steps resulted in noticeable degradation to DNS service.

In preparation for the rollover, ICANN org also created test environments that a validating resolver operator could use to assess their readiness for the rollover. The *2017 KSK Rollover External Test Plan*[23] described three such tests. In addition, ICANN organized extensive monitoring before and during the rollover described in the *2017 KSK Rollover Monitoring Plan*[24], to allow the community to assess if some resolvers were having problems with the rollover and if a backout was potentially going to be triggered.

Implementing the Operational Plans

After community review of the operational plans, ICANN org took the steps defined in those plans.

[21] See https://www.icann.org/en/system/files/files/ksk-rollover-systems-test-plan-22jul16-en.pdf
[22] See https://www.icann.org/en/system/files/files/ksk-rollover-back-out-plan-22jul16-en.pdf
[23] See https://www.icann.org/en/system/files/files/ksk-rollover-external-test-plan-22jul16-en.pdf
[24] See https://www.icann.org/en/system/files/files/ksk-rollover-monitoring-plan-15sep16-en.pdf

- 7 September 2016: ICANN org completed testing for resolvers bundled with popular operating systems to determine which have validating resolvers built in.
- 27 October 2016: The Root KSK Operator generated KSK-2017 during Ceremony 27 and stored in the HSMs in the KMF in Culpeper, Virginia.[25]
- 2 February 2017: The Root KSK Operator copied KSK-2017 to the HSMs in the KMF in El Segundo, California during Ceremony 28.[26]
- 13 March 2017: ICANN org launched the real time testbed to help resolver operators determine if they were prepared for the rollover.
- 18 April 2017: ICANN started collecting DNSKEY frequency statistics and error related traffic statistics from several root server operators.
- 27 April 2017: The Root KSK Operator signed DNSKEY records that included KSK-2017 at Ceremony 29.[27]
- 11 July 2017: KSK-2017 appeared in the root zone.
- 1 September 2017: ICANN started collecting RFC8145 data from several root server operators.

In addition, all items from the *2017 KSK Rollover Systems Test Plan* were tested by the Root KSK Operator in different phases before each of the items on which they were testing were rolled out.

Predicted Risks for Rolling the DNS Root Key

At the time that the operational plans were developed, the technical community assumed that the most likely problem with the rollover would be the DNSKEY record set increasing in size at various steps in the plan. The concern was that large DNS messages in certain responses from the root zone would be fragmented before reaching the querying resolvers, those resolvers might not be able to get fragmented records, and would eventually stop operating. However, some in the community pointed out that some widely used zones already had large DNSKEY record sets, and there were no noticeable problems with those zones. Still, the concerns about packet size had a large impact on the operational plans, particularly with respect to the post-rollover monitoring program.

After the first few steps of the rollover occurred, the technical community became less concerned about the size of the root's DNSKEY record set, and more focus was put on the second predicted risk: systems that did not yet have KSK-2017 installed. The technical community assumed that most validating resolvers would automatically update their trust anchor configuration using *Automated Updates of DNSSEC Trust Anchors* (RFC 5011), or would receive an updated trust anchor configuration from software vendors. But it was also well known that some resolver operators had been manually updating their resolvers's trust anchor configuration, and these resolvers would require manual attention. Any operator relying on manual updates who did not install KSK-2017 as a trust anchor would not be ready for the rollover.

ICANN org published and widely publicized two documents targeted at resolver operators to raise awareness of how to update to KSK-2017 as a trust anchor. *Checking the Current Trust*

[25] See https://www.iana.org/dnssec/ceremonies/27
[26] See https://www.iana.org/dnssec/ceremonies/28
[27] See https://www.iana.org/dnssec/ceremonies/29

Anchors in DNS Validating Resolvers[28] showed operators who used most popular resolver packages how to verify the status of their trust anchors, and *Updating of DNS Validating Resolvers with the Latest Trust Anchor*[29] showed how to update the trust anchor if they were not already using KSK-2017.

7. Postponing the Rollover in 2017 and Planning the New Rollover

In April 2017, the IETF published *Signaling Trust Anchor Knowledge in DNSSEC* (RFC 8145).[30] This protocol describes a mechanism for a validating resolver to report to the root server operators the trust anchors that the resolver is using. Vendors of resolver software quickly implemented the new specification and made that software available to their users.

Soon after, upgraded resolvers were sending that data to the root servers, and most of the root server operators reported the data to ICANN for combining and distribution. Root server operators, particularly ICANN and Verisign, began sharing and analyzing the data.

ICANN org's analysis of the data from the first three weeks of September 2017 included data from six root servers. The results of that analysis were that 11,692 unique addresses reported key tag data. Of that population, 577 reported that they only had KSK-2010 configured as a trust anchor. The result was that it appeared that 5% of resolvers were not ready for the KSK roll on 11 October 2017.

The analysis of the data at the time was complicated by many factors:

- Dynamic IP addresses made the situation look worse by inflating true number of sources.
- Resolvers that acted as DNS forwarders made the situation look better if they obscured multiple validators behind the forwarder.
- At the time, some BIND versions reported trust anchors even if a resolver was not validating.

As the community started to analyze the telemetry, the data was confusing. A much higher percentage of resolvers indicated only KSK-2010 as a trust anchor than expected, even though KSK-2017 should have already been trusted by any resolver using *Automated Updates of DNSSEC Trust Anchors* (RFC 5011).

In order to help the technical community perform their own analyses of the data, ICANN org began publishing graphs based on that data; those graphs are still being updated and made available.[31] For example, a recent graph with the historical data from 2017 is shown in Figure 2.

[28] See https://www.icann.org/dns-resolvers-checking-current-trust-anchors
[29] See https://www.icann.org/dns-resolvers-updating-latest-trust-anchor
[30] See https://tools.ietf.org/html/rfc8145
[31] See http://root-trust-anchor-reports.research.icann.org/

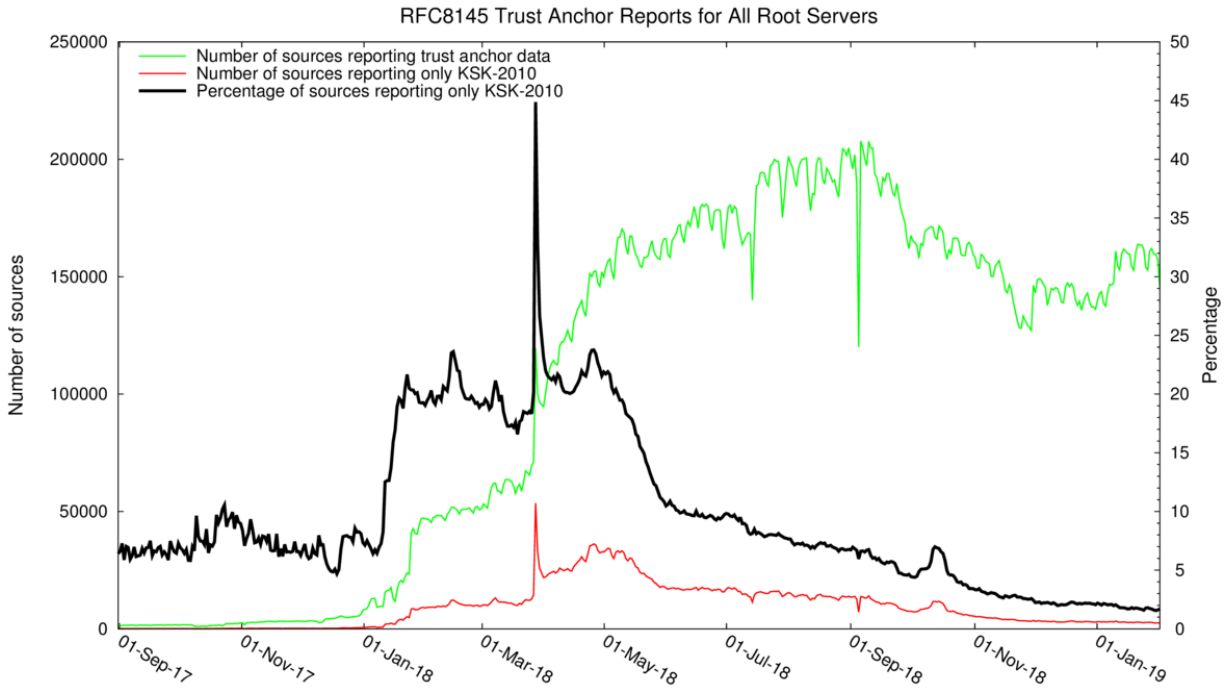

Figure 2. Trust anchor reports from all root servers, February 2019

Due to the uncertainty over the meaning and significance of this data, the ICANN org decided to postpone the rollover. On 27 September 2017, ICANN issued the official announcement of the postponement.[32] It said, in part, that the rollover "...is being delayed because some recently obtained data shows that a significant number of resolvers used by Internet Service Providers (ISPs) and Network Operators are not yet ready for the Key Rollover." It further stated, "There may be multiple reasons why operators do not have the new key installed in their systems: some may not have their resolver software properly configured and a recently discovered issue in one widely used resolver program appears to not be automatically updating the key as it should, for reasons that are still being explored."

ICANN published *Postponing the Root KSK Roll*[33] so that the community could see the decision process that led to the postponement. Immediately after the postponement, ICANN initiated an intensive research effort to try to understand the telemetry being received[34], followed by widespread discussions in the DNS technical community.

A new plan for rolling the KSK was developed. The operational plans for the 2018 rollover are listed on the same web page as the original operational plans.[35] The new plans are significantly shorter than the original plans because many of the steps from the original plans had already

[32] See https://www.icann.org/news/announcement-2017-09-27-en
[33] See https://www.icann.org/en/system/files/files/root-ksk-roll-postponed-17oct17-en.pdf
[34] See https://www.icann.org/news/blog/update-on-the-root-ksk-rollover-project
[35] See https://www.icann.org/resources/pages/ksk-rollover-operational-plans

taken place by 2018. The new set of plans included an additional document, *Steps of the KSK Roll Already Performed in 2017*.[36]

On 1 February 2018, the new plan was put out for Public Comment.[37] In the announcement, ICANN org stated, "There was agreement during these discussions that there is no way to accurately measure the number of users who would be affected by rolling the root KSK, even though there was a belief that better measurements may become available for future KSK rollovers. The consensus of those involved in the discussions was that the ICANN should proceed with rolling the root zone KSK in a timely fashion while continuing outreach to ensure that the word of the rollover reach as wide an audience as possible."[38]

After two months, 20 parties from many ICANN communities commented on the new plan.[39] ICANN org summarized the comments, and created a revised plan based on the comments.[40] The ICANN Board then requested advice from Root Server System Advisory Committee (RSSAC), Security and Stability Advisory Committee (SSAC), and Root Zone Evolution Review Committee (RZERC) on the new plan.[41] RSSAC[42], SSAC[43], and RZERC[44] each replied with extensive commentary on the plans. As the Board was considering the comments from RSSAC, SSAC and RZERC, ICANN org published *What To Expect During the Root KSK Rollover*[45] to help the community understand what would and would not be seen on 11 October 2018. The ICANN Board approved proceeding with the new plan on 18 September 2018.[46]

8. Rolling the KSK in 2018

After the Board approval for the rollover, ICANN kept up its communication efforts to find operators of validating resolvers who had not yet configured KSK-2017 as a trust anchor.

On 11 October 2018, the Root KSK Operator published a root zone with DNSKEY record set signed by KSK-2017 for the first time. This step represented the actual rollover and the change produced only a very few minor observable effects on the global DNS.[47] On 13 October 2018, less than 48 hours after the key change, the DNS Operations, Analysis, and Research Center (DNS-OARC)[48] hosted an informal technical panel about the rollover at a meeting in Amsterdam.[49] The presentation[50] included many comments and questions from the audience.

---

[36] See https://www.icann.org/en/system/files/files/steps-of-the-ksk-roll-already-performed-in-2017.pdf
[37] See https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en
[38] See https://www.icann.org/news/blog/announcing-draft-plan-for-continuing-with-the-ksk-roll
[39] See https://mm.icann.org/pipermail/comments-ksk-rollover-restart-01feb18/
[40] See https://www.icann.org/en/system/files/files/report-comments-ksk-rollover-restart-23apr18-en.pdf
[41] See https://www.icann.org/resources/board-material/resolutions-2018-05-13-en#1.g
[42] See https://www.icann.org/en/system/files/files/rssac-039-07aug18-en.pdf
[43] See https://www.icann.org/en/system/files/files/sac-102-en.pdf
[44] See https://go.icann.org/2J8iWMX
[45] See https://www.icann.org/en/system/files/files/ksk-rollover-expect-22aug18-en.pdf
[46] See https://www.icann.org/resources/press-material/release-2018-09-18-en
[47] See https://www.icann.org/news/announcement-2018-10-15-en
[48] See https://www.dns-oarc.net/
[49] See https://indico.dns-oarc.net/event/29/timetable/#all.detailed
[50] See https://youtu.be/yT51FwPG0jE?t=4230

There were only a few reports of resolver outages after 11 October 2018. Two ISPs were reported in the press as having problems, but no one in the DNS community was able to gain further information from either of those ISPs indicating whether or not the rollover had been a cause of the reported problems. In *Operational Report on the Root DNSSEC Key Signing Key Rollover*,[51] the root server operators said that "that there was no impact on the root server system as consequence of the KSK rollover".

Traffic to the root servers did change somewhat due to the rollover. ICANN org is constantly monitoring data about queries being sent to various root server operators. After the rollover, the overall rate of queries for the root's DNSKEY record set doubled, although that traffic increase is still just a tiny fraction of the traffic to the root servers.

The cause of the increase is not yet understood and is under investigation. The increase can be seen here 48 hours after the rollover as the difference between the red line (the number of queries measured around the time of the rollover) and the light green line (the same measurement, but a week earlier):

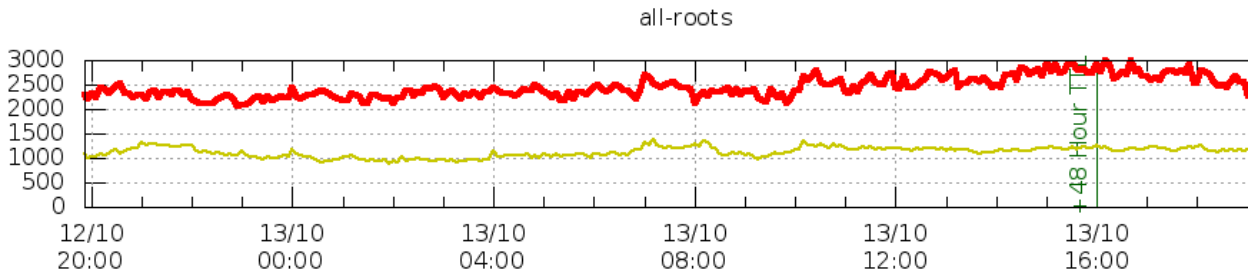

Figure 3. Increased rate in queries for the root DNSKEY RRset after the rollover

Data from resolvers using *Signaling Trust Anchor Knowledge in DNSSEC* (RFC 8145) continues to be sent to the root servers. The data continues to be puzzling. A resolver with only KSK-2010 configured as a trust anchor would not able to perform any successful DNSSEC validation after 13 October 2018. However, even months after the rollover, over 9000 resolvers are reporting that they have only KSK-2010 as a trust anchor.

9. Revoking and Removing the Old Key in 2019

On 11 January 2019, the root zone was published with KSK-2010 marked as revoked according to the mechanism described in *Automated Updates of DNSSEC Trust Anchors* (RFC 5011). The revocation only affected resolvers that implement RFC 5011; other resolvers should not have even seen the change. Although this step had been planned for many years, ICANN org reminded the community before it occurred.[52]

ICANN and the DNS community monitored root server traffic and DNS technical forums after the revocation was introduced to the root zone. There were no public reports of any Internet users affected by the revocation. Most root servers saw an increase in the percentage of root

[51] See https://go.icann.org/2NZABoD

[52] See https://www.icann.org/news/blog/icann-is-revoking-the-old-key-signing-key-this-week

DNSKEY queries relative to all queries.[53] The cause for this increase, which appears to be independent of the increase after the rollover, is not yet understood and is under investigation. The increase can be seen here 48 hours after the rollover as the difference between the red line (the number of queries measured around the time of the rollover) and the light green line (the same measurement, but a week earlier):

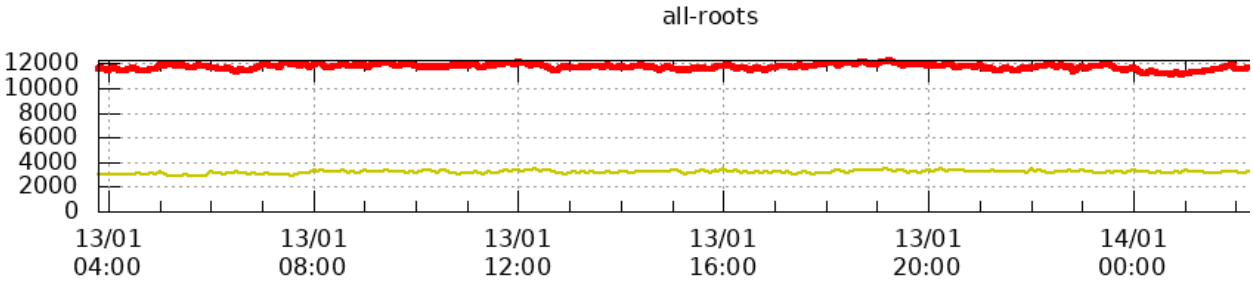

Figure 4. Increased rate in queries for the root DNSKEY RRset after the revocation

This document is being published before the last two steps of the rollover process have been taken. Those steps are:

- On 22 March 2019, the root zone will no longer be published with KSK-2010 in the DNSKEY record set. This step is not expected to have any consequence on validating resolvers because KSK-2010 has not been used for signing the DNSKEY records since the rollover on 11 October 2018.

- During root key ceremonies held in the second and third quarters of 2019, the Root KSK Operator will remove KSK-2010 from the HSMs that are used to sign the root zone. This step will not affect the DNS because these keys are simply stored in the devices, and are not visible on the Internet.

10. Rollover Communications

Coordinated and clear communication was a critical element of the KSK rollover. ICANN's communications outreach was aimed at helping change the KSK with little or no disruption to the Internet. Because the validating resolvers are managed only by their operators, there was no means to measure or control all of the elements involved in the rollover. The strategy focused on publicizing the broad message that the root zone KSK is changing, with more detailed supporting documents for those who would need it.

Complicating this effort was the difficulty identifying everyone who needed to be made aware of the new key. A definitive contact list of resolver operators does not exist, which means many modern outreach tools were not available. Without the ability to create demographic categorizations, tailored messaging was particularly difficult. Materials had to appeal to both novice and advanced operators, and to address the wide variety of software tools and processes in place. There were no means to estimate progress, measure saturation of the message, or track the most effective channels for communications. The long, slow pace of the

[53] See https://mm.icann.org/pipermail/ksk-rollover/2019-January/000630.html

project presented an additional challenge: keeping the appropriate audiences both adequately prepared and engaged throughout the rollover.

ICANN org participated in the communications effort by speaking at Internet and DNS operators' events, and other regional events. These presentations were designed to appeal to audiences that had a vested interest in DNSSEC. The talks were designed to build public trust in the operation of the KSK by giving as much information as possible as early as possible. There were a few rounds of these talks: the first round described the operational plans, the second described the early progress of the steps, and the third described the delay decisions.

ICANN org sent notices to some technical constituencies to raise their awareness of the KSK rollover so that they could spread the word to their members. For example, messages went to all top-level domain (TLD) operators (even though there was little to no impact on TLD operations) because they might get questions from stakeholders. ICANN org also encouraged public resolver operators to check their readiness for the rollover. ICANN org asked telecommunications regulators, Government Advisory Committee (GAC) members, and Internet Exchange Point organizations (IXPs) for assistance in reaching network operators.

ICANN's regional staff gave presentations at local DNS-related meetings that were not as technically focused as the operator meetings. In addition, some presentations were given by community members on behalf of ICANN. For example, some events were covered by local Trusted Community Representatives (members of the community who regularly participate in the root key ceremonies) and local SSAC members. There was also extensive outreach through social media, particularly Twitter, and ICANN blog posts.

Finally, ICANN org also engaged with the developers of validating resolvers and other DNSSEC-related software. These efforts led to software improvements and more outreach to their customers to preparing for the rollover.

11. Conclusions from the Rollover

In the course of the process, ICANN and the technical community learned many things that can apply to future rollovers. This section summarizes some of the most salient of those lessons.

Resolvers

It is impossible to predict how resolvers will react to KSK changes – The community was surprised by the lack of problems on 11 October 2018 when the signature on the root zone's DNSKEY set was changed. It was surprised again on 11 January 2019 when many resolvers started sending more DNSKEY queries to the root after KSK-2010 was revoked. It is now clear that the diversity of resolver software and configurations makes predicting how the overall system will act little more than guesswork, even with extensive testing ahead of time. In addition, the lack of good mechanisms to report how resolvers are configured blinds the community from knowing how ready the DNS ecosystem is for updates of any kind, not just for the KSK.

Having two 2048-bit KSKs caused no noticeable harm – Early in the rollover planning, there was concern that having both KSK-2010 and KSK-2017 would cause failure in some resolvers due to the size of the DNSKEY record set causing message fragmentation. The KSK rollover generated no evidence to support that concern.

RFC 8145 telemetry has many odd behaviors – The *Signaling Trust Anchor Knowledge in DNSSEC* (RFC 8145) data received from the root servers included reports from resolvers that were not ready for the rollover, but clearly have no users, making the data much less useful than hoped. Also, the data received after 11 January 2019 indicates that some implementations are actually reporting all records from the DNSKEY records in the root zone, not just from trust anchors. We reach this conclusion because some instances were reporting using the revoked KSK-2010 key as a trust anchor.

Some resolver operators do not understand what their resolvers do – During ICANN's outreach efforts, many operators asked questions that indicated that they did not understand what the various settings in their configurations did. They could not determine if they were using automatic updates of the KSK or even if they were using DNSSEC validation. As a result, doing surveys of operators did not give reliable results.

Outreach

Vendor outreach increased readiness – ICANN's engagement with vendors of resolver software showed direct results. Vendors fixed bugs, expedited revised software versions to resolver operators, and increased communications between some of the vendors and their users about the KSK rollover, particularly about using automated updates for trust anchors.

A long rollover process can have negative consequences – The decision to have a long period between the publicity launch for the rollover and the actual rollover event made the communication impact less effective. The long period was caused by a few factors, such as wanting to align the current KSK operations and the existing institutional schedule. The original plan intended a two year period from when KSK-2017 was created to when it was supposed to be used for signing. This created a lack of urgency among the operators of validating resolvers, and some did not pay attention to ICANN's communications. It also made choosing the particular operator venues for the communications difficult.

ICANN cannot determine which general outreach efforts helped prepare for the rollover – ICANN org used a wide range of methods to publicize the rollover, such as speaking engagements at operators' events and announcements in social media. However, there was scant feedback to those efforts, so it was not clear which were more effective in reaching the operators of validating resolvers. The messaging to end users was, in essence, "this information does not pertain to you, but please pass it along to the operator of your resolver". There were no metrics and extremely little feedback indicating which strategies were most effective.

The realtime testbed was not effective – The design of the testbed (using subzones under icann.org with testbed trust anchors) confused many users. Of the hundreds of users of the testbed, only a tiny fraction responded to requests for feedback on the testbed, and of those, many didn't understand what they were testing.

The result of the rollover process was the KSK being changed with only a very small amount of disruption visible to Internet users. Thus, the most significant conclusion to be drawn from the process for this first rollover was that it was an overwhelming success.