

Plan for Continuing the Root KSK Rollover

ICANN Office of the CTO

01 February 2018



1. History

On 27 September 2017, the ICANN organization announced¹ that it was postponing the root KSK rollover originally scheduled for 11 October 2017. The postponement was based on newly discovered information concerning validating recursive resolvers that might not be ready for the rollover.

After the postponement, ICANN org researched the new data to determine if it could be useful in determining when to roll the root KSK. On 18 December 2017, the ICANN org reported² to the community the results of its preliminary research. In that report, we detailed that the collected data does not afford any clear explanation as to why so many resolvers appeared to still be using only the earlier KSK. As a result, we asked for community input on how to proceed.

Specifically, ICANN org asked the community, on the ksk-rollover@icann.org mailing list, how we could best determine whether to proceed with the root KSK rollover.

2. Community Feedback

An active discussion ensued on the mailing list³. Many participants offered specific views on what should constitute ICANN's next steps. While there was a wide range of suggestions, the vast majority supported the view that the KSK rollover should proceed in a timely fashion.

As background, RFC 8145⁴, *Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)*, is a protocol that allows a validating recursive resolver to send data to root zone operators about the trust anchors that the resolver has installed. The purpose of this was to get a rough assessment of which resolvers were ready for the rollover. However, because the DNS

¹ See <https://www.icann.org/news/announcement-2017-09-27-en>

² See <https://www.icann.org/news/blog/update-on-the-root-ksk-rollover-project>

³ See <http://mm.icann.org/pipermail/ksk-rollover/2018-January/date.html>

⁴ See <https://www.rfc-editor.org/rfc/rfc8145.txt>

allows forwarding of queries, most of the messages received at the root zone that indicated that particular resolvers were not ready for the rollover were not helpful.

Even after a concerted effort, ICANN org could often not determine which resolvers sent the message (such as when the resolver had a dynamic address), so there was no way to determine how many users would be affected by the rollover or why those resolvers had not updated their trust anchors. Additionally, even when ICANN org could identify the specific resolver, efforts to contact the operator were often unsuccessful.

The discussion on the mailing list took these limitations into account. There was wide agreement during the discussion that there is no way to accurately measure the number of users who would be affected by rolling the root KSK, even though better measurements may become available for future KSK rollovers. There was also discussion of a future protocol⁵, *A Sentinel for Detecting Trusted Keys in DNSSEC*, that might give more valuable information for future root KSK rollovers. That in turn, prompted a discussion about how long it might take to standardize and deploy such a protocol.

3. Plan to Roll the Root KSK

Before the postponement, ICANN org had published an extensive set of plans for rolling the root KSK⁶. Most of these plans were fully executed before the postponement. (Using the steps described in the Operational Implementation Plan, the postponement occurred during Phase D.) Based on the feedback we received during the discussion, ICANN org proposes the following plan for moving forwards.

3.1 Roll the Root KSK on 11 October 2018

The ICANN org plans to take the next step of rolling the Root KSK on 11 October 2018, assuming that such a step is approved by the ICANN Board of Directors. This follows the same steps that were outlined in the published plans but with the rollover date moved forward exactly one year. The discussion with the community did not result in any specific measurable criteria to stop the rollover over from progressing. The ICANN org therefore intends to proceed with the rollover and will request a resolution from the ICANN Board of Directors affirming this plan.

The date of 11 October 2018 was chosen to give the community time to review the plan with a public comment period and to give the ICANN Board of Directors time to approve it after consulting any parties it may wish to contact. This date also gives ICANN org plenty of time to publicize the new date and attempt to get more validating resolver operators ready for the roll over. (Based on the way that KSKs are published in the root zone, the only available dates in 2018 for the rollover are 11 April 2018, 11 July 2018, and 11 October 2018.)

⁵ See <https://tools.ietf.org/html/draft-ietf-dnsop-kskroll-sentinel>

⁶ See the section on “Operational Plans” at <https://www.icann.org/resources/pages/ksk-rollover>

3.2 Continue Extensive Outreach

The ICANN org will increase its efforts to reach the operators of validating recursive resolvers to explain how they can prepare for the KSK rollover ahead of the new date. This outreach will allow ICANN org and others in the community to document any common or frequent reasons for resolvers' having only KSK-2010. If new reasons emerge, ICANN org will tailor additional messaging and possibly take additional mitigating steps (such as talking to vendors of DNS systems if new implementation-specific issues are discovered).

Implicit in the outreach plan is the same assumption that the community had for the earlier (postponed) plan: there will likely be some systems that will fail to resolve names starting on the day of the rollover. The outreach will attempt to minimize the number of affected users while acknowledging that the operators of some resolvers will be unreachable.

ICANN org is particularly interested in hearing additional community ideas as to ways we might increase outreach to operators of validating resolvers, so they will be ready for the rollover.

3.3 Publish More Observations of Trust Anchor Report Data

ICANN org will publish monthly snapshots of the RFC 8145 trust anchor report data that we receive from several root servers. We will encourage the community to help identify particular resolvers that are not ready for the rollover, and also ask that it analyze all available data for other valuable insights. ICANN org will continue to do this after the rollover, for a period of at least two months.