At-Large Workspace: Plan to Restart the Root Key Signing Key (KSK) Rollover Process

Public Comment Close	Statement Name	Status	Assignee (s)	Call for Comments Open	Call for Comments Close	Vote Open	Vote Close	Date of Submission	Staff Contact and Email	Statement Number
02 April 2018	Plan to Restart the Root Key Signing Key (KSK) Rollover Process	ADOPTED 13Y, 0N, 0A	Sebastien Bachollet Hadia Elminiawi Javier Rúa-Jovet John Laprise Lutz Donnerhacke	01 April 2018	02 April 2018	03 April 2018	06 April 2018	02 April 2018	Paul Hoffman paul.hoffman@icann.org	**AL-ALAC-ST-0418-02-01-EN**

Hide the information below, please click here >>

Brief Overview

Purpose: This Public Comment seeks public review of the plan to roll the root key signing key (KSK). The plan includes more publicity about being prepared for the rollover, analysis of the data being seen indicating the level of preparedness, and the actual rollover itself on 11 October 2018.

Current Status: The technical community discussed possible ways to determine when to roll the root KSK on the ksk-rollover@icann.org mailing list, and ICANN used that discussion as the basis for this plan.

Next Steps: ICANN organization will prepare a final plan that bases on the input from the public comments and present a full plan to the ICANN Board for approval.

Section I: Description and Explanation

The Plan for Continuing the Root KSK Rollover (https://www.icann.org/en/system/files/files/plan-continuing-root-ksk-rollover-01feb18-en.pdf [PDF, 93 KB]) describes how ICANN intends to roll the root key signing key (KSK). It is based on input from the community that followed ICANN's earlier decision to postpone the rollover. In summary, the plan is to roll the root KSK on 11 October 2018 after more publicity that is intended to help prepare operators for the rollover and making more data about the preparedness available.

Section II: Background

In 2009, the Root Zone Management partners (ICANN and Verisign, also called the "RZM partners") collaborated to deploy Domain Name System Security Extensions (DNSSEC) in the root zone, which culminated in the first publication of a validated signed root zone in July 2010. That signature was based on a key signing key (KSK) that is maintained securely by ICANN. It was later agreed that "Each [root zone] KSK will be scheduled to be rolled over through a key ceremony as required, or after 5 years of operation."

In December 2014, ICANN solicited volunteers from the community to participate with the RZM Partners in a Design Team to develop the Root Zone KSK Rollover Plan. That plan was put out for public comment on 6 August 2015, and was published on 7 March 2016.

On 27 September 2017, ICANN announced that the plan to change the cryptographic key that helps protect the Domain Name System (DNS) is being postponed. On 18 December 2017, ICANN began collecting comment from the community about the acceptable criteria for proceeding with the KSK rollover. The result of that discussion on the ksk-rollover@icann.org mailing list is the plan that is now open for comment.

Section III: Relevant Resources

Plan for Continuing the Root KSK Rollover: https://www.icann.org/en/system/files/files/plan-continuing-root-ksk-rollover-01feb18-en.pdf [PDF, 93 KB]

Section IV: Additional Information

- *Root Zone KSK Rollover*: https://www.icann.org/resources/pages/ksk-rollover
- *Root Zone KSK Rollover Plan*: https://www.iana.org/reports/2016/root-ksk-rollover-design-20160307.pdf [PDF, 1.19 MB]
- *KSK Rollover Postponed*: https://www.icann.org/news/announcement-2017-09-27-en
- *Update on the Root KSK Rollover Project*: https://www.icann.org/news/blog/update-on-the-root-ksk-rollover-project

Section V: Reports

Staff Contact

Paul Hoffman
paul.hoffman@icann.org

FINAL VERSION TO BE SUBMITTED IF RATIFIED

The final version to be submitted, if the draft is ratified, will be placed here by upon completion of the vote.

FINAL DRAFT VERSION TO BE VOTED UPON BY THE ALAC

The final draft version to be voted upon by the ALAC will be placed here before the vote is to begin.

The ALAC and At-Large Community understand the need to roll the KSK but parts of the community have strong concerns for the potential impact on users world-wide.

We believe that a holistic review is needed including a risk assessment of the alternatives, in time for further discussion at ICANN62. The assessment should include then current information related to the RFC 8145 trust anchor reports, the prognosis for availability of the in-development IETF “sentinel” mechanism and the potential for using the sentinel mechanism to create a greater level of comfort prior to the KSK rollover.

In parallel, ICANN should ramp up its awareness campaign using all possible conduits to reach ISP, telcos, and governments as well as critical sectors who must be able to continue to function post-rollover and who may be in a position to communicate with key DNS providers in their regions. Banking is one such sector that must not be put offline and which may have valuable contacts in their local areas. RIRs may have good contact information for large ISPs and other large users in their regions.

ICANN should also make available an information packet, in at least the languages ICANN normally supports, and preferably more, which will allow users and businesses to understand the issue (i.e. in simple terms) and tell them what they need to do/ask with regard to their local ISPs.

ICANN should provide a simple test web address and/or application that will allow users to verify if the resolver they typically use is DNSSEC-aware. If it is not, then they are likely to be unaffected by the KSK rollover. If their resolver is DNSSEC-aware, then they should be told what to do to try to verify that their provider is aware of and prepared for the rollover (recognizing that the technical support most end-users can contact will not likely be aware of terms such as DNSSEC, KSK or Rollover). http://dnssec.donnerhacke.de is an example on which such a tool may be modelled.

ICANN should provide a list (either viewable or searchable) of DNS resolvers known to be DNSSEC enabled for which we definitively know either do or do not have the new trust-anchor installed, and the awareness campaign should describe how end users can check this list. An automated app that users could run on various platforms would be even better.

Lastly, the At-Large Community has concerns that the rollover is scheduled to take place on a Thursday (and most likely Friday in some parts of the world). That seems like a plan designed to maximize and prolong any problems. We would like to understand the potential and possibility of a minimal delay to ensure that the day-of-the-week issue reduces impact instead of increases it.

FIRST DRAFT SUBMITTED

The first draft submitted will be placed here before the call for comments begins.

Another proposed Draft (Hadia)

The At– Large Advisory Committee (ALAC) of the ICANN takes this opportunity to thank ICANN org for opening for public comments the plan to restart the Root Key Signing (KSK) Rollover Process and is glad to provide its comments herein

The postponement of the KSK roll over on 11 October 2017 was based on newly discovered information concerning validating recursive resolvers that might not be ready for the rollover, to this end ICANN org researched the new data to determine if it could be useful in determining when to roll the root KSK, however on 18 December 2017, ICANN org reported to the community the results of its research, in that report, ICANN detailed that the collected data does not provide any clear explanation as to why so many resolvers appeared to still be using only the 2010 KSK. Most of the messages received at the root zone that indicated that particular resolvers were not ready for the rollover were not helpful, ICANN org could often not determine which resolvers sent the message or why those resolvers had not updated their trust anchors. Additionally, even when the resolvers were identified efforts to contact the operator were often unsuccessful.

Taking into consideration that

- It is not for seen that new reliable data will be available soon.
- There is nothing to indicate that operators of DNS resolvers that are operating with only the 2010 KSK will fix their systems soon.
- The existence of DNSSEC is important to protect the integrity of the DNS data, where DNSSEC applies digital signatures to DNS data to authenticate the data's origin and verify its integrity as it moves throughout the Internet.
- It was agreed that each root zone KSK will be scheduled to be rolled over through a key ceremony as required, or after 5 years of operation and 6 years have already elapsed
- Postponing the KSK rollover might put the security of the DNS at risk, where the key could be compromised, lost among others risks stated in the SSAC Advisory on DNSSEC Key Rollover in the Root Zone on 7 November 2013.

The ALAC recognizes that while it is important to guarantee that the users affected are as minimum as possible it is equally important for the security of the DNS to proceed with the KSK Rollover. To this end the ALAC supports the proposed plan for the KSK rollover while highlighting the importance of an extensive outreach plan and requesting a detailed PR plan that includes all the necessary information and documents, and post-rollover recovery guides for unprepared DNS resolvers, This is in addition to the recommendations previously mentioned in the

---

The ALAC is pleased to have the opportunity to comment on the “Plan to Restart the Root KSK Rollover Process”.

DNSSEC changes the nature of the most decentralized service of the Internet, the DNS, fundamentally. It transforms a lightweight "lookup table" into a trustworthy database. It's trust is made up of two important fragments: solid cryptography implementations and transparent operations.

DNSSEC anchors the zone trust by hopping the delegation hierarchy backwards. But this process does terminate at the root. Implementing the trust for the root itself is incredible hard, ultimately it's not a technical problem at all. At this point, the trust (KSK) information needs to be put in the hands of countless network operators all over the world. This task is attributed to ICANN. AtLarge has to do it's own outreach on this subject using it's own distributed structure.

Cryptographic elements always have a lifetime, if they are keys or algorithms. It is good operational practice to change the keys regularly in order update the material and to ensure, that all processes are still in place. Changes of algorithms require a working key change process. Therefore the important root keys (where all the trust is rooted) need to be changed, too.

During the preparations of the rollover, various issues arose especially from embedded and operator-less devices. Efforts were made to estimate the impact of an KSK change for affected user groups. But all the data is still vague.

The proposed plan is to schedule the rollover for October this year, missing two possible earlier dates. The gained time should be used for intensify the communication with the network operator crowd out there. Waiting for new protocols to be deployed in order to guess more accurately is not an option. So the communication should concentrate on preparation check lists and post-rollover recovery guides for validating recursors.

ALAC supports this plan: Shifting the schedule by exactly one year makes is much more easy for outsiders to keep in time with the activities. April is clearly to short for the necessary communication. Starting in July will collide with holiday breaks in several countries. Because we depend on the operators, the October date is more appropriate in terms of workload and memorizing the important dates.

ICANN should provide a test page for the end users, which tell them in a very simple way, if they are affected by the KSK rollover or not (example http://dnssec.donnerhacke.de/). This page should offer a link to the gathered information from RFC 8145: The end user can enter the IP of the resolver (preferably automatically detected using a Nonce-FQDN) to check, if the active resolver is already trusting all active keys. This tool should be stay in place for further rollovers.

There are some recommendations:

- Do not publish changes near the end of the week (Friday to Sunday can not considered as work days), choose only Tuesday or Wednesday.
- Because it's impossible to gather detailed information about every possible situation, prepare a worldwide anti-blame PR action. Try to get this event into the news, it has to be broadcasted in the same way as the Year2000 problem. Ensure, that every problem during the roll over will be attributed to the ISPs. Strictly speaking try to blame the ISPs, hosters, and IoT companies beforehand through the press, (social) media, and TV shows. This action has to reach the climax some weeks before the date.
- Use the opportunities of the distributed ICANN sub-organisations (for AtLarge: ALSs) to distribute knowledge into the communities.
- Allow the end users to self-test their own environment by providing a appropriate web-page.

The rise of IoT starts to create swamps of non updateable network devices. If the KSK rollover is further delayed, more and more such devices will be deployed, all of them unable to deal with an upcoming KSK change. The only chance to get those developers and companies on board is to rollover the KSK. Regularly.

Alternative Text: (courtesy of John Laprise)

Whereas:

- SSAC has issued two advisories on the KSK Rollover
- [SAC063] SSAC Advisory on DNSSEC Key Rollover in the Root Zone (07 November 2013)
- [SAC073] SSAC Comments on Root Zone Key Signing Key Rollover Plan (05 October 2015)
- ICANN issued a revised KSK Rollover draft plan for public comment and plans to execute the rollover in October 2018
- The KSK Rollover was a topic of intense discussion during the ICANN61 meeting in Puerto Rico
- ALAC affirms that the KSK Rollover is necessary
- ALAC is cognizant of the nature of the risks of action and delay but not their relative weights

Resolved:

The ALAC advises the Board

- to provide a holistic risk assessment to the community on the KSK Rollover at ICANN62 comparing the relative risks of implementing the KSK rollover as provided in the revised plan vs. further delaying the KSK rollover. The risk assessment should include an evaluation of both the technical and reputational risks to the security and stability of the Internet and should reflect opinions of the SSAC, RSAC, and Risk Committee
- To direct ICANN to develop a robust ISP mitigation strategy in the event of resolver failure affecting end users and communicate it to the community
- To provide clarification on the communication plan. ALAC notes that the recipients for the KSK rollover communication plan considerably overlap those of the DNSSEC implementation

Furthermore

- Upon receipt of the risk assessment at ICANN62, ALAC will be better prepared to offer advice on the KSK Rollover Plan in a timely fashion prior to its proposed execution in October 2018