Registries Stakeholder Group Statement

Issue: **Plan to Restart the Root Key Signing Key (KSK) Rollover Process**

Date statement submitted: **2 April 2018**

Reference URL: https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en

Background[1]

On 27 September 2017, ICANN announced that the plan to change the cryptographic key that helps protect the Domain Name System (DNS) was being postponed.

On 18 December 2017, ICANN began collecting comments from the community about the acceptable criteria for proceeding with the KSK rollover, what resulted in the Plan to Restart the Root KSK Rollover Process, which is up for public comment.

The plan includes more publicity about being prepared for the rollover, analysis of the data being seen as indicating the level of preparedness, and the plan for the actual rollover on 11 October 2018.

Registries Stakeholder Group (RySG) comment:

The RySG notes that ICANN announced on 27 September 2017 that the plan to change the cryptographic key that helps protect the Domain Name System (DNS) would be postponed. On 18 December 2017, ICANN began collecting comment from the community about the acceptable criteria for proceeding with the KSK rollover.

The RySG recognizes the current challenge faced by ICANN in conducting the first KSK rollover since its introduction in July 2010. As a general statement, we support the proposed plan to delay the KSK rollover until the proposed date of 11 October 2018 and believe that ICANN should be open to further extending the timeline to allow more comprehensive study of the potential impacts. Most importantly, ICANN must capitalize on the time until rollover to undertake following publicity and awareness-building to help prepare operators for the rollover and to making more data about preparedness available. Noting that this is the first rollover of the KSK, the RySG recognizes its precedent-setting importance and the need to get it right rather than rush to a deadline.

[1] *Background: intended to give a brief context for the comment and to highlight what is most relevant for RO's in the subject document – it is not a summary of the subject document.*

The RySG understands that there is little urgency to rush the KSK rollover because (a) ICANN prudently chose a 2048-bit RSA key initially, and this key size is still appropriate for long-term security; and (b) the KSK is well-managed under DNSSEC practice statements. Nevertheless, it is important to eventually change the KSK, both to follow best practices for key management (which would dictate that the key should have already been changed), and to ensure that the rollover process has been conducted with operational excellence and proven for future use. Failure to do so could risk erosion of trust in DNSSEC.

As such, the RySG believes it is worth taking the time to get this right, including at least the one-year delay ICANN has already introduced, while ensuring the development of key metrics and measures of success. ICANN should be open to considering further delays if engaged parties believe they will improve preparedness and awareness, improve upon limited data available about the impact, or minimize breakage. The RySG is keenly aware that an individual registry operator's own excellence with DNSSEC would be undercut if the root KSK rollover fails.

The RySG notes potential risks that would arise from a rollover that results in exceeding the acceptable breakage levels, including DNS root fragmentation, reduced trust in the DNS, rise of alternative namespaces, as well as fostering adoption of alternative governance models. It is important to prioritize the stability, security and resiliency of the DNS over strict adherence to a proposed timeline for its own sake.

Further, the RySG believes a rollover from one KSK to another should be managed separately from *rollout* of a new KSK – which just makes it available for future rollover. Rollout should be treated as a community activity with clearly defined success criteria. ICANN should set clear goals for how many resolvers have the new KSK, and ensure that those goals are met before rolling over irreversibly from the old KSK to the new.

General Comments

Support meaningful analysis of whether further postponement of the rollover is appropriate in light of ongoing technological developments.

ICANN's decision to postpone the rollover was based on the concern that there was, and continues to be, a lack of understanding of why resolvers were not properly configured, and they needed time to investigate. Ideally, that investigation would have revealed a set of clear causes for the improper configuration, allowing further communication and actions to be targeted at addressing those specific issues. But in the end, the analysis was not as conclusive as hoped. The RySG is very concerned that the data and related observables that led to the initial postponement of the initial KSK rollover continue to tell a worsening story, but understands that there is some indication that the worsening story may have more to do with the measurement apparatus than the state of deployment itself. The fact that the measurement apparatus has such shortcomings is a cause for concern in its own right.

We suggest that ICANN monitor, and sponsor if needed be, developments within the technical community that could lead to effectively measuring the potential break-up of the DNSSEC validation

chain that could occur during the roll-over. Some examples include (1) the ongoing work to deploy the A 5 Sentinel for Detecting Trusted Keys in DNSSEC ("KSK sentinel") that could provide a better understanding of impact and clues for how to minimize negative impact in rollover; (2) ad-network based measurement of end-user perception of the DNS system; (3) a possible new ZSK signing only a test TLD, and that ZSK being signed only by the new KSK. We believe that ICANN should be open to further delay to allow the continued development of such technologies that can better measure the impacts of the rollover and whether risk thresholds are being met. ICANN should also foster community discussion of the tradeoffs between pushing forward with the transition and further delay.

Prioritize outreach to operators.

We were informed by an IP address registry that at this point, no regional outreach has been conducted through the RIRs that allocated IP address to networks knowingly not updating their KSK. Such outreach could foster adoption of automatic roll-over procedures, and we strongly encourage that to happen. If further postponement is necessary to carry out robust outreach, then this warrants consideration and further discussion within the community.

Provide a complete, updated project plan to the community for review and comment.

While the comment period provided a high-level summary of the additional research carried out since the initial postponement of the rollover there it is unclear whether and how ICANN intends to apply these findings to the overarching project plan. ICANN does not explicitly state whether it intends to follow the previously published rollout plan, not to mention providing updated timelines and contingency mechanisms based upon the additional research. We recommend that the full project plan be revised and published to the community for consideration and comment, with any revisions explicitly noted.

Review of Previous SSAC Advice

The RySG notes that ICANN's Security & Stability Advisory Committee (SSAC) issued an advisory on DNSSEC Key Rollover in the Root Zone, dated November 07, 2013 (SAC063). In this advisory, the SSAC gave advice on relevant operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services). The SSAC proposed the following five recommendations for consideration and discussion, which the RySG flags for review and further attention, particularly where the SSAC's recommendations were either not implemented, or were implemented without sufficient rigor, effectiveness or transparency. Following our review of these SSAC recommendations, the RySG has the following input and questions:

- **Recommendation 1**: Internet Corporation for Assigned Names and Numbers (ICANN) staff, in coordination with the other Root Zone Management Partners (United States Department of Commerce, National Telecommunications and Information Administration (NTIA), and

VeriSign), should immediately undertake a significant, worldwide communications effort to publicize the root zone KSK rollover motivation and process as widely as possible.

- **RySG**: What actions has ICANN taken thus far and what more needs to be done to accomplish the goal?

- **Recommendation 2**: ICANN staff should lead, coordinate, or otherwise encourage the creation of a collaborative, representative testbed for analyzing behaviors of various validating resolver implementations, their versions, and their network environments (e.g., middle boxes) that may affect or be affected by a root KSK rollover, such that potential problem areas can be identified, communicated, and addressed.

  - **RySG**: What, if any, steps has ICANN staff taken toward fulfilling this recommendation? What has ICANN learned about the different behaviors and implementations that could be impacted by a rollover?

- **Recommendation 3**: ICANN staff should lead, coordinate, or otherwise encourage the creation of clear and objective metrics for acceptable levels of "breakage" resulting from a key rollover.

  - **RySG**: In the prior plan, ICANN defined the acceptable level of breakage as less than 0.5% of the estimated Internet end-user population. ICANN should confirm that the principles and thresholds established in the prior plan apply to the rescheduled rollover. Further, it is impossible to estimate or directly measure end user impact across billions of Internet users, and simply measuring impact to resolvers is a poor substitute due to variations in reach. How does ICANN intend to capture the impact to end users? Are there any metrics for how close to this level the current deployment of the new root KSK is (if the rollover were to occur today), and is there a way to estimate this as the October date approaches? Beyond that, how are risks associated with breakage being communicated?

- **Recommendation 4**: ICANN staff should lead, coordinate, or otherwise encourage the development of rollback procedures to be executed when a rollover has affected operational stability beyond a reasonable boundary.

  - **RySG:** Has this been developed? What criteria and thresholds have been set, and what methods will be used to determine whether thresholds have been reached given the impossibility of direct measurement? Who has authority to initiate rollback?

- **Recommendation 5**: ICANN staff should lead, coordinate, or otherwise encourage the collection of as much information as possible about the impact of a KSK rollover to provide input to planning for future rollovers.

- **RySG:** Is this data collection plan in place? If so, what are the metrics and measurables? Is delay to allow deployment of the KSK sentinel warranted to improve understanding of potential impact?

Conclusion

The RySG is concerned about the impact of the KSK Rollover (and its delay) on gTLD registry operator obligations for operationalization and full lifecycle management of DNSSEC (to include EDNS0 and EPP support). This underscores the need for proper diligence and relying party (i.e., validating recursive name server) preparedness at parent layers (i.e., the root ZSK and KSK) of the DNSSEC PKI before any changes are made, or else resolution of TLD and child domains will be disrupted, with corresponding implications for contractual compliance.

It is critical to the security, stability and resiliency of the DNS that DNSSEC management be rigorous -- well managed with operational excellence and well-documented procedures. With all the rigor and theatre around DNSSEC key ceremonies for the root, and the fact that there doesn't seem to be any pressing cryptographic necessity to force this initial KSK roll-over (arguably the most dangerous) at some specific date, getting it right with minimal negative impact is surely more important than simply getting it done by some arbitrary date.

References:

https://www.icann.org/en/system/files/files/sac-063-en.pdf
https://www.icann.org/en/system/files/files/plan-continuing-root-ksk-rollover-01feb18-en.pdf
https://www.icann.org/resources/pages/registries/registries-en
https://www.icann.org/news/blog/update-on-the-root-ksk-rollover-project