RSSACXXX: RSSAC Statement Regarding ICANN’s Updated KSK Rollover Plan 10 August 2018

1 Background

On 13 May 2018, the ICANN Board requested the Root Server System Advisory Committee (RSSAC), the Security and Stability Advisory Committee (SSAC) and the Root Zone Evolution Review Committee (RZERC) to provide the Board advice on the "Updated Plan for Continuing the Root KSK Rollover" and associated plan documents, and to report back to the Board by 10 August 2018 if possible.[1]

The DNS Key Signing Key (KSK) is used to cryptographically sign the Zone Signing Key (ZSK), which is used by the Root Zone Maintainer to then sign the root zone of the Internet's DNS. The updated plan calls for a KSK rollover that would take place on October 11, 2018. In this advisory, the RSSAC provides advice on the ICANN organization’s updated plan for continuing the root KSK rollover.[2]

RSSAC believes that the October 11th, 2018 rollover date is the most critical in the proposed timeline as it is the only date that may have any negative impact on the Root Server System, as it is on this date that the new KSK will be put into production use to sign the root zone. The discussion below relates primarily to the events on that day unless otherwise noted.

2 Scope of RSSAC's Advice

Per its Charter, the role of the RSSAC is to advise the ICANN community and Board on matters relating to the operation, administration, security, and integrity of the Internet's Root Server System (RSS).

Given its charter, the RSSAC *limits its comments to its scope (i.e., the impacts of the proposed KSK rollover timeline to the RSS)*. A broader set of issues such as communication and outreach, data analysis of potential breakage, risk assessment, and post roll issues may need to be addressed, but are outside of RSSAC’s scope.

With that in mind, the RSSAC offers the following reassurances and concerns regarding potential impacts to adopting the proposed “Operational Plans for the Root KSK Rollover” plan.

[1] See “Getting Additional Input on New KSK Roll Plan”, https://www.icann.org/resources/board-material/resolutions-2018-05-13-en#1.g

[2] See “Operational Plans for the Root KSK Rollover”, https://www.icann.org/resources/pages/ksk-rollover-operational-plans

3 Reassurances

There are a number of aspects of root server operation related to the KSK rollover that the RSSAC feels should not be of significant concern to the Board and the broader ICANN community.

First, the RSSAC reaffirms its commitment to serve the most recently available root zone data provided by IANA via the Root Zone Maintainer. This is originally expressed in RSSAC001 as:[3]

> *[E.3.2-D] All Root Servers will continue to serve precise, accurate zones as distributed from the Root Zone Maintainer.*
>
> *No Root Server has ever, or will ever, serve a zone that was modified following distribution by the Root Zone Maintainer. In any case, it would be impossible for an individual operator to modify the signed RRsets within the zone, now that it is DNSSEC-signed, without invalidating signatures. A Root Server Operator will not intentionally serve an older zone than current zone provided by the Root Zone Maintainer.*

Second, the RSSAC is confident that no problems or changes in traffic would arise on October 11th due to the sizes of DNS packets sent to and from root servers. The root zone has been operating with two published KSKs since July 11, 2017. The KSK rollover will consist of updating the signature records (RRSIGs) of the DNSKEY RRSets. The other content and the structure of the root zone will be left unchanged. As such, no change in request or response packet sizes are expected on October 11th. Any changes in recursive resolver behaviour are expected to result from the interpretation of the content. Note that the subsequently scheduled revocation of the original KSK, commencing January 11 2019 and scheduled for completion on March 22 2019, will entail serving slightly larger responses for certain queries to the root zone during this key revocation period.

Third, since mid-2017 ICANN's Office of the CTO (OCTO) has been receiving, and will continue to receive, real-time measurement data from 12 of the 13 root server identities. This data is updated every 60 seconds and sent directly to ICANN OCTO. It is also shared with all Root Server Operators (RSOs) via their collaboration system. These measurements have been designed in collaboration by ICANN OCTO and Verisign specifically to monitor changes to DNSSEC keys in the root zone. They were previously used in 2016 when the root zone Zone Signing Key (ZSK) length was increased to 2048-bits. These real-time measurements will be monitored by operators and OCTO staff very closely upon resumption of the KSK rollover plan. Should any problems or concerns arise, ICANN, in cooperation with its root zone management partners (IANA naming services provider and the root zone maintainer), can make the decision to execute its back out plan.

Fourth, ICANN can expect most RSOs to contribute full packet capture data (colloquially "DITL" data) on and around October 11th upon resumption of the KSK rollover plan. Typically the data is captured over a period of three days. Although such data is not generally useful for

[3] See "RSSAC001: Advisory on Service Expectation of Root Servers"

real-time decision making, it is valuable for post-facto analysis and may be of use to advise future rollovers.

Lastly, there will be close cooperation between IANA, OCTO, the Root Zone Maintainer (RZM), and the RSOs leading up to and throughout the entire event. The time of the rollover on October 11th (i.e. publication of the new zone file) will be agreed upon in advance, and progress will be clearly communicated to all parties. The RSOs are committed to being available and vigilant during the rollover to monitor their infrastructure for any indications that users or recursive name servers appear to be experiencing difficulties.

4 Items the ICANN Board should consider addressing

4.1 Potential increase in traffic to the RSS

RSSAC has heard from some members of the technical community that have expressed concern that an increase in traffic from misconfigured resolvers may occur after the October 11th, 2018 date in the rollover plan. However, RSSAC is not aware of any method able to estimate such a potential load increase. However, RSSAC believes that there is little risk of this occurring and that there will be no impact to the stability of the RSS even if such a load increase occurs.

4.2 Review of the published recoverability plans

The KSK rollover back out plan[4] was written in July of 2016, updated[5] in April of 2018, and may become a critical procedure that needs to be invoked immediately in case of KSK rollover failure. This document, its procedures and triggers should be reviewed by all parties in the rollover (RSOs, RZERC, and IANA) to ensure it remains adequate and implementable. RSSAC pledges that all of the RSOs will be prepared to participate in monitoring and measuring to ensure adequate data is available upon which a rollback decision can be made.

5 Conclusion

Although RSSAC identifies several technical items in this statement, we do not see a technical reason for these items to cause any delay in resuming the KSK rollover plan on the current proposed schedule.

[4] https://www.icann.org/en/system/files/files/ksk-rollover-back-out-plan-22jul16-en.pdf

[5] https://www.icann.org/en/system/files/files/2018-ksk-rollover-back-out-plan.pdf