ICANN BOARD INFO PAPER NO. 2017.09.23.1h

TITLE:	**KSK Roll Current Status and Possible Next Steps**
PROPOSED ACTION:	**The ICANN organization is directed to roll the DNS root KSK as soon as is practical** **For Board Consideration and Approval (see additional document for resolution language)**

EXECUTIVE SUMMARY:

The technical community has instructed ICANN organization to update the root zone key signing key (KSK), a multi-step process that will result in a new key that will be used by all resolvers that validate DNS responses using the DNSSEC protocol. The ICANN organization has already taken almost all of the preliminary steps towards updating the KSK, keeping the community informed along the way about the progress and involving the technical community in the planning and design efforts. The next major steps for rolling the root zone KSK happen on 22 September 2017 and 11 October 2017.

The ICANN Board has been kept abreast of the status and steps of the KSK roll, but has not formally approved the roll itself. This document provides background and explains the issues with the Board approving the KSK roll.

BACKGROUND:

In May 2010, ICANN published its "DNSSEC Practice Statement for the Root Zone KSK Operator"[1] (commonly called the "DPS"), which sets out its commitments and intentions in creating and maintaining the root zone KSK. Although most of the DPS talks about securely maintaining the KSK, Section 6.5 says:

> *Each RZ KSK will be scheduled to be rolled over through a key ceremony as required, or after 5 years of operation. [. . .]*

[1] *See* http://www.root-dnssec.org/wp-content/uploads/2010/06/icann-dps-00.txt

The first root zone KSK was published in July 2010. Members of the technical community began reminding ICANN organization of this commitment in 2013, ahead of the five-year anniversary of the creation of the KSK.

In November 2013, SSAC published SAC063, "SSAC Advisory on DNSSEC Key Rollover in the Root Zone"[2], which extensively described the need and risks of rolling the KSK for the root zone. Based on that document, in December 2014, ICANN solicited volunteers from the technical community to participate with the Root Zone Management (RZM) Partners, comprised of ICANN, Verisign, and U.S. Dept. of Commerce NTIA, in a Design Team to develop the Root Zone KSK Rollover Plan. The resulting report, "Root Zone KSK Rollover Plan"[3], was a comprehensive set of technical and operational recommendations intended to guide the RZM Partners in producing a detailed implementation plan for executing the first Root Zone KSK rollover. The Design Team report contained many recommendations as well as an assessment of the risks of performing the root key roll.

The ICANN organization evaluated public comments on the Design Team report and created a set of plans for implementing the KSK key roll. These include:

- "KSK Rollover Communications Plan"[4], detailing the ways that the ICANN organization will publicize the upcoming key roll to the various communities that need to be prepared

- "2017 KSK Rollover Operational Implementation Plan"[5], describing in detail the operational steps to accomplish the 2017 KSK Roll project, including the timeline of the process

- "2017 KSK Rollover External Test Plan"[6], covering the preparation of operational test environments, accessed by the general Internet public, to evaluate whether external systems are prepared to participate in the KSK roll

---

[2] *See* https://www.icann.org/en/system/files/files/sac-063-en.pdf
[3] *See* https://www.iana.org/reports/2016/root-ksk-rollover-design-20160307.pdf
[4] *See* https://www.icann.org/en/system/files/files/ksk-rollover-comms-plan-22sep16-en.pdf
[5] *See* https://www.icann.org/en/system/files/files/ksk-rollover-operational-implementation-plan-22jul16-en.pdf

- "2017 KSK Rollover Monitoring Plan"[7], describing the plan to monitor the effects of changing the trust anchor for the root zone in the traffic towards root servers

- "2017 KSK Rollover Systems Test Plan"[8], listing the actions needed to test changes to ICANN's infrastructure involved in the KSK roll

- "2017 KSK Rollover Back Out Plan", listing the anticipated deviations from the Operational Implementation Plan based on anomalies occurring while executing the operational plan https://www.icann.org/en/system/files/files/ksk-rollover-back-out-plan-22jul16-en.pdf

After public review of the plans and consultation with the RZM Partners, the ICANN organization began implementing the plans in October 2016. The two major streams of actions were public outreach and operational preparations. Public education about the purpose of the roll and the steps that operators would need to take was initiated by many departments within ICANN organization (particularly Communications, the Office of the CTO, and Global Stakeholder Engagement), following the communications plan. The operational preparations included the creation of the new KSK in October 2016 at the regular key ceremony; this ceremony was the most-watched ceremony to date.

The remaining steps in the plans have been taken throughout 2017. The various communities have been actively engaged, and there have been no significant missteps noted in any of the plans. Public perception of the roll has been nearly universally positive.

Assessment of Risks

There are two types of risk associated with rolling the root zone KSK: those associated with the operational process of rolling, and those associated with not doing the roll.

---

[6] *See* https://www.icann.org/en/system/files/files/ksk-rollover-external-test-plan-22jul16-en.pdf
[7] *See* https://www.icann.org/en/system/files/files/ksk-rollover-monitoring-plan-15sep16-en.pdf
[8] *See* https://www.icann.org/en/system/files/files/ksk-rollover-systems-test-plan-22jul16-en.pdf

Both sets of risks have been documented widely in SAC063 from SSAC, in the Design Team report, and in the plans from ICANN organization. This section gives a high-level overview of the risks.

The major risks associated with performing the roll are that it exposes behavior in validating resolvers that significantly affects the stability, security, or resilience of the DNS and cannot be mitigated during the process. The various plans deal with both detecting such behavior as early as possible and mitigating it when it appears. For example, it is likely that, despite all the publicity from ICANN and resolver software vendors, some validating resolvers will start to fail to resolve when the KSK is rolled; this might be mitigated at the time by the affected operators updating their copy of the KSK.

The major risks associated with delaying the key roll is that the longer one waits to make an operational change, the less likely it is that the operator will remember how to make that change. This desire to not lose institutional memory about how the KSK process works was repeatedly stated by the technical community as the primary justification for performing the key roll. (It should be noted that the need to roll the key to prevent it from being broken by cryptographic analysis is minute, and would not be applicable for at least another decade.)

NEXT STEPS

Staff recommends the Board direct the ICANN organization to complete the steps in rolling the root zone KSK.

Signature Block:

Submitted by: David Conrad

Position: CTO

Date Noted: 12 September 2017

Email: david.conrad@icann.org

ICANN BOARD INFO PAPER NO. 2017.09.23.1h

TITLE: **KSK Roll Current Status and Possible Next Steps**

PROPOSED ACTION: **For Board Consideration and Approval**

PROPOSED RESOLUTION:

Whereas, the Root Zone KSK (key signing key) Operator DPS (DNSSEC Practice Statement) from 2010 contains this statement "Each RZ KSK will be scheduled to be rolled over through a key ceremony as required, or after 5 years of operation."

Whereas, the technical community published in March 2016 an proposed plan to roll the DNS root KSK through a multi-step process that would last over a year.

Whereas, ICANN organization published in July 2016 an operational implementation plan for ICANN to roll the DNS root KSK through a process where each step can be observed by the community to be sure that the process was not creating unexpected problems.

Whereas, ICANN organization published in July 2016 an external test plan to allow DNS resolver operators to test their readiness for the anticipated KSK roll.

Whereas, ICANN organization published in July 2016 an back out plan detailing how major steps in the plan to roll the KSK could be reversed in case significant security, stability, or resiliency issues in the DNS were discovered.

Whereas, ICANN organization published in September 2016 a plan for monitoring the steps in the anticipated KSK roll in order to detect any anomalies that would affect the security, stability, or resiliency of the DNS.

Whereas, for over a year, ICANN organization has been educating the community about the intended plan to roll the DNS root KSK through talks at operators meetings, interviews in the

press, and general social media.

Whereas, most of the preliminary steps of the plan have already been acted upon, and none of them have caused any noticeable effects in the security, stability, or resiliency of the DNS.

Resolved (2017.09.23.xx), the ICANN organization is directed to roll the DNS root KSK as soon as is practical.

PROPOSED RATIONALE:

Why is the Board addressing this issue now?

The next step in the KSK roll is anticipated to happen on September 22, 2017 when the root zone grows to its largest size due to normal addition of a second ZSK (zone signing key). If there is no problem with the step that adds the ZSK, the next step is anticipated to happen on October 11, 2017, when the root zone will be signed with the new KSK; this is the full KSK roll. Assuming that these steps work well and no back out is required, there are a few more minor clean-up steps planned for future months.

What is the proposal being considered?

To instruct ICANN organization to continue with the plan expressed in "2017 KSK Rollover Operational Implementation Plan" (https://www.icann.org/en/system/files/files/ksk-rollover-operational-implementation-plan-22jul16-en.pdf) and "2017 KSK Rollover Monitoring Plan" (https://www.icann.org/en/system/files/files/ksk-rollover-monitoring-plan-15sep16-en.pdf), as modified by "2017 KSK Rollover Back Out Plan" (https://www.icann.org/en/system/files/files/ksk-rollover-back-out-plan-22jul16-en.pdf) if needed.

What stakeholders or others were consulted?

Numerous technical stakeholders have been consulted for over a year. There have been detailed presentations at network operators' meetings throughout the world, at technical meetings such as IETF and DNS-OARC, and at ICANN meetings.

The design team for the proposed plan included members of the technical community from around the world, who took detailed review comments during their creation of the plan.

What significant materials did the Board review?

The Board can review the documents linked from the page at https://www.icann.org/kskroll. That page has been widely referenced in the presentations mentioned above.

Are there positive or negative community impacts?

The main positive community impact is proof that ICANN can successfully act on our commitments to maintain the security, stability, and resiliency of the DNS root KSK. An additional positive impact is that the technical community has shown a greater interest in the technical implementation details of ICANN's key signing ceremonies.

To date, there have been no significant negative community impacts. During the future steps in the KSK roll, there may possibly be noticeable security, stability, or resiliency issues discovered with the roll process. If those issues are significant enough for ICANN to need to back out of the roll, the act of rolling back could cause different stability issues while lessening the issues from the roll. These are discussed in great detail in "2017 KSK Rollover Back Out Plan" (https://www.icann.org/en/system/files/files/ksk-rollover-back-out-plan-22jul16-en.pdf), which has been widely reviewed in the technical community.

Are there fiscal impacts or ramifications on ICANN (strategic plan, operating plan, budget); the community; and/or the public?

The next steps in the key roll are already accounted for in the operating plan and budget. It is not

anticipated that the roll will cost the community or the public any money.

Are there any security, stability or resiliency issues relating to the DNS?

There are possible security, stability, or resiliency issues with rolling the root KSK if the roll exposes operational issues, but there are also significant security and resiliency issues of not rolling the root KSK. The balance between these two were considered by the technical community during the planning stages of the roll and there was strong consensus that performing the roll was warranted.

Signature Block:

Submitted by: David Conrad

Position: CTO

Date Noted: 12 September 2017

Email: david.conrad@icann.org