SAC108
SSAC Comments on the IANA Proposal for Future Root Zone KSK Rollovers

An Advisory from the ICANN Security and Stability Advisory Committee (SSAC)
29 January 2020

Preface

This is an advisory to the ICANN Board, the ICANN Organization staff, the ICANN community, and, more broadly, the Internet community from the ICANN Security and Stability Advisory Committee (SSAC) about the Internet Assigned Number Authority's (IANA) proposal for future root zone Key Signing Key (KSK) KSK rollovers.

The SSAC focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), administrative matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to other parties, and the advice offered here should be evaluated on its merits.

Table of Contents

Executive Summary

This publication represents the full SSAC input to the Proposal for Future Root Zone KSK Rollovers ICANN Public Comment Proceeding.[1]

The SSAC reviewed the proposal in order to assure itself, and others, that the proposal will not introduce any stability or reliability issues to the root zone, the Root Server System (RSS), or the larger DNS ecosystem. Overall, the SSAC finds no issue with the proposal that should prevent the IANA from moving forward, and would like to thank the IANA for developing a strong proposal. The SSAC does find some aspects of the proposal could use more detailed explanations and further consideration, and expects IANA to produce a more detailed final plan for public consultation prior to rolling the KSK again. This comment also includes future considerations that IANA should take into account for subsequent rollovers.

[1] See https://www.icann.org/public-comments/proposal-future-rz-ksk-rollovers-2019-11-01-en

1 Background

The DNS root zone was first signed with DNSSEC in 2010. On October 11, 2018 the DNSSEC Key Signing Key (KSK) was first rolled in the root zone. Having now completed that first roll, the Internet Assigned Numbers Authority (IANA) has asked the ICANN Community to respond to its plan for subsequent KSK rollovers. The SSAC would like to thank ICANN, and specifically IANA, for engaging with the technical community on planning related to KSK rollovers, and for incorporating past advice from the technical community into its current work.

This comment represents the SSAC's full input to IANA on its *Proposal for Future Root Zone KSK Rollovers*, which will henceforth be referred to in this document as the Proposal.

The SSAC has previously commented on root zone KSK rollovers in SAC063, SAC073 and SAC102. This comment specifically addresses concerns relating to future KSK rolls, and focuses on items in the Proposal where the SSAC has concerns. In general, the SSAC is confident that the Proposal as written is an adequate and viable high-level plan and does not believe that further delay in planning for subsequent KSK rollovers is merited.

2 Analysis

2.1 Lack of Detail

While this proposal is intentionally and properly presented as a high-level overview and not a detailed implementation plan, the SSAC feels that the Proposal is missing some important details that should be clarified in the final plan. The SSAC expects that the final plan will address these concerns and contain more detail on these topics and others where necessary, contain numbered pages and labeled figures, and will be published for further input and review.

For example, it is not clear if there should be a gap between when the key rotation takes place and when the revocation bit is set. The Proposal states that in phase E the new KSK is active, but the previous KSK has not yet had its revocation bit set.

In addition, further clarification and more details would help to understand the figure on page 5.

- It is not clear from the table that in phase E the previous KSK is still valid and signed by the new KSK. The table on page 4 has useful information, but it seems to be missing some important data.
- It would be useful to identify the minimum and maximum times for each phase. There are a lot of timing constraints that are implied, and sometimes stated, but not called out explicitly.
- The Proposal should be more explicit in showing for how long both the old key and the new key sign the Zone Signing Key (ZSK) (i.e., cross signing).

Much of the rest of section two highlights aspects of the Proposal where the SSAC would like to see more detailed discussion and clarification in the final plan.

2.2 Key Deletion and Destruction

The Proposal does not include clear details on how keys will be destroyed after being removed from the root zone. The table in section 2.1 states that phases G and H are where the old key will be deleted from the first and second Key Management Facilities (KMFs). It does not specify how the key will be destroyed, or to what specification key destruction must adhere to.

The Proposal does not state when the previous KSK will be deleted from the root zone. Phase F states that the previous key remains in the root zone with its revoked bit set. Then Phases G and H state that the previous KSK is deleted from both KMFs, but nowhere is it stated when the key is deleted from the root zone.

2.3 Phases and Rollover Cycling

There is a gap of 10 months and 11 days during the transition between phases D and E where there is only one valid key that can be activated. This results in the inability to roll forward during a compromise event.

The 2019 KSK roll used a 3 month period where the old key (KSK-2010) was retained in the root zone, but as it signed nothing its presence was meaningless to validating resolvers. The Proposal does not explicitly state how phase E handles the old (now-superceded) KSK. If the Proposal intends to retain the superceded (but as yet unrevoked) KSK in the DNSKEY RR of the root zone in phase E it should say so explicitly.

2.4 Outreach

The communication plan appears to send a note to the root-dnssec-announce email list. While RFC5011-capable resolvers will also be able to pick up the new key, more detailed communication plans should be included in the Proposal, at least for the first few rounds of this process.

The SSAC has brought up the importance of outreach in the past.[2] The SSAC still believes that it is necessary to publicize the root zone KSK rollover activities as widely as possible. We also understand ICANN did significant outreach including but not limited to writing letters to all regulators in the world. It would be good if the outreach activities matched some evaluation of the effect of the activities that took place in the 2019 KSK roll.

The SSAC has previously provided advice on the need for planning for extraordinary circumstances, such as key compromise or roll back scenarios.[3] The SSAC still believes that it is necessary for IANA to both develop such procedures and communicate them widely to the community.

[2] See SAC063, recommendation 1

[3] See SAC063, recommendation 4

2.5 Contingency Planning

The Proposal should include greater discussion on the handling of a compromise event at each phase in the process. In addition to key compromises, it is important to see a fast, reasonable, and believable safe rotation timeline worked out in case an expedited rotation is needed.

2.6 Reverting to a Previous Phase

Section 2 of the Proposal states:

> *If a phase is extended, or if there is a situation which requires the process to be reverted to the previous phase, all actions associated with the next phase are postponed by at least one calendar quarter or until the RZM Partners decide to transition to the next phase.*

The Proposal should note exactly which phase transitions are irreversible and which could possibly be reverted.

2.7 Standby KSK

Section 2.5 of the Proposal states:

> *Earlier trust in the generated key allows it to be more successfully used for an emergency KSK rollover. If the active KSK is compromised and the standby key remains secure, signing can be quickly switched to the new KSK and everyone who already trusts this standby key should be able to immediately validate with the new signatures. If a standby key is not yet trusted, an emergency KSK rollover has a greater potential for negative impact.*

The Proposal should be clearer as to the periods when the incoming key can be considered as a "standby key" in the sense of the role described here.

2.8 Measurement

The SSAC supports section 3.1 of RSSAC046, which states.

> *The plan lacks discussion on measuring the stability implications of future KSK rollovers. It is not clear how decisions regarding whether to go forward with a phase transition, or not go forward with a phase transition, will be made absent of any measurement data. To be more consistent, predictable and deliberate in future KSK rollovers, IANA should promote the development of a root telemetry mechanism.*

The SSAC has previously provided similar advice on the need for a measurement system to detect "breakage" in KSK rollovers, and collect appropriate data for measuring future rollover successes or failures.[4]

[4] See SAC063, recommendations 3 and 5

2.9 Risk Management

The Proposal considers contingency planning and outreach, but does not address risk management. The outreach and contingency planning phases should include a risk management profile and an action framework, both oriented towards non-technical audiences (e.g., regulators, policy makers), to mitigate technical and non-technical risks.

3 Future Considerations

This section contains topics the SSAC believes are relevant to future KSK rolls, but are not directly related to the Proposal.

3.1 Documentation

The SSAC would like to see much of the documentation that has been published over the years about DNSSEC and KSK rollovers, much of which is internal to ICANN or only casually prepared, published in an open venue such as the IETF. The working set of documentation on DNSSEC and KSK rollovers should be maintained as circumstances and plans change.

The SSAC expects IANA to produce a more detailed final plan for future Root Zone KSK Rollovers for public consultation prior to rolling the KSK again. This could be a new plan or an update to existing, but outdated, publications. For example, the Root Zone KSK Rollover Plan,[5] and/or the DNSSEC Practice Statement.[6] The detailed final plan should reflect updated considerations and frameworks from the previous KSK roll and the Proposal.

3.2 Algorithm Changes

The Proposal does not cover changes to the algorithm used to generate the KSK. The SSAC believes that changes to the algorithm in use are best handled separately, and not with this proposal. The SSAC expects IANA to revisit algorithm rolls once the regularity of KSK rolls has been established, and after IANA has taken into account the community feedback on the subject.

3.3 Response Sizes

It is unknown what would happen if there were three KSKs in the root zone at once. It would be good to know the impact of this in case it should become necessary in a contingency. Due to constraints on the size of UDP packets it may not be possible with even moderately sized RSA keys of 2048 bits. Research should be undertaken to determine the impact of large responses on both IPv4 and IPv6 DNS resolvers. Earlier research is documented in Appendix A of SAC063.

[5] See https://www.iana.org/reports/2016/root-ksk-rollover-design-20160307.pdf

[6] See https://www.iana.org/dnssec/icann-dps.txt

4 Acknowledgments, Statements of Interests, and Dissents and Withdrawals

In the interest of transparency, these sections provide the reader with information about four aspects of the SSAC process. The Acknowledgments section lists the SSAC members, outside experts, and ICANN staff who contributed directly to this particular document. The Statements of Interest section points to the biographies of all SSAC members, which disclose any interests that might represent a conflict—-real, apparent, or potential—-with a member's participation in the preparation of this Report. The Dissents section provides a place for individual members to describe any disagreement that they may have with the content of this document or the process for preparing it. The Withdrawals section identifies individual members who have recused themselves from discussion of the topic with which this Report is concerned. Except for members listed in the Dissents and Withdrawals section, this document has the consensus approval of all of the members of SSAC.

4.1 Acknowledgments

The committee wishes to thank the following SSAC members for their time, contributions, and review in producing this report.

SSAC members
Joe Abley
Jaap Akkerhuis
Tim April
KC Claffy
Patrik Fältström
James Galvin
Geoff Huston
Andrei Kolesnikov
Warren Kumari
Jacques Latour
Barry Leiba
Danny McPherson
Ram Mohan
Russ Mundy
Rod Rasmussen

ICANN staff
Andrew McConachie (editor)
Danielle Rutherford
Kathy Schnitt
Steve Sheng

4.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at:
https://www.icann.org/resources/pages/ssac-biographies-2019-01-08-en

4.3 Dissents and Withdrawals

There were no dissents or withdrawals.