SAC102
SSAC Comment on the Updated Plan for Continuing the Root KSK Rollover

A Comment from the ICANN Security and Stability Advisory Committee (SSAC)
20 August 2018

Preface

This is a comment 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 ICANN organization's Updated Plan for Continuing the Root KSK Rollover.

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.

1 SSAC Comment on the Updated Plan for Continuing the Root KSK Rollover

On 13 May 2018, the ICANN Board requested the SSAC to provide advice to the Board on the "Updated Plan for Continuing the Root KSK Rollover".[1,2] This comment represents the SSAC's response to that request.

After reviewing pertinent information in the time available, the SSAC has not identified any reason within the SSAC's scope[3] why the rollover should not proceed as currently planned. Additionally, the SSAC suggests that ICANN establish a framework for scheduling further rolls of the root KSK based on analysis of the outcomes of this initial roll of the KSK.

The SSAC is aware that the suspension of the plan in 2017[4] was caused by the consideration of new data that was not clearly understood, and which exposed a previously-unquantified risk. The SSAC is also aware that this data has been further analysed and notes that there is confidence[5] that this data does not alter the original assessment of overall risk with the KSK rollover. The plan to continue the KSK rollover differs from the earlier plan principally in the timeline. SSAC's comments and recommendations on various aspects of the root KSK rollover in prior SSAC advisories[6,7] remain unchanged and have been addressed in the ICANN plans.[8,9]

The assessment of risk in this particular area has some uncertainty and therefore includes a component of subjective judgement. Individuals (including some members of the SSAC) have different assessments of the overall balance of risk of the resumption of this plan. The decision as to what level of risk is acceptable remains one for the ICANN Board to assess.

---

[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] See "ICANN Bylaws, Section 12.2(b)i", https://www.icann.org/resources/pages/governance/bylaws-en/#article12

[4] See "KSK Rollover Postponed", https://www.icann.org/news/announcement-2017-09-27-en

[5] See, for example, "Minimal User Impact Expected from Root Zone Key Signing Key (KSK) Rollover", https://www.icann.org/news/blog/minimal-user-impact-expected-from-root-zone-key-signing-key-ksk-rollover

[6] See SAC063: SSAC Advisory on DNSSEC Key Rollover in the Root Zone

[7] See SAC073: SSAC Comments on Root Zone Key Signing Key Rollover Plan

[8] See "2017 KSK Rollover Operational Implementation Plan", https://www.icann.org/en/system/files/files/ksk-rollover-operational-implementation-plan-22jul16-en.pdf

[9] See "2018 KSK Roll Operational Implementation Plan", https://www.icann.org/en/system/files/files/2018-ksk-roll-operational-implementation-plan.pdf

2 Acknowledgments, Disclosures of Interests, 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 Disclosures 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 Comment. 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 Comment is concerned. Except for members listed in the Dissents and Withdrawals sections, this document has the consensus approval of all of the members of SSAC.

2.1 Acknowledgments

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

SSAC members
Benedict Addis
Jaap Akkerhuis
Lyman Chapin
kc claffy
Jay Daley
Patrik Fältström
Paul Ebersman
James Galvin
Robert Guerra
Geoff Huston
Merike Kaeo
Andrei Kolesnikov
Warren Kumari
Jacques Latour
Barry Leiba
John Levine
Carlos Martinez
Danny McPherson
Ram Mohan
Russ Mundy
Rod Rasmussen
Suzanne Woolf

ICANN staff
Roy Arends
David Conrad

Andrew McConachie (editor)
Kathy Schnitt
Steve Sheng

2.2 Disclosures of Interest

SSAC member biographical information and Disclosures of Interest are available at: https://www.icann.org/resources/pages/ssac-biographies-2018-03-02-en

2.3 Dissents

Lyman Chapin, kc claffy, Jay Daley, Warren Kumari and Danny McPherson have provided the following dissent:

The decision to proceed with the keyroll is a complex tradeoff of technical and non-technical risks. While there is risk in proceeding with the currently planned roll, we understand that there is also risk in further delay, including loss of confidence in DNSSEC operational planning, potential for more at-risk users as more DNSSEC validation is deployed, etc.

While evaluating these risks, the consensus within the SSAC is that proceeding is preferable to delay. We personally evaluate the tradeoffs differently, and we believe that the risks of rolling in accordance with the current schedule are larger than the risks of postponing and focusing heavily on additional research and outreach, and in particular leveraging newly developed techniques that provide better signal and fidelity into potentially impacted parties.

We would like to reiterate that we understand our colleagues' position, but evaluate the risks and associated mitigation prospects differently. We believe that the ultimate decision lies with the ICANN Board, and do not envy them with this decision.

Finally, we would also like to expressly acknowledge the ICANN staff for all of their research, outreach, and discussion on this matter thus far.

2.4 Withdrawals

Joe Abley