Staff Report of Public Comment Proceeding

Plan to Restart the Root Key Signing Key (KSK) Rollover Process	
Publication Date:	23 Apr 2018
Prepared By:	Paul Hoffman, Office of the CTO

Public Comment Proceeding	
Open Date:	1 Feb 2018
Close Date:	2 Apr 2018
Staff Report Due Date:	23 Apr 2018

Important Information Links
Announcement
Public Comment Proceeding
View Comments Submitted

Staff Contact:	Paul Hoffman	**Email:**	paul.hoffman@icann.org

Section I: General Overview and Next Steps

The plan received 20 comments from organizations and individuals. The large majority of the comments indicated that the ICANN organization should proceed with the plan; some of these comments came with suggestions on additional steps ICANN org should add to the plan. A few of the comments suggested that the plan not proceed.

Based on the comments, ICANN org will propose to the ICANN Board that the rollover plan described in the call to the community be expanded to include more outreach and more publication of data that is available to ICANN org. This revised plan will be available by 1 May 2018, and a formal request to the ICANN Board will be made at that time.

Section II: Contributors

At the time this report was prepared, a total of twenty (20) community submissions had been posted to the forum. The contributors, both individuals and organizations/groups, are listed below in chronological order by posting date with initials noted. To the extent that quotations are used in the foregoing narrative (Section III), such citations will reference the contributor's initials.

Organizations and Groups:

Name	Submitted by	Initials
Afilias	Joe Abley	A
Verisign	Burt Kaliski	V
Snake Hill Labs	Bill Snow	SHL
gTLD Registries Stakeholder Group	Paul Diaz	RSG
Internet Society	Olaf Kolkman and Dan York	ISOC
At-Large Advisory Committee	ICANN At-Large Staff	ALAC
ICANN Business Constituency	Steve DelBianco	BC
Non-Commercial Stakeholder Group	Rafik Dammak	NCSG

Individuals:

Name	Affiliation (if provided)	Initials
Ólafur Guðmundsson		ÓG

Stephane Bortzmeyer		SB
Frederico A C Neves		FACN
Barry Leiba		BL
Geoff Huston	APNIC	GH
Jacques Latour	Canadian Internet Registration Authority (CIRA)	JL
Tony Finch		TF
Russ Mundy		RM
Jim Reid		JR
Evan Hunt	Internet Systems Consortium	EH
Jay Sudowski	Handy Networks	JS
Phil Regnauld	Network Startup Resource Center	PR

Section III: Summary of Comments

General Disclaimer: This section intends to summarize broadly and comprehensively the comments submitted to this public comment proceeding but does not address every specific position stated by each contributor. The preparer recommends that readers interested in specific aspects of any of the summarized comments, or the full context of others, refer directly to the specific contributions at the link referenced above (View Comments Submitted).

Comments that encouraged going forward with the plan as-is (9):
ÓG
SB
BL
GH
RM
JR
EH
PR
NCSG

Comments that encouraged going forward with the plan, with additional suggestions (7):
FACN: Wants a more detailed outreach plan from ICANN that provides documentation/presentation material that could be used by the local operators community, and to engage with more ICANN communities, ccNSO members in particular.

JL: ICANN should work with all the major search engine to make the DNSSEC/DNS failure-related searches (for terms like SERVFAIL, DNSSEC, DNS resolution failure, and so on) more obvious during the rollover. This should also be mobile-friendly.

A: ICANN should facilitate planning and community consultation on measurement of and improvements to the many technical mechanisms involved in KSK rollover and establishes a regular cadence for future scheduled root KSK rollovers.

TF: Included ideas for root key rollovers after this one.

SHL: Included ideas for root key rollovers after this one.

RSG: ICANN should undertake greater publicity and awareness-building campaigns. ICANN should make more data about preparedness available. ICANN should develop key metrics and

measures of success.

ISOC: ICANN and associated partners should continue further study of the RFC 8145 data to better understand the risks. ICANN should continue to expand communication and outreach activities to help the community of network operators be prepared to address any issues on 11 October 2018.

Comments that did not give an opinion on going forward, with additional suggestions (1):

JS: Included ideas about giving the community more information on how ICANN researched the operators of the IP addresses from the RFC 8145 data. Also suggested additional outreach methods.

Comments that proposed not going forward with the plan, but instead use a different plan (3):

V: ICANN should reframe root KSK publication as a standalone activity with its own success criteria, rather than as just a step in the rollover plan. Before proceeding with the root KSK rollover, ICANN should publish measurable goals for the KSK rollout, including monthly or more frequent metrics for how many operators have been notified of the new KSK (and what level of notification is "good enough"), how many have acknowledged awareness of the new KSK, how many have installed the new KSK, how much root server traffic these operators represent, how many Internet users they serve, and how many Internet properties risk becoming unreachable if KSK rollover were to occur the time the metrics are reported. The rollover should not start until the rollout consistently meets these documented goals.

ALAC: ICANN should perform a risk assessment of alternatives to the current plan. The assessment should include current information related to the RFC 8145 trust anchor reports, the prognosis for availability of the in-development IETF "sentinel" mechanism and the potential for using the sentinel mechanism to create a greater level of comfort prior to the KSK rollover. ICANN should provide a simple test web address and/or application that will allow users to verify if the resolver they typically use is DNSSEC-aware. The comment also expresses concern that 11 October 2018 is a Thursday/Friday and thus could prolong problems.

BC: ICANN should do further research into the state of resolvers and how many users would lose access to the DNS as a result of the rollover being done. ICANN should delay further until better information is available, such as until after the kskroll-sentinel protocol is deployed. The timing of the rollover should be a data-driven decision to the greatest extent possible. ICANN should provide a comprehensive updated plan to the community to ensure transparency and consistency of expectations, as well as to allow for robust community comment. Although the report cites data from research carried out by the Office of the CTO, this data is not available for community review.

Section IV: Analysis of Comments

General Disclaimer: This section intends to provide an analysis and evaluation of the comments submitted along with explanations regarding the basis for any recommendations provided within the analysis.

It is clear that the large majority of comments from individuals and organizations support the plan as specified or support the plan with some additions. The following addresses the three comments that proposed not going forward with the plan, but instead use a different plan.

V: The operational plan accepted by the community already has the KSK publication as a standalone activity with its own success criteria; what is being proposed is proof of sufficient resolvers having seen the publication. In order to measure "how much root server traffic these operators represent, how many Internet users they serve, and how many Internet properties risk becoming unreachable if KSK rollover were to occur the time the metrics are reported", ICANN would need to have a registry of all the validating resolvers, their operators, and the number of

users that the resolvers they serve. This represents a massive change to the way that the DNS has operated since its inception, going from permissionless use of DNS services to instead needing to be identified so that ICANN can meet publication response metrics. Such a change to how DNS resolution service has always been provided seems both controversial as well as unimplementable in any foreseeable timeframe. The implication of this requirement would thus suggest the KSK rollover never be performed, something the community has already decided against.

ALAC: Although risk assessments are often useful when there is sufficient data on which to perform the assessment, a risk assessment on the KSK rollover with the very limited information that is possible to get from resolvers on the Internet would be based on what most people agree would be, at best, guessing. In specific, the RFC 8145 data changes radically when one looks at how many users historically have been associated with particular resolver addresses, and it is unlikely the forthcoming kskroll-sentinel protocol will be sufficiently widely enough deployed in any foreseeable timeframe to yield data to make a solid decision based on percentage of users who will be affected by the rollover. Further, no one in the technical community has suggested any other source of data that can be used in the current DNS. In the forthcoming outreach for the rollover, ICANN will include pointers to public sites allowing checking of DNSSEC validation by users' resolvers. The reason that rollover needs to happen on a specific day (the 11th of the month in January, April, July, or October) will also be described better in the updated test plan materials.

BC: Recent data analysis by APNIC indicates that the number of users who would be negatively affected by the rollover would be under 0.1%; this analysis was not available at the time the plan was put together for the community. After more discussion in the IETF, it is now deemed unlikely that the kskroll-sentinel protocol will be widely enough deployed in any foreseeable timeframe to yield sufficient data to make a solid decision based on percentage of users who will be affected by the rollover. Thus, ICANN org will be unable to ever make the decision as data-driven as everyone would desire. ICANN will certainly update the operational plans that were being used before the postponement to both include the new dates as well as give results from the steps already taken. The data we used to create the plan, as well as new analysis and other data that other respondents have asked for, will soon be made available for public review.

Given this preponderance of support, ICANN org will create a revised and expanded set of plans that includes many of the suggestions for how to reduce the risk of a key rollover on 11 October 2018.