Report of Public Comments

Title:	Design Team Review of Plan for DNS Root Zone KSK Change
Publication Date:	19 October 2015
Prepared By:	Edward Lewis

Comment Period:	
Comment Open Date:	6 Aug 2015
Comment Close Date:	Extended to 5 Oct 2015

Important Information Links
Announcement
Public Comment Box
View Comments Submitted

Staff Contact:	Edward Lewis	**Email:**	edward.lewis@icann.org

Section I: General Overview and Next Steps

The comments will be presented to the Design Team to address while preparing their final report.

Section II: Contributors

At the time this report was prepared, a total of 14 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
APNIC Labs	George Michaelson	AL
Business Constituency	Steve DelBianco	BC
IIS (formerly .SE)	Anne-Marie Eklund Löwinder	SE
Security and Stability Advisory Committee	Julie Hedlund	SS
Beijing Internet Institute	Shane Kerr	BI

Individuals:

Name	Affiliation (if provided)	Initials
Stephane Bortzmeyer		SB
James Gannon		JG
Maciej Andziński	NASK, .pl registry	MA
Daisuke HIGASHI		DH
Warren Kumari		WK
Joao Luis Silva Damas		JD
Dan York	ISOC	DY
Tim April		TA
Yoshitaka Aharen		YA

Section III: Summary of Comments

General Disclaimer: This section is intended to broadly and comprehensively summarize the comments

submitted to this Forum, but not to address every specific position stated by each contributor. Staff 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).

COMMUNICATIONS PLAN

[SB] The "communication plan" seems a bit light.

[MA] Do you plan any far-reaching information campaign among ISPs? For example in cooperation with RIRs?

[WK] The described communication plan is neither broad enough nor long enough.

[BC] The BC recommends a communications program in advance of this change to inform ISP communities around the world

[DY] largest concern is with the need for a more solid communication plan

[DY] ensure that the "real-time communications channels" are also available in some form OUTSIDE of just the RSSAC and RZM Partners

[SE] It [ref #9] is also very important to work closely together with strong and experienced local internet communities such as NOGs, ccTLDs and RIRs.

MEASUREMENTS

[AL] Measurements and Reporting: ... a weak reference to any measurements that may be conducted during these critical phases. This is insufficient in our view

[WK] 13% of the population may be adversely affected, but does not discuss how to refine this number

[BC] lack of any measurements during implementation – no metrics, no documented post-mortem. Developing metrics, using NIST SP 800-55 or some other implementation performance framework, will serve the current team, future teams, and the community

[SE] Good suggestion [#12]. To measure is to know.

[YA] It is very helpful if some indicators are provided to measure influence to the resolvers

JUSTIFICATION AND TIMING OF KEY ROLL

[AL] Timing of the KSK roll:... “Why roll now?"

[JD] very little in the draft report reasoning for the need to perform a root KSK rollover

[AL] Scheduling and Operational Tasks:... rigid adherence to a calendar irrespective of operational support considerations appears to be an inappropriate prioritisation

[WK] there is still no clear schedule for the keyroll. ICANN should acknowledge the fact that they are slipping behind the implicit schedule

[DY] lack of a concrete timeframe

[TA] it should happen sooner rather than later

[YA] adequately advance announcement is more important than selecting weekdays

CONCERNS RELATED TO ADHERENCE TO RFC 5011

[SB] About RFC 5011, ... risk of bad configuration

[AL] KSK-signed sentinels: ... envisaged that the roll process could use the incoming KSK to sign some sentinel record in the root zone

[AL] RFC5011 Capability Signalling:...no active signalling of RFC5011 capability currently exists, it is possible that we could delay a planned KSK roll long enough to deploy DNS code changes

[SE] This recommendation [#2] is very important. Software, both separate and integrated in operating systems has not been tested with RFC 5011 for the root level, and the mechanism hasn't been tested on the public internet at all.

ORIGIN OF DOCUMENT

[SB] On the governance side, the document only comes from US organizations (ICANN, Verisign, NTIA)

[BC] all contributors appear to be from Verisign, NIST, NTIA, and ICANN

FALLBACK PLANS

[AL] Key Overlap:... Why is there not a period of overlap

[TA] suggest that some consideration be paid to the requirements and process that ICANN and the root operators should follow in the event that an unacceptable number of end users are DoSed

[YA] very helpful if actions for resolver administrators regarding rollback were described.

ASSESSMENT OF PRIOR WORK, OTHER TEST BEDS

[WK] It is unclear from this document how much of the prior work was incorporated

[SS] there is not a comprehensive correlation of the recommendations in SAC63 with material presented in the ICANN KSK Rollover Plan...the SSAC would like to see the final report respond

directly to each of the recommendations in SAC 063,

[SB] Among the testbeds, Yeti <https://yeti-dns.org/> is not mentioned.

[BI] propose research or survey the community for novel approaches

[BI] test the KSK roll approach in a testbed that looks similar to the production environment. This includes both lab tests, and larger testbeds such as Yeti.

CRYPTOGRAPHIC CONCERNS

[AL] Algorithm Agility:... doesn't clearly explain why larger RSA-based DNS response payloads would be preferable to smaller ECDSA DNS response payloads.

[DH] Root KSK/ZSK algorithm should be changed to one with shorter key size such as ECDSAP256SHA256 for _now_ to keep DNSKEY reply size less than IPv6 minimum MTU (payload size 1232 bytes) in the future.

[BC] planning toward moving to RSA/DSA 2048 (or stronger) encryption for both the key-signing key (KSK) and zone-signing key (ZSK)

[DY] encourage the Design Team and RZM Partners to continue to monitor the deployment of DNSSEC-validating resolvers supporting ECDSA

RELATION TO TRANSITION

[JG] not accounted for the potential role of the Post Transition IANA (PTI) entity that is envisioned by the CWG-Stewardship

[JG] Risk: Concerns over the stability of the root zone KSK system in the event that the IANA functions are no longer performed by ICANN or its PTI subsidiary and instead are performed by an independent IANA Functions Operator as a result of the outcome of a separation process in the future.

[JG] set out a clear differentiation between the responsibilities of ICANN and the responsibility of the IFO

[JG] SSR Department staff and a new IFO?

[JG] SSAC/RSSACs relationship with a new IFO?

[JG] Recommendation 9 of the design team be modified to read "...ICANN in cooperation with the RZM partners and the IANA Functions Operator, should..."

TRUST ANCHOR CONVEYANCE

[SE] This recommendation [#3] is very important. To be aware of the process on how IANA publish the root key and how you can achieve trust in that publication and distribution is a desirable state.

Channels for distribution of the root key must be established in an open and transparent manner.

[SE] The recommendation [#4] is extremely important since ICANN haven't been working with this area at all during the five years that the trust anchor has been published.

OTHER COMMENTS

[AL] Serialized Key Rolls:... What are the issues involved in staging multiple incoming keys?

[DH] Channel Partners: ... DNS software/appliance producers should be included ... F5 Networks

[WK] does not discuss anything to do with emergency key rolls

[JD] does not address the need to re-examine the processes involved in the generation of the incoming key nor the signing of the ZSKs

[JD] need to review all the steps, from a procedural and implementation point of view to ensure that, for instance, the outgoing KSK is not cleared from the HSMs too early, that the correct key is indeed used at each step where it needs to be used, with consistency, etc.

[DY] an ongoing routine of regular root zone KSK rollovers

[BI] process seems both novel and complicated.

Section IV: Analysis of Comments

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

All of the comments will be passed to the Design Team for consideration in developing the final report. In many cases, the comments point to discussions held but were insufficiently documented. In particular, comments that the document is a product of ICANN, NTIA (NIST) and Verisign indicates that the integral role of the international panel of experts from the community who performed the work presented in the document was overlooked. Although the panel was not chosen with globalization in mind, none of the experts from the community are from the US nor do they reside in the US.

The feedback will be useful in guiding where more documentation time should be spent as well as gauging, to some extent, the priority of concerns. Some of the comments address topics that are out of scope for the effort.