Staff Report of Public Comment Proceeding

Proposal for Future Root Zone KSK Rollovers	
Publication Date:	7 August 2020
Prepared By:	Kim Davies

Public Comment Proceeding	
Open Date:	1 November 2020
Close Date:	31 January 2020
Staff Report Due Date:	30 April 2020

Important Information Links
Announcement
Public Comment Proceeding
View Comments Submitted

Staff Contact:	Kim Davies	**Email:**	kim.davies@iana.org

Section I: General Overview and Next Steps

In a project spanning between 2015 and 2019, ICANN and PTI successfully conducted the first rollover of the Root Zone KSK, which involved a globally-coordinated change to the cryptographic trust anchor configured in DNSSEC-enabled devices. This consultation proposed a draft framework for future such rollovers, seeking to carry over what worked and build upon that experience.

During the original preparation of the staff report following this consultation period, normal operations were interrupted by the COVID-19 pandemic, and disaster recovery operations were performed to hold an exceptional key signing ceremony and delay non-essential work items. Preparation for future root zone KSK rollovers was suspended to focus on these immediate operational needs, and to monitor the impacts of the pandemic on future operational planning.

Current Status: Staff have reviewed and analyzed the comments, but do not have a concrete timeline to propose for the next KSK rollover at this time due to the uncertainty of current events. Normal operations have generated signatures until the end of March 2021, and it is not currently anticipated that further key signing ceremonies will be conducted until next year.

Next Steps: Staff will continue to monitor and adapt to the COVID-19 pandemic in its day-to-day operations. A timeline for the next scheduled KSK rollover will be reconsidered when there is greater confidence face-to-face operations and international travel to the US can safely resume, or alternative accommodations can be designed should the restrictions to conducting ceremonies prove to be long-term. It is unclear whether permanent impacts of the pandemic will demand reconsideration of the fundamental timeline for future rollovers. Some of the responses have suggested additional research that we will propose for funding during Fiscal Year 2022, for which budget development is now underway.

Section II: Contributors

At the time this report was prepared, a total of eleven 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
Japan Registry Services	Satsuki Hori and Yoshiro Yoneya	JPRS
ICANN Business Constituency	Steve DelBianco	BC
ICANN Non-Commercial Stakeholder Group	Rafik Dammak	NCSG
ICANN Root Server System Advisory Committee	Andrew McConachie	RSSAC
ICANN Security and Stability Advisory Committee	Andrew McConachie	SSAC

Individuals:

Name	Affiliation (if provided)	Initials
Nicolas Antoniello	—	Antoniello
John Dickinson	Sinodun Internet Technologies	Dickinson
Erwin Lansing	DK Hostmaster	Lansing
Michael Richardson	Sandelman Software Works	Richardson
Roland M. van Rijswijk-Deij	NLnet Labs	Rijswijk-Deij
Michael StJohns	NthPermutation Security	StJohns

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.

General Comments

- Support for the plan (Antoniello, BC, JPRS, Lansing, SSAC)
- Support for the transparency/engagement of the process (BC, Rijswijk-Deij)
- Proposal adversely affects software's ability to support DNSSEC verification (NCSG)

Timing

- Extend the period of overlapping keys such that there is always a standby key in the trust anchor set (JPRS, StJohns)
- Consider risk of loss of skills as key generation/revocation actions happen infrequently (StJohns)
- Do not consider it important to retain institutional knowledge to perform key rollovers, they should continue to be viewed as special events (Rijswijk-Deij)

- Support earlier generation and pre-publication of trust anchors (BC, Rijswijk-Deij, NCSG)
- Limit pre-publication of trust anchors to a closed audience (BC)
- Consider pre-publishing two keys in advance, although not via RFC 5011 due to packet size limitations (Rijswijk-Deij)
- Seek a predictable, periodic process (Lansing, RSSAC)
- Three year interval is appropriate (BC, Lansing)
- Periodic rollovers are not sufficiently justified, and risks operational stability as the ability for validators to keep up with regular changes is not proven (NCSG)
- Consider operational impacts if the "validFrom" and "validUntil" properties change due to unexpected events (Dickinson)
- Plan should include any time needed to revise KSK management software (NCSG)
- Plan should explain how measurement data will factor into decision making on transitioning to the next phase (RSSAC)

Algorithms and Key Quality

- Consider whether operational delays in withdrawing keys from service would exceed guidance on cryptographic lifetimes (StJohns)
- Consider whether to only publish the public key fingerprint rather than the public key in advance (Richardson)
- Commence work on preparing to change the root signing algorithm (Lansing, Rijswijk-Deij, RSSAC)
- Do not predicate general rollover planning on creating an algorithm rollover process (Lansing, RSSAC, SSAC)

Key Storage

- No reason to retain standby key on HSMs until they are actively used for signing (StJohns)
- Update the Storage Master Keys in the HSMs to delete a retired key (StJohns)
- Consider co-generating keys across multiple devices, rather than the current approach of generating the key on a single HSM and exporting it to the others in the fleet (StJohns)
- Focus on ensuring compromise never occurs, as there is no identifiable use case for a standby key, particularly as they are stored in the same facility as the active key. (Rijswijk-Deij)

Additional Predicates

- A complete operational procedure with all necessary preconditions and possible outcomes must be developed and verified prior to future rollovers (NCSG)
- Formal security analyses of harms and benefits should be a precondition for future rollovers (NCSG)
- Share risk management assessment for both technical and non-technical audiences (SSAC)
- Develop a root telemetry mechanism (RSSAC)
- Study the impact of three KSKs in the root zone at once due to packet size impacts (SSAC)

Outreach

- Guide different audiences (e.g. software developers, end users, ceremony participants) based on what they should expect in each phase (JPRS)
- Perform proactive outreach to software vendors to disseminate new trust anchors each time they change (Rijswijk-Deij)
- Seek explicit confirmation from key software vendors to ensure timeline accords with the lead times they require to disseminate trust anchors via their mechanisms (Richardson)

- Put a final plan, or amended procedural documentation, for a second round of public comment prior to a future rollover (SSAC)
- Evaluate the success of outreach efforts for the prior KSK roll, to inform future outreach approach (SSAC)
- Develop specific outreach approach for key compromise and roll-back events (SSAC)

Documentation Improvements

- Explicitly link "validFrom" and "validUntil" properties in the trust anchors to the phases in the document (Dickinson)
- Add "replication" as a phase in the overall lifecycle (BC)
- Improve clarity of timeline graphic (Dickinson, JPRS, Richardson, SSAC)
- Add reference to RFC 7958 for common definitions (Dickinson)
- Clarify documentation on when a key is equipped to act as a standby key (SSAC)
- Clarify documentation on when phases can be reverted or are irreversible, and anticipated response in the event of key compromise during that phase (SSAC)

Other

- Consider whether RFC 5011 Section 5 needs revision (StJohns)
- Consider alternating site of key generation between facilities (Antoniello)
- Consider impacts of replacement lifecycle of ceremony hardware on key rollover timing (Antoniello)
- Proper security analyses to motivate the proposed approach are not published (NCSG)

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.

Theme	Evaluation/Response
Rollovers negatively impact DNSSEC deployment generally	Our assessment is the best approach to ensuring software has the appropriate agility to handle key rollovers is to hold them regularly. The operational environment requires the latent capability for keys to be changed with minimal notice (i.e. in the event of a compromise), so we need to strive for broad operational readiness to update trust anchor configurations. More frequent rollovers that exercise these mechanisms should highlight potential problems with nonadaptive trust anchor configurations earlier and allow problems to be remedied quicker.
Adjust timings to provide constant coverage by a standby key	The proposed approach was designed to avoid three keys concurrently being published in the DNS, however, based on feedback on this consultation we'll study this issue further (see next row). If we can

	identify a timing that can accommodate this without unacceptable impacts associated with increased packet size, we see it as a useful goal to provide this coverage.
Impacts of number of keys and packet size	We agree that the consequences of the increased size of DNS packets should be carefully examined and will factor this into our pre-planning.
Maintaining HSM operator skills over long intervals	We do not consider this a significant risk. All phases of the key lifecycle are routinely tested during staff training and research activity, and all phases of key management are thoroughly pre-scripted. Each ceremony is rehearsed in advance with test equipment. Key management is also performed on comparable equipment for other ICANN business activities in parallel by the same operations team.
Retention of standby keys on HSMs	While it is true that standby keys do not need to be retained on the HSMs, there is presently not an in-scope location that can retain the exported keys to the same level of protection. Storing the standby keys offsite will require a more fundamental re-evaluation of the model and storing the keys on-site outside of the HSM does not appear to provide any benefit. Storing the standby keys in the HSM also simplifies their lifecycle management and aids redundancy.
Replacing the SMK after key destruction	All exported backups of the key are destroyed in the same ceremony during which the key is deleted, therefore there is no need to replace the SMK. Further, each HSM contains a single SMK which is required to export other KSKs on the device, and regeneration of the SMK would require recalling all 7 recovery key shareholders to a key ceremony to be re-issued credentials.
Measurement and telemetry requirements	We will seek RSSAC's expertise and guidance to identify appropriate instrumentation that can be useful in decision making as it pertains to key rollovers.
Risk management assessment	We agree more details on our risk assessments should be shared and will develop this further.
Software vendor engagement	We agree that additional pro-active engagement with key software vendors would increase confidence in the suitability of the plan. We also note that the IANA timezone database project has a similar dependency

	on propagation through software vendors and provides similar guidance on lead time to effectively disseminate changes through vendor channels.
Alternate key generation site	We will consider how to alternate the key generation site, as it will encourage greater diversity in the in-person participation of the events.
Co-generate keys rather than generate and replicate	We will explore the viability of these alternative key generation approaches.
Limit access to public keys prior to their active use	The keys are generated at public events and the details of the public key are immediately knowable through published artefacts of the ceremony. It would be difficult to keep this component secret while retaining the transparency of the ceremony. Further, limiting access would negate the benefit of using the longer window to enhance propagation.
Lack of specific details in the proposal	This consultation document was not intended to be a comprehensive procedure that covers all aspects of future rollover, rather it was intended to obtain general consensus on the high-level approach. The next phase would be to operationalize the concepts into the comprehensive and detailed procedural documentation that is already employed in administering the KSK. This documentation is maintained under the auspices of the Root KSK Policy Management Authority (PMA), and subject to third-party audit against the SOC 3 framework. Much of the requested detail is already present in these internal operational procedures, and we will evaluate making these procedures more public.
Future consultation on this proposal	We will take under consideration the proposal to put this plan for a second formal comment period. At a minimum, we expect to share drafts of pertinent procedures with TCRs, operational mailing lists and other interested parties, and provide the opportunity to revise and adapt procedures based on feedback as has already been the culture of KSK management. As noted elsewhere, we will also seek to make specific outreach to software vendors.
Algorithm rollovers	We recognize there is significant interest that algorithm rollovers be researched with a view to future operationalization in the root zone. To that end, we will be proposing allocations in the PTI and ICANN FY22

	budget cycles to commence this work. These draft budgets will be put for community review later in 2020.
General editorial comments and suggestions	Suggestions relating to improving the clarity or specificity of the document will be taken into consideration for revisions and other material that will be developed. We appreciate the feedback.