Future Root Zone
KSK Rolls

Kim Davies
VP, IANA Services; President, PTI
Problem Statement

• First KSK was created in 2010 (“KSK-2010”)
• Design team was formed to develop a set of recommendations on how to perform a rollover
• Originally scheduled for 2017, the second KSK (“KSK-2017”) ultimately started signing the zone on 11 October 2018
  • One year pause in process to consider impact of anomalous telemetry data
• Rollover successfully occurred with minimal disruption
• What do we want to do now?
Initial feedback

• Recognizing community interest in the rollover was at its peak during and shortly after the rollover, we solicited comments and directed responses to the ksk-rollover list for capture.
• We undertook to analyze those comments in 2019H2 and produce a recommendation for future rollovers
• Common themes in this early commentary:
  • KSK rollover should be a routine event
  • KSK should be rolled over annually
  • Introduce backup and/or standby keys
  • Perform more monitoring of impacts of larger keysets
  • Consider alternate signing algorithms
Our proposal

• Create a predictable approach to future rollovers
• Plan for a three-year rollover interval to balance desire for more regular rollovers with the operational complexity involved
• At least two years for the new trust anchor to be published in advance, allowing greater propagation before the rollover
• Use similar phased approach aligned with the quarterly key ceremony schedules
Proposed key lifetime

- It takes 3 quarters to generate and successfully replicate the new KSK
- 7+ quarters in standby state: pre-populated and capable for unscheduled roll
- 12 quarters in active state: signing the zone
- 3 quarters to revoke: revocation period plus destruction in KSKs
Subsequent key lifetimes
Choice of Interval

• A common suggestion from early commenters was to perform an annual rollover.
• Because of the multiple quarters in advance to generate, pre-populate and pre-publish KSKs, plus quarters following for revocation and destruction, and annual cycle (without any delays) would have 4 or more KSKs in play at some times.
• We consider this to result in too much unneeded complexity for KSK operations
  • KSK handling operations in the key ceremony context is time-intensive and each additional act introduces risk of error.
• KSK ceremonies are already more lengthy due to:
  • Multiple KSRs being signed for multiple phase/fallback scenarios
  • Replacement cycles (HSMs, TCRs, Smart cards, etc.)
• We want to keep ceremonies to a manageable length to ensure participant focus on the key items
Earlier generation

- The lifecycle results in the earlier generation of the KSK than was used in the KSK-2017 plan
- Provides several benefits:
  - At least two years for software vendors and other distributors of the trust anchor to upgrade their distributions
  - Provides a greater window when, should an emergency unscheduled rollover be performed, have a ready KSK to use that is at least partially shared with operators
  - Any negative impacts of sharing the key earlier on security outcomes was considered negligible
No backup or standby key

- We have not proposed a dedicated backup or standby key, other than the pre-published key acting in a standby capacity.
- As we do not have alternate facilities to a suitable specification to store any additional key, the benefit appears to be marginal.
  - Storage in the existing 2 KMFs would result in fate-sharing that mitigates the benefits for most scenarios.
  - Detailed consideration needed for any kind of storage alternative.
Algorithm Change

- We agree this needs to be investigated.
- However, we don’t believe a mature approach is known, and thus it is not an IANA operationalization exercise, but rather first a research exercise.
- We propose activity relating to research into algorithm change be performed as a separate activity, perhaps much like the original rollover explorations.
Public Consultation

• We’ve published a paper that outlines the approach.
• It is now open for public comment
• Public comment period is posted now, open until end of January
• We will distill the feedback in the new year and turn them into operational practice
In Summary

- The rollover from KSK-2010 to KSK-2017 was widely considered successful
- We seek to replicate this success with a similar methodology
- Our aim is to target a 3-year active period for each KSK
  - Annual rollovers would result in too much overlap between lifecycles, too much operational complexity
  - We create the KSK early to allow greater period of time for pre-population and provides more time for use in an unscheduled/emergency scenario
- Please provide feedback to us, either endorsing the approach and suggesting alternatives
- We will try to finalize the approach in the new year and communicate our operational plan
Bonus Slide: Trusted Community Representatives

• We are almost at the 10 year anniversary for KSK operations
• Trusted Community Representatives are the community volunteers that observe ceremonies, and oversee key shares used to activate the KSK
• Current class of TCRs all originate from the 2010 selection round
• Recognizing some wished to retire and our backup pool of pre-selected TCRs was shrinking, we created an evergreen solicitation for Statements of Interest
  • http://iana.org/tcr
• First selections have been made with the new process
  • Backup pool back to 10 per our target
• Additional selections will be made as backups are promoted to replace active TCRs
• If you are interested, please apply!
Useful reading on the history to date

- Root Zone KSK Rollover Plan (March 2016)

- Review of the 2018 DNSSEC KSK Rollover (March 2019)

- ICANN Project page for last rollover
  https://www.icann.org/resources/pages_pages/ksk-rollover
Thank you!

kim.davies@iana.org