Root KSK Updates

Kim Davies
VP, IANA Services; President, PTI

PTI | An ICANN Affiliate

ICANN COMMUNITY FORUM 67
7–12 March 2020

Updates

- Consultation on Future KSK Rollovers
- Retrospective on Ceremony 40
- Planning for Ceremony 41

Consultation on Future KSK Rollovers

- 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?**

. IN DS 20326 8 2
E06D44B80B8F1D39A95C0B0D7C65D084
58E880409BBC683457104237C7F8EC8D

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

Public Consultation

- We published an outline of the approach.
- https://www.icann.org/public-comments/proposal-future-rz-ksk-rollovers-2019-11-01-en
- Public comment period closed last month, in the process of distilling feedback received from 11 comments.
- Currently in the process of compiling staff report (delayed due to key ceremony issues we’ll discuss in a moment)

Some themes in comments

- Pre-publication of standby key
    - Various opinions on whether it is problematic
- Timing changes
    - Adjust number of keys or periods to provide for constant coverage with a standby key
    - Consider sunset provisions for key strength
    - Consider loss of skills by HSM operators
    - Other suggestions for tweaking phases
- Risk mitigations
    - Consider not keeping standby keys in the HSMs
    - Consider alternate mechanisms for generating keys
- Algorithm roll
    - Some felt it was necessary to be a ‘blocker’ for this project, others felt it being a parallel activity was OK

More themes in comments

- Cadence
  - Seems to be general support
- Outreach to communicate root-related changes
- Editorial suggestions for the document itself
- Additional IANA mandates
  - Measurement
  - Advice to regulators and policy makers

A surprise?

- Some responses argued for much more specificity or comprehensiveness in the consultation material
- Our plan had been to consult and obtain agreement in the high-level principles outlined, then convert it into a detailed implementation — including DPS amendments, operational practices and procedures.
- How can we capture and capitalize on the proven experience of the first key rollover without trying to resolve all open questions about future KSK operations?
  - Some items require deep research beyond IANA's competency
  - We have a small team and larger projects need multi-year planning, funding, recruiting ICANN resources, community teams, etc.
- Not clear if we didn't communicate this well enough, or the expectation was all of the details needed to necessarily be put to public comment first.

KSK Ceremony 40

(The last one)

Key Ceremony 40

- Scheduled for 12 February 2020
- Objectives
  - Sign the 2020Q2 key material (covering April-June 2020)
  - Decommission a HSM
- Pre-ceremony activity included maintenance work to upgrade the lock assemblies within the safe
  - These are performed in administrative ceremonies that are audited to the same standard as the key signing ceremonies, but do not involve HSM activation
  - Administrative ceremonies can also include when we induct new staff members into trusted roles
  - TCRs that are available are invited to witness these administrative ceremonies

Key Ceremony 40

- On 11 February, the pre-ceremony work was being conducted to upgrade the lock assembly with a newer model.
- The safe would not open.
  - The device indicated the combination was dialed correctly, but the bolt did not retract to allow safe access.
  - Electrical or mechanical failure of the lock.
- The remedy exercised one of the worst-case disaster recovery scenarios that had been contemplated — “drilling the safe”.
  - Approximately 20 hours across two days to drill into the lock assembly, remove the bolt, to allow the safe to open
  - Followed by safe remediation and installation of new lock
  - Complicated by triggering anti-defeat mechanisms in the lock due to novel materials in safe construction

Some takeaways

- Ceremony was successfully conducted with a 4 day delay
- Gained valuable experience that will inform our future plans for disaster recovery
- Community volunteers and staff alike supported us around the clock to bring the issue to conclusion and perform key ceremony
- Some revisions to administrative ceremonies moving forward to provide greater transparency.

KSK Ceremony 41

(The next one)

Key Ceremony 41

- Scheduled for 23 April 2020 (10 year anniversary!)
- Objectives
  - Sign the 2020Q3 key material (covering July-September 2020)
  - Replace two Trusted Community Representatives (COs)
- Currently expected to be held as planned, but the evolving Coronavirus situation has caused us to focus on developing contingencies in case the situation deteriorates
- Ongoing work
  - Periodic re-evaluation of participants ability to travel
  - Continuous monitoring of evolving threat situation
  - Building out contingency scenarios
- Notably, the design of the Key Management Facilities is designed to enable key operations to be performed in a disaster recovery scenario without the minimum number of TCRs present.
  - The exact triggering conditions, however, have not been well defined.

Contingency ideas

- Roughly in increasing order of severity:
  - Hold the ceremony with less than ideal number of people present
  - Advance the ceremony date
  - Postpone the ceremony date
  - Hold the ceremony in the alternative facility
  - Induct new TCRs to replace those unable to travel
  - Sign key material beyond a single quarter
  - Perform ceremony with less than 3 TCRs physically present, and/or below other staffing minimums
- Long-term mitigators for future ceremonies:
  - Re-evaluate alternate KMF locations
  - Reconfigure how many TCRs are needed, their geographic locations, can they overlap roles, etc.
- Areas we are exploring DPS updates
  - More precise triggering conditions mapped out in advance for contingency scenarios

Thank you!

kim.davies@iana.org