KSK Rollover

James Mitchell

IANA Community Day
17 November 2022

Agenda

- Background
- Proposal for Future KSK Rollovers
- Public comment review
- Standby keys
- Next steps

Background

- The first KSK rollover was a multi-year process that eventually saw the successor and current key become active on 11 October 2018
- OCTO published a Review of the 2018 DNSSEC KSK Rollover (November 2019)
  - There were only a few reports of resolver outages after 11 October 2018 ... [unable to ascertain] whether or not the rollover had been a cause of the reported problems.
  - There was no impact on the root server system
- ICANN published a Proposal for Future Root Zone KSK Rollovers (November 2019) for public comment.

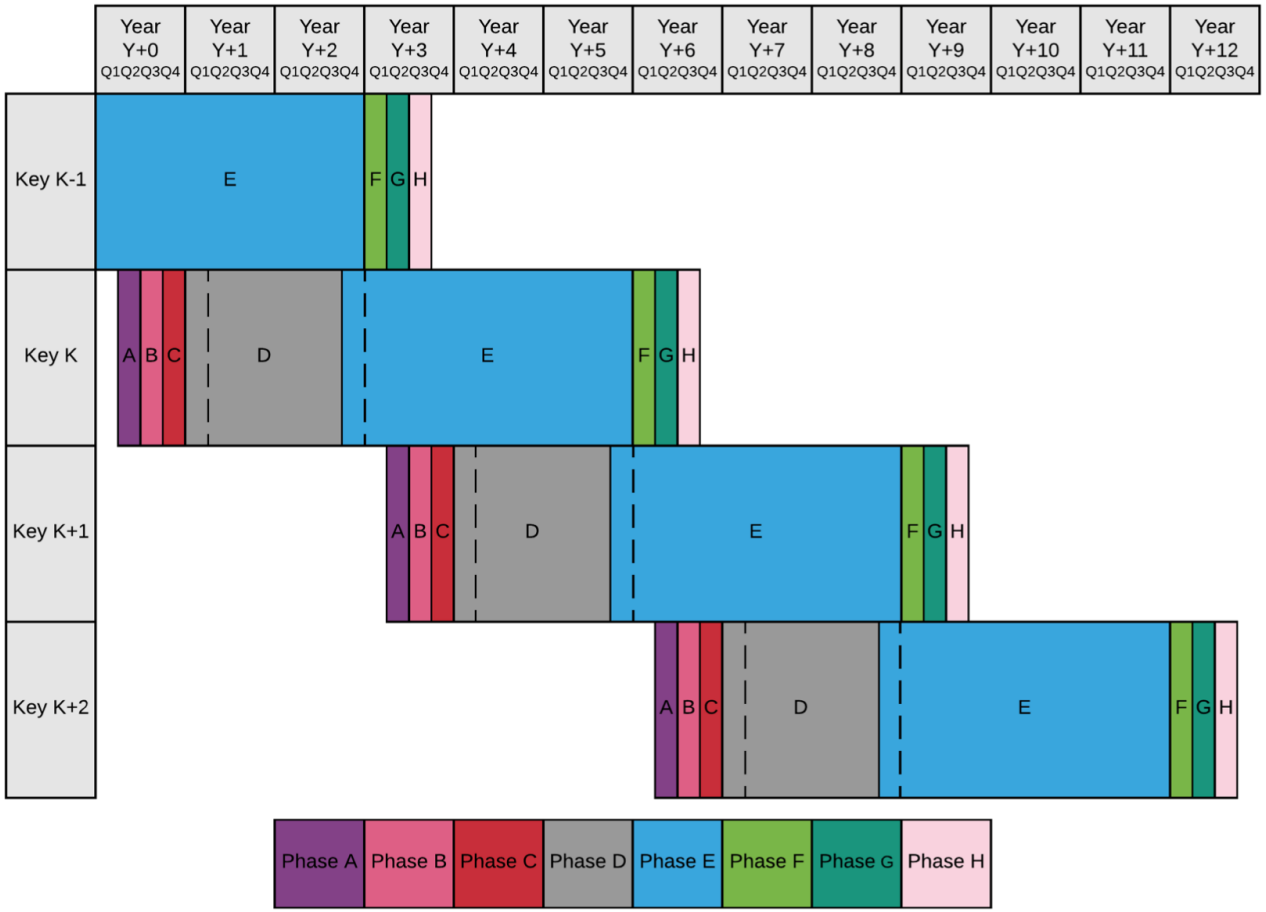
Impact of the pandemic

- The emerging pandemic led to establishment of emergency procedures
  - We weren't sure if we would be able to congregate for a ceremony
  - We couldn't predict the course of the pandemic
  - Travel was impacted with closure of borders, suspension of visa processing, and cancelation of flights
- Emergency procedures
  - Operation with minimal staff-only ceremonies
  - Remote participation from TCRs
  - Generation of signatures for three quarters
- Emergency procedures have since been rolled back

Proposal for Future KSK Rollovers

- Proposal for steady-state KSK rollovers
- Recognizes the general success of the first rollover and intention to reuse the operational plans.
  - https://www.icann.org/resources/pages/ksk-rollover-operational-plans
- Recommends establishing a three-year active period
  - Frequent enough that ICANN and the community will be well-practiced in the KSK rollover process
  - Infrequent enough to reduce the operational complexity of managing multiple keys
- Recommends establishing a two-year pre-publication period allowing software and devices time to adopt and trust the standby KSK before the rollover to an active state.

Proposal for Future KSK Rollovers



A. Generation
B. Replication
C. Signing
D. Publication/Ready
E. Active
F. Revocation
G. Deletion
H. Deletion

Public comment review

- Community responses from eleven from individuals and groups covered sixteen themes.
- Lack of specific details in the proposal
  - Proposal based on the 2018 Operational Plans. Broader Policy and Procedure documents have since been published:
    - https://www.iana.org/dnssec/procedures
- Maintaining skills over long intervals
  - 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 and rehearsed.

Public comments review

- 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
- Alternate the key generation site
  - The proposed timeline has keys generated in Q2 (East) and replicated in Q3 (West) and therefore key generation favors one site and one set of TCRs.
- 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.

Standby key

- Rollover plan is designed for periodic non-emergency rollover to limit the operational lifetime of any one key. A long pre-publication period assists with the distribution and adoption of the next trust anchor.
- A standby key is designed to facilitate a swift response to unplanned events. A successor key may function as a standby key once it is in the Ready state.
  - Except when the successor key shares the same fate as the active key.
- To be broadly effective, use of a standby key will require significant changes to the operational practices and design of KSK management functions.
- **Takeaway**: the successor key may not be an effective standby key.

Next steps

- Operational ready to generate keys by Q2 2023
  - Expect to complete the credential reissue in Q1 2023.
  - Introduce new signing software in Q2 2023. This necessitates a new version of the Ceremony Operating Environment (COEN).
- Incorporate the proposal and responses from public comment into operational plans. These plans will be put to public comment if there are material changes from the proposal or to our procedures.

Be informed

- Join the ksk-rollover mailing list
  - https://mm.icann.org/listinfo/ksk-rollover
- Follow ICANN for announcements
  - https://www.icann.org/en/announcements
- Become a Trusted Community Representative:
  - Cryptographic Operators who are actively involved in our key ceremonies
  - Recovery Key Share Holders who are involved in our disaster recovery planning
  - https://www.iana.org/help/tcr-application

Engage with PTI

PTI | An ICANN Affiliate

Thank You and Questions

Visit us at **iana.org**
Email: iana@iana.org