Root Zone DNSSEC Update

Kim Davies
VP, IANA Services; President, PTI

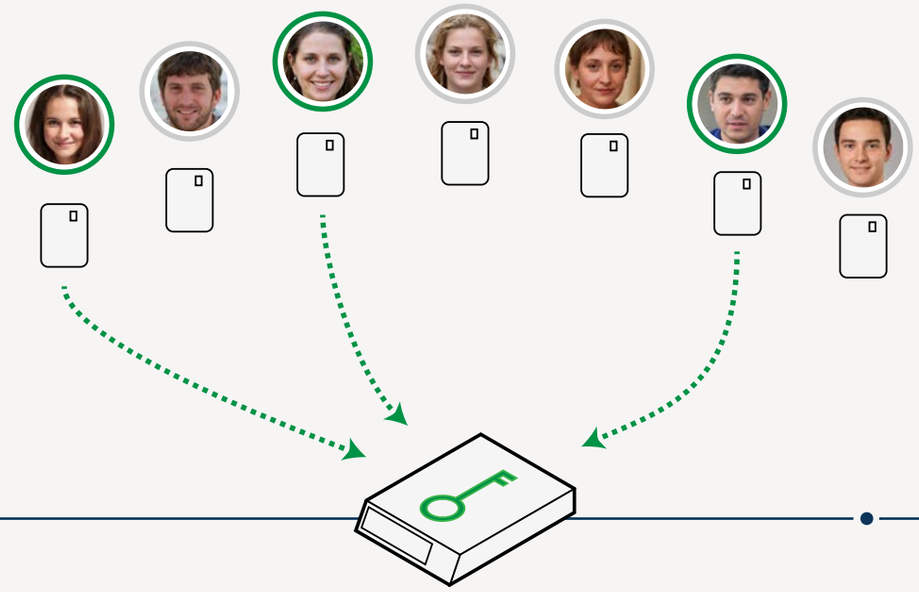
PTI | An ICANN Affiliate

Quarterly Ceremonies

- Key Signing Ceremony are being conducted at their regular cadence (every 3 months)
  - During 2020-2021 this was altered as a COVID-19 mitigation, but we can now confidently hold them as scheduled
- In-person attendance by trusted community representatives has resumed
  - Remote participation temporarily to limit exposure risk
- The last remaining deviation is the lack of participation by external witnesses and media
  - Will assess this based on contemporary risk analysis by ICANN Security Operations prior to each ceremony
  - We have had media interest that has been declined to recent ceremonies, but we'd like to foster awareness as soon as we can

Trusted Community Representatives

- Daniel Kaminsky replaced by David Lawrence as RKSH
  - More info in ICANN 72 presentation
- With in-person TCR participation at ceremonies resuming, significant turnover of TCRs is being planned for
  - Many TCRs have served since 2010 and are looking to move on
  - We seek an orderly, staggered change to TCRs to ensure knowledge retention
- We are always looking for SOIs: https://iana.org/tcr
  - Prize diversity in applicants, the TCRs as a whole are intended to bring a diversity of skills, backgrounds and attributes



Next KSK Rollover

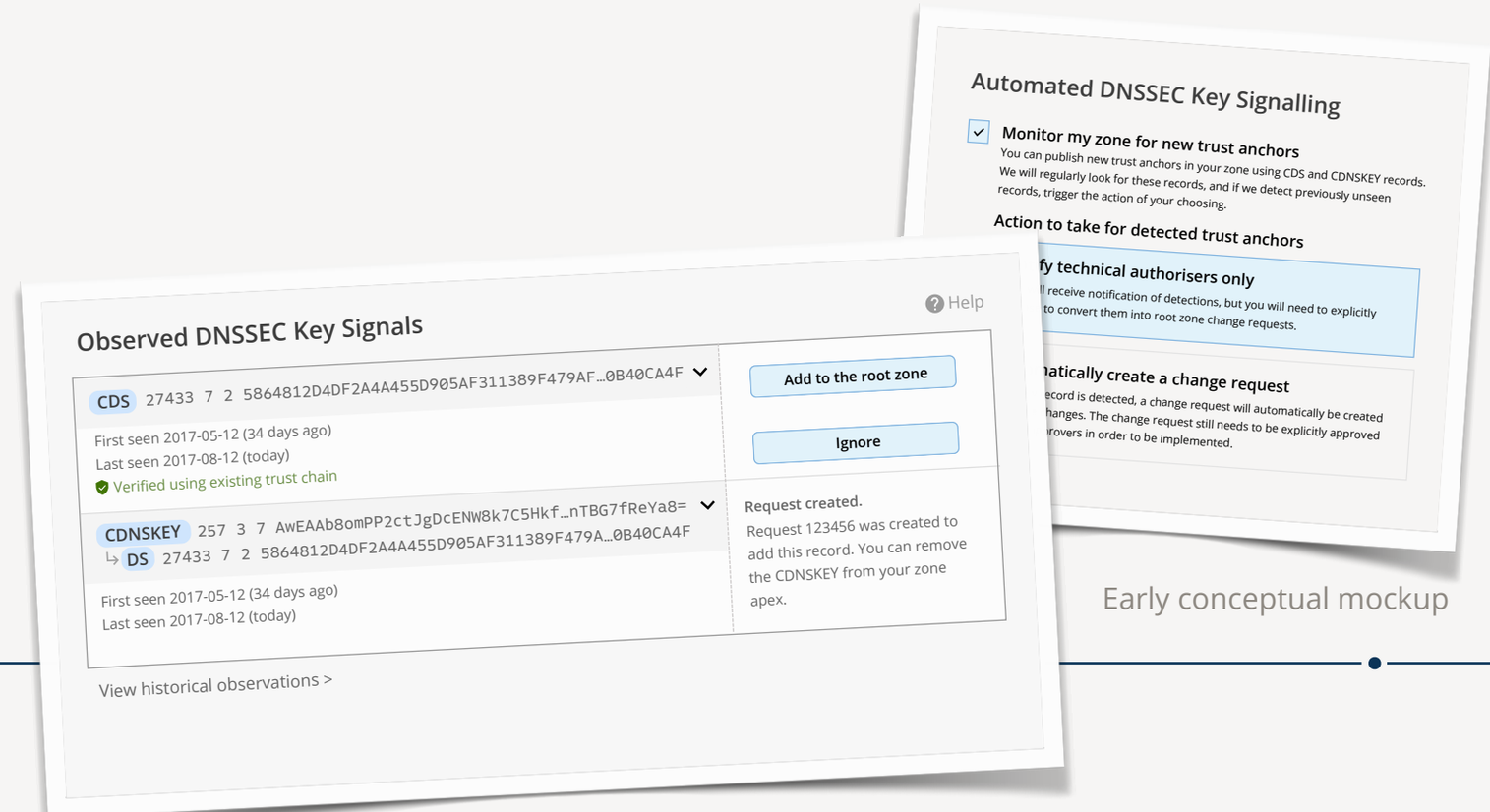
- First KSK was created in 2010, rolled to the next KSK on 11 October 2018
- In 2020, we conducted a public comment proceeding to gain feedback on future rollovers:
  - https://www.icann.org/en/public-comment/proceeding/proposal-for-future-root-zone-ksk-rollovers-01-11-2019
  - Some feedback included generating a standby key and providing longer lead time for public key propagation (More detail at ICANN 67)
  - It concluded, *"… 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 …"*
- We believe we are now at a level of certainty to start this planning, which will begin this fiscal year.

Algorithm Rollover

- We've committed to performing research and preparatory work for an algorithm rollover in the DNS root zone
  - Root Zone currently uses RSA/SHA-256
  - Algorithm rollover could migrate to an elliptic curve based algorithm, for example
- The next KSK rollover is not planned to be an algorithm roll
  - We expect the exploratory work to take too long to be ready
  - Expect to convene a design team similar to the process for the last KSK rollover
    - Use the resources of OCTO and contractors to support the exploration of issues, including test beds and the like
    - Develop a set of requirements that will then be used to develop an operational plan against
- Kick off of the project anticipated for November

Processing DS records

- We mentioned at ICANN 74 there had been no interest signalled in CDS support at the root zone
  - A few people raised their hands that they are interested
- Will consider the concept as part of a broader concept of proactive monitoring of delegations
  - Root Zone Update Study has recommended we institute such a process
  - Expect to engage with the community on specifics to inform our plans



Early conceptual mockup

Engagement kickoff

- Adjacent to the **ICANN DNS Symposium**, we will be holding a session on IANA technical evolution
  - https://www.icann.org/ids
- Two key themes will be:
  - Tech Check Evolution
  - Algorithm rollover for the DNS root zone
- Encourage your participation there, as we flesh out our thoughts in more detail
- Will also do online engagement, public comment periods and the like, throughout the process so there will be ample opportunity to contribute.
- But thoughts are welcome any time (including now!)

IANA Community Day
17 November 2022, Brussels

Thank you!

kim.davies@iana.org