

Root Zone KSK Update

Kim Davies
VP, IANA Services; President, PTI

October 2023

PTI | An ICANN Affiliate



Algorithm Rollover Study

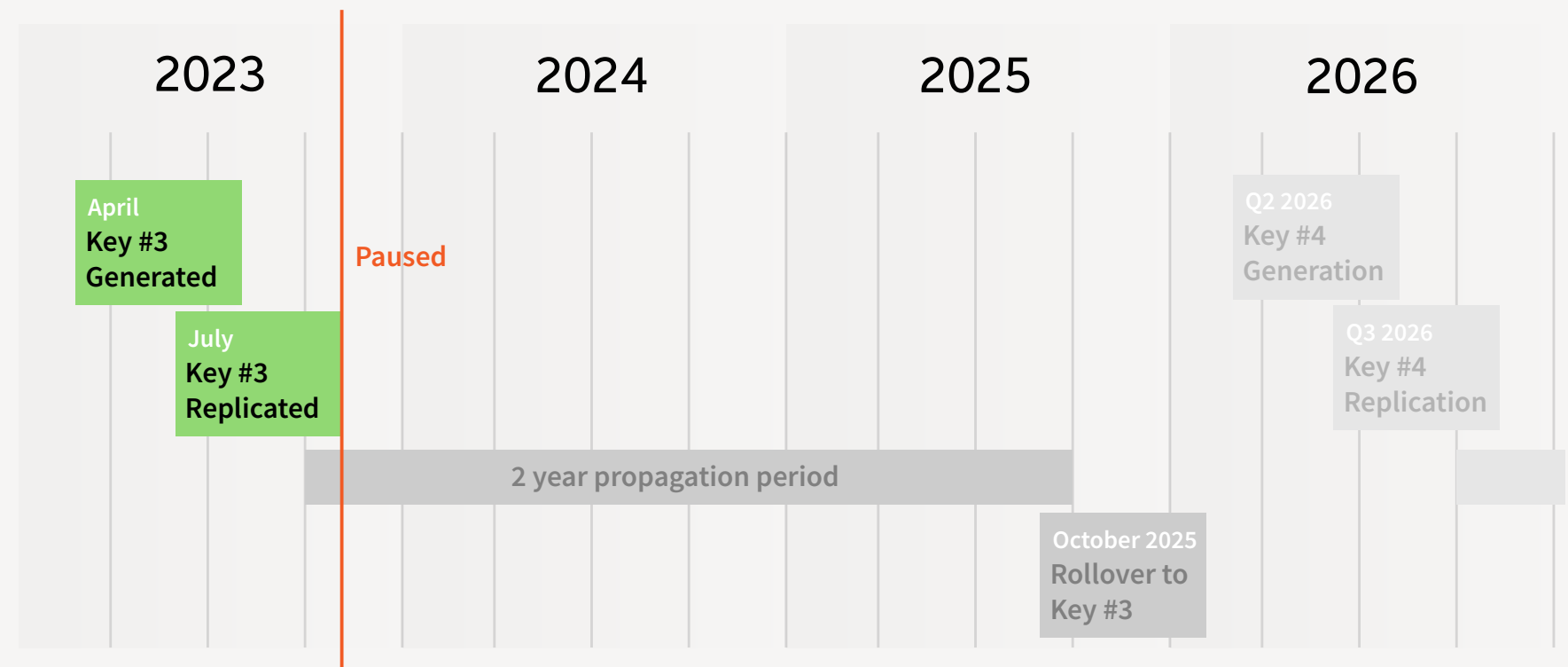
- Community convened in January to develop requirements to update the cryptographic key in the Root Zone
 - How to select an algorithm?
 - How to change the algorithm?
- Draft findings published 19 October, now seeking public comment
 - <https://www.icann.org/en/public-comment/proceeding/draft-report-of-the-root-zone-dnssec-algorithm-rollover-study-19-10-2023>
 - Comments close December 4

Algorithm Rollover Study (2)

- Does not specifically provide a timeline for changing the algorithm, but does recommend the algorithm is changed before it becomes necessary.
 - Not planned for next rollover.
- Found a rollover from the current KSK/ZSK key size to ECDSA would result in truncated NXDOMAIN responses from the root
 - Currently comprise about 50% of the traffic which would be a significant change
- Team noted option to reduce the size of the ZSK prior to rollover, promote protocol updates to reduce the response sizes during an algorithm rollover
- What to expect
 - Staff report due by the end of the year
 - Design team will meet early next year to consider the feedback and produce a final report.

2nd Key Rollover

- We've embarked on the 2nd ever replacement of the key
 - Highly orchestrated event, propagation to all validators through vendor updates etc.
- Generated the key in April 2023, replicated to second facility in July 2023
 - RSA/SHA-256 algorithm
- Paused activity to propagate
 - Public key not published/placed in trust anchor file



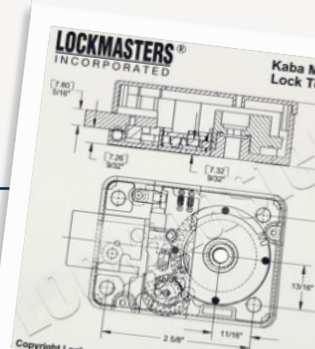
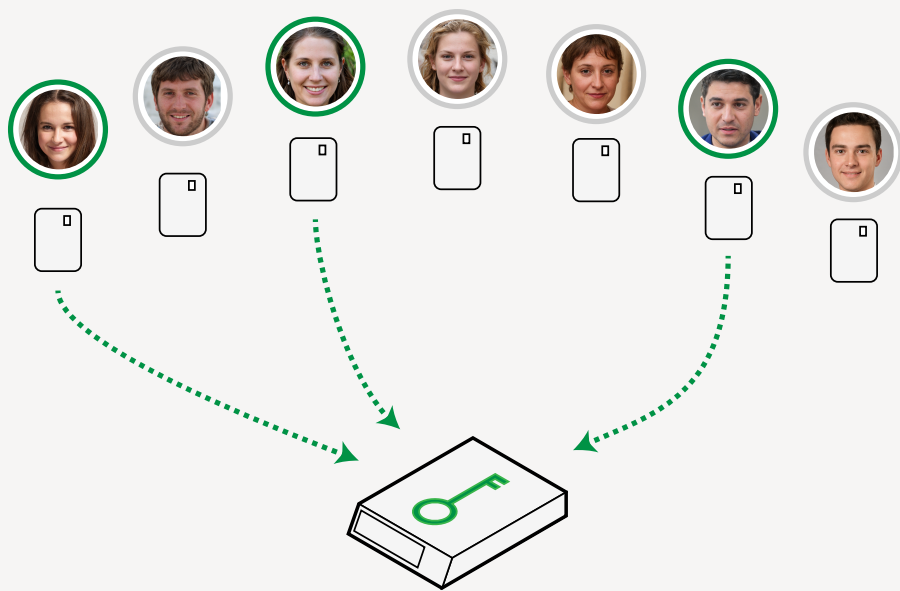
HSM Replacement

- Vendor of our AEP Keeper HSMs is exiting the HSM business
- Current landscape of FIPS 140 Level 4 HSMs is grim
- Evaluated four successor vendors, hardware trials with two:
 - Utimaco
 - Thales (Luna USB HSM G7)
- What can the community expect?
 - Likely will seek to drop to Level 3 HSM
 - Requires DPS amendment and possibly compensating controls
 - Procedural updates
 - Alternative HSMs are not like-for-like replacement, interact with them in different ways
 - No change in overall security posture
 - Further updates toward end of year

Trusted Community Representatives

- Community members are a key part of how we protect the key and build trust.
- Participate in and oversee ceremonies
- Maintain credentials required to activate the key.
- Diversity is important — including geography, skills and gender
- We're looking for volunteers to apply, particularly from underserved regions and with new skillsets

<https://iana.org/tcr>



Thank you!