

Root Zone KSK Rollover Update

Kim Davies
VP, IANA Services & President, PTI

Dublin
October 2025

PTI | An ICANN Affiliate

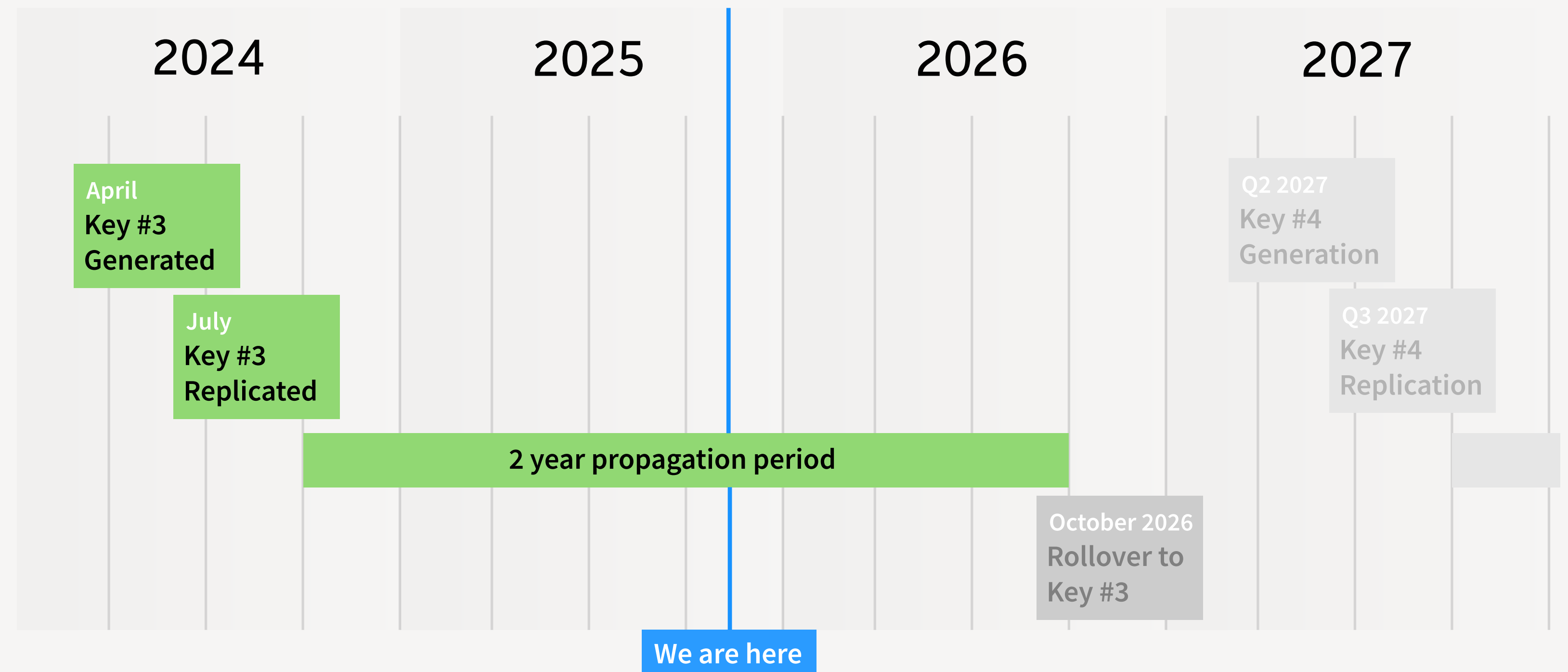


Background

- SSR2 recommended that IANA work with other root zone partners and the global community to develop a consensus plan for future root DNSKEY algorithm rollovers.
- Design Team provided recommendations on the topics of cryptographic function selection and future implementation plans.
- IANA is chartering and initiating the project to build operational capabilities to change the algorithm.
 - Recurring process to evaluate the algorithm
 - Detailed operational plans for the rollover
 - Updates to policies and procedures
 - Software support

Updating the key

- We've embarked on the 2nd ever replacement of the key
 - Highly orchestrated event, propagation to all validators through vendor updates etc.
 - Delayed due to (a) COVID, and (b) key hardware vendor change; but now underway
- Implements a 3 year cadence, with new algorithm potential in 2027 and beyond



Now available

- The new trust anchor is now available for propagation (XML file)
 - Most users will adopt it naturally through software updates
 - Will appear in the DNS itself starting 11 January 2025 (RFC 5011)
 - Note — new format per RFC7958bis

Key Status

This table provides additional guidance on how keys have been issues and used. Software implementers should rely on the XML trust anchors file for normative parameters on keys.

INFORMAL NAME	STATUS	DETAILS
KSK-2024	Pre-Publication	Generated 2024-04-26 (attestation) with key tag 38696 and label Kmyv6jo. Expected to be published in DNS on 2025-01-11, and actively signing starting 2026-10-11.
KSK-2017	Active	Generated 2016-10-27 (attestation) with key tag 20326 and label Klajeyz. Signing since 2018-10-11.
KSK-2023	Abandoned	Generated 2023-04-27 (attestation) with key tag 46211 and label Kmrfl3b. Will not be used, superseded by KSK-2024.
KSK-2010	Retired	Generated 2010-06-16 (attestation) with key tag 19036 and label Kjgmt7v. Signing between 2010-07-15 and 2018-10-11.

<https://iana.org/dnssec/files>

What to expect for this rollover

- Rollover planned to occur 11 October 2026
- Communication outreach to begin mid-year
 - What to expect during the Root KSK rollover
 - Key practices
 - Readiness
- Key revocation in January 2027 (RFC 5011)
- Key and HSM destruction the following quarters

Preparing for an algorithm change

- Planning the subsequent rollover will also change the algorithm
 - Recommendation to perform controlled rollover to ensure preparedness
 - Benefit of smaller signatures from changing to other algorithms (e.g. ECDSA)
- Public consultation expected in Q1 2026
- Key generation in Q2 2027
- Conservative approach
 - Pre-publication of signatures
 - Sign with both algorithms for two years
 - Reduce the size of the ZSK
- Changes to process
 - Can't pre-publish the successor key as with a non-algorithm rollover
 - KSK and ZSK operations now occur at the same time

Systems development

- Considering test server to support *local* accelerated RFC 5011 testing
 - Working implementation of the operational plan and phases.
 - Give resolver vendors sufficient time to test and deploy their software.
- Key generation, signing, and procedure compliance
 - HSM testing and familiarization
 - Updates to the signing software
- Updates to the systems (both IANA and root zone maintainer)

Call for volunteers

<https://iana.org/tcr>



Thank you!

kim.davies@iana.org