Registries Stakeholder Group Statement

Proposed Root KSK Algorithm Rollover

Date statement submitted: 3 April 2026

(this is a copy of the comment submitted via the ICANN public comment platform)

Reference url:
https://www.icann.org/en/public-comment/proceeding/name-collision-procedure-documentation-29-01-2026

Background[1]

This Public Comment proceeding requests community feedback on the proposed DNS root zone Key Signing Key (Root KSK) algorithm rollover. The Root KSK is the global trust anchor for DNSSEC and is managed under the Internet Assigned Names Authority (IANA) functions.

The proposal sets out a multi-year implementation plan, beginning with the generation of a new ECDSA Root KSK in 2027 and ending with the retirement of the RSA Root KSK in 2029. Community feedback is particularly encouraged on the following topics:

- The proposed algorithm rollover methodology and implementation timeline.
- Operational readiness, including resolver and authoritative server compatibility
- Identification of additional risks that haven't been considered by the plan

Documents

- **Proposal for Root Zone KSK Algorithm Rollover (pdf, 351.21 KB)**

Related RySG comments

- RySG comment on the Draft Report of the Root Zone DNSSEC Algorithm Rollover Study (1 December 2023)
- RySG comment on the Plan to Restart the Root Key Signing Key (KSK) Rollover Process (2 April 2018)

Registries Stakeholder Group (RySG) comment

The gTLD Registries Stakeholder Group (RySG) welcomes the opportunity to comment and is supportive of the proposal for Root Zone KSK algorithm rollover. Of note, we want to highlight a couple of items from the proposal.

- The proposal recommends ECDSA using P-256 curve with SHA-256 for the next Root KSK algorithm. The RySG supports this choice for the next root algorithm noting that it is widely supported and implemented today.

- In order to minimize UDP truncation and fallback to TCP for root zone queries, the proposal recommends reducing the RSA zone signing key size from 2048 bits to 1536

[1] Background: intended to give a brief context for the comment and to highlight what is most relevant for RO's in the subject document – it is not a summary of the subject document.

bits. The RySG supports this recommendation and doesn’t have concerns with the proposed change.

- The RySG supports the proposed 4 year schedule. We note that it is in line with ICANN’s established timelines for root KSK rollovers (https://www.icann.org/en/system/files/files/proposal-future-rz-ksk-rollovers-01nov19-en.pdf)