RSSAC Statement on KSK Algorithm Rollover
06 April 2026

Public Technical Identifiers (PTI), supported by the DNS Community, proposes to replace the Key-Signing Key (KSK) algorithm for the DNS root with a new one.[1] The purpose for this operation would be to shift from using the RSA cryptographic algorithm to the ECDSA cryptographic algorithm. The RSSAC supports making this change.

This change is well-advised for several reasons.

1. The plan for making the change is sufficiently engineered and appears solid.

2. The proposal has been widely shared, and is generally supported by, the general DNS community. Specifically, the Internet Engineering Task Force (IETF) has indicated its use is recommended for both signing and validation.[2]

3. The ECDSA algorithm is modern and is the preferred default in modern DNS software and installations.

4. The DNSKEY records in the zone files will become smaller in size. This decreases traffic volumes and eases the load on both the root name servers and the resolvers sending the queries. This is a welcome operational change.

5. The ECDSA algorithm has been well tested and deployed operationally by many other zones for a number of years and its use globally has surpassed the use of the RSA algorithm used for the root zone.[3] It is expected that all major DNS resolver implementations will handle the new algorithm gracefully.

6. The RSSAC's only concern with the plan is the well documented need to decrease the size of the zone signing key (ZSK) in anticipation of the change, but the RSSAC believes this short-term trade off is acceptable given the longer term benefits.

The RSSAC sees notable benefits with making this change, and sees very few and minor risks. The RSSAC therefore supports going forward with making this change.

---

[1] See ICANN Public Comment, Proposed Root KSK Algorithm Rollover, https://www.icann.org/en/public-comment/proceeding/proposed-root-ksk-algorithm-rollover-03-02-2026
[2] See Domain Name System Security (DNSSEC) Algorithm Numbers, https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml
[3] See DNSSEC and DANE Deployment Statistics, https://stats.dnssec-tools.org/#/?dnssec_param_tab=0&trend_tab=0

RSSAC064
Approved by the RSSAC on 06 April 2026