Dear Registrar,

The IETF has published updated guidance for DNSSEC cryptographic algorithms, reflecting current DNSSEC cryptographic and operational practices. As a result, several DNSSEC signing algorithms that were previously in use are now considered weak or deprecated.

We strongly recommend that DNS operators performing DNSSEC signing or managing DNSSEC operations transition away from weak and deprecated DNSSEC signing algorithms due to the significant security risks they pose.

This recommendation is based on earlier communications, and guidance published by the IETF in RFC 9904, RFC 9905, and RFC 9906, which provide authoritative direction on DNSSEC algorithms, key sizes, cryptographic strength, and operational practices. These documents reflect the current state of DNSSEC deployment and serve as a reference for aligning implementations with modern security expectations.

Deprecated DNSSEC Algorithms

As per the above RFCs, the following DNSSEC algorithms are deprecated and **MUST NOT** be used for new key generation or zone signing:

- RSA/SHA-1 (RSASHA1, RSASHA1-NSEC3-SHA1)
- DSA (DSA, DSA-NSEC3-SHA1)
- ECC-GOST (GOST R 34.10-2001)
- RSAMD5

Additionally, SHA-1 **MUST NOT** be used as a digest algorithm for DS records. DNS/DNSSEC operators currently using this digest algorithm are strongly encouraged to plan a transition away from it.

Furthermore, in the IANA DNSSEC Digest Algorithms registry, SHA-256 (Digest Type 2) is the only algorithm currently designated as MUST for both DNSSEC delegation and DNSSEC validation, making it an appropriate choice for interoperability on the Internet.

Recommended DNSSEC Algorithms

The following DNSSEC algorithms are currently **RECOMMENDED**:

- RSA/SHA-256 (RSASHA256)
- ECDSA P-256 (ECDSAP256SHA256)
- ECDSA P-384 (ECDSAP384SHA384)
- Ed25519 (EdDSA)

DNSSEC algorithm transitions must be carefully planned to avoid validation failures, ensure DS records are updated before KSK retirement, and maintain resolver compatibility through dual-signing when required. RIPE Labs published an article which discusses their prior experience with a DNSSEC algorithm roll-over which may provide useful advice.

All gTLD registry operators are contractually bound to follow this new guidance. Therefore, your systems may require updates to properly interact with some gTLD registry operators. If you have questions regarding a specific gTLD and updates they may require, please contact the registry operator for that gTLD.

Additionally, you may also find it helpful to review the DNSSEC Deployment Guidebook for ccTLDs that was published in OCTO-029 and its reference documents.

If you have any questions on this issue, please feel free to reach out to ICANN org's Global Support Center.

Best Regards,
Technical Services Team
Global Domains Division
Internet Corporation for Assigned Names and Numbers (ICANN)