Dear Registry Operator,

This is a courtesy notice that a DNSSEC-related RFC (RFC 9904) was recently published by the IETF. This RFC updates RFC 4034: as a reminder, Registry Operators are required to comply with RFC 4034 and its successors. This courtesy notice is being shared in light of the importance of this RFC.

RFC 9904 introduces new columns to the DNS Security Algorithm Numbers and Digest Algorithms IANA registries, which indicate whether algorithms in those registries can be used for various purposes. Two subsequent RFCs (RFC 9905 and RFC 9906) then update those columns, based on current cryptographic analysis of some algorithms. As a result, several DNSSEC signing algorithms that were previously in use are now considered weak or deprecated.

Per the updates made to the IANA registry, Registry Operators are expected to transition away from weak and deprecated DNSSEC signing algorithms.

The above expectation is based on earlier communications, and guidance published by the IETF in RFC 9904, RFC 9905, and RFC9906, which provide authoritative direction on DNSSEC algorithms, key sizes, cryptographic strength, and operational practices.

These documents 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

In light of the deprecation of the algorithms listed above, the following DNSSEC algorithms are currently **RECOMMENDED** for DNSSEC Signing in the DNS Security Algorithm Numbers Registry. Registry Operators should use one or more of the following:

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

Algorithm Rollovers

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. The gTLD zone **MUST** remain valid at all times, as required by the Registry Agreement.

For reference, RIPE Labs published an article which discusses their prior experience with a DNSSEC algorithm roll-over which may provide useful advice.

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)