Multiple Algorithm Rules in DNSSEC

Shumon Huque

ICANN DNSSEC & Security Workshop

June 9th 2025, Prague, CZ.

Background

ICANN73 (March 2022) - “RFC Adjustments for Multi-Signer” (S. Huque)

Proposed relaxing the rules for the use of multiple algorithms in DNSSEC, to allow multi-signer configurations to work across providers that supported different signing algorithms.

And also to allow signed zone migration across providers that used different algorithms (which typically involves a transient case of multi-signer).

RFC 4035: Protocol Modifications for DNSSEC

Section 2.2 (last paragraph)

> There MUST be an RRSIG for each RRset using at least one DNSKEY of each algorithm in the zone apex DNSKEY RRset. The apex DNSKEY RRset itself MUST be signed by each algorithm appearing in the DS RRset located at the delegating parent (if any).

Proposal was to simply remove this restriction.

And simply rely on zone owners to take reasonable actions - if they wanted to deploy a configuration with multiple distinct algorithms and allow for single algorithm signed responses at each provider or server, they should only use well-known, widely supported algorithms.

RFC 6840: Clarifications .. for DNSSEC

Section 5.11

```
This requirement applies to servers, not validators.  Validators
SHOULD accept any single valid path.  They SHOULD NOT insist that all
algorithms signaled in the DS RRset work, and they MUST NOT insist
that all algorithms signaled in the DNSKEY RRset work.
```

Proposal was to change the “SHOULD NOT” phrase here to “MUST NOT”.

That way validating resolvers must not require that signatures of all algorithms denoted in the DS RRset must be present in responses. (Note: this is already largely true today, though there are some implementations which have an option that can change this behavior).

A current and more nuanced proposal

After some detailed discussions with other DNS protocol engineers, a more nuanced proposal has emerged, documented in an IETF draft on “Multiple Algorithm Rules in DNSSEC”.

- Authors: Shumon Huque (Salesforce), Peter Thomassen (deSEC), Viktor Dukhovni (OpenSSL), Duane Wessels (Verisign), and Christian Elmerot (Cloudflare).

We now propose to relax the cited protocol restrictions more selectively, in the presence of well known algorithms, which we formally propose to designate as UNIVERSAL.

While still protecting against “downgrade to insecure” attacks.

Summary Issues

Current protocol rules are too restrictive to support several desired use cases:

- Multi-Signer configurations where each multi-signer party supports a different signing algorithm.
- Non-disruptive transfer of a signed zone between DNS providers that support disjoint signing algorithms.
- Pre-publication of a trust anchor in preparation for an algorithm rollover (such as for the root zone)
- Independently rolling the algorithm for a KSK or ZSK.
- Computational burden for online signers supporting a zone with multiple algorithms.

https://www.ietf.org/id/draft-huque-dnsop-multi-alg-rules-05.html

Workgroup:	Internet Engineering Task Force
Updates:	4035, 6840, 8624 (if approved)
Published:	28 May 2025
Intended Status:	Standards Track
Expires:	29 November 2025

Authors:	S. Huque	P. Thomassen	V. Dukhovni	D. Wessels	C. Elmerot
	Salesforce	*deSEC, SSE*	*Google LLC*	*Verisign*	*Cloudflare*

Multiple Algorithm Rules in DNSSEC

Abstract

This document restates the requirements on DNSSEC signing and validation and makes small adjustments in order to allow for more flexible handling of configurations that advertise multiple Secure Entry Points (SEP) with different signing algorithms via their DS record or trust anchor set. The adjusted rules allow both for multi-signer operation and for the transfer of signed DNS zones between providers, where the providers support disjoint DNSSEC algorithm sets. In addition, the proposal enables pre-publication of a trust anchor in preparation for an algorithm rollover, such as of the root zone.

This document updates RFCs 4035, 6840, and 8624.

UNIVERSAL and FORMERLY-UNIVERSAL algorithms

UNIVERSAL

- Algorithms are that are widely supported by almost all validators, and are recommended for signing, in RFC 8624 (and 8624-bis).
- Presently, only 8 (RSASHA256) and 13 (ECDSAP256SHA256), are thus designated.

FORMERLY UNIVERSAL

- Widely supported, but are now deprecated, or with declining support.
- Presently, 5 (RSASHA1) and 7 (RSASHA1-NSEC3-SHA1).

The IANA DNSSEC algorithms registry is proposed to be extended with a universality column to allow such designations to be declared.

Updated Signer Requirements

from Section 2.2. Signer Requirements

1. Absent any UNIVERSAL algorithms in the DS RRset or trust anchor set, or when any FORMERLY UNIVERSAL algorithms are present, signers MUST sign with all algorithms listed.
2. Otherwise, signers MUST sign with at least one UNIVERSAL algorithm listed in the DS RRset or trust anchor set. Other signatures are OPTIONAL

UNIVERSAL and FORMERLY UNIVERSAL algorithms SHOULD NOT appear together in a DS RRset or trust anchor set. In fact, FORMERLY UNIVERSAL algorithms are best avoided: signers SHOULD transition to other algorithms that are UNIVERSAL

Updated Validator Requirements

from Section 2.3. Validator Requirements

1. When the DS RRset or trust anchor set for a zone includes an unsupported FORMERLY UNIVERSAL algorithm, validators MUST treat the zone as unsigned, even if the DS RRset or trust anchor set lists another supported algorithm.
2. Otherwise, validators MUST accept any valid path. ← same as today

Implementing these rules requires validators to keep a record of unsupported FORMERLY UNIVERSAL algorithms, so that the zone's security status can be established upon inspection of a DS record or TA set.

```
example.com.    DS      <keytag>  8 <digesttype> <digest.
example.com.    DS      <keytag> 13 <digesttype> <digest.
```

Provider/Signer 1:

```
example.com. DNSKEY 257 <proto> 8 <key> (KSK1)
example.com. DNSKEY 256 <proto> 8 <key> (ZSK1)
example.com. DNSKEY 256 <proto> 13 <key> (ZSK2)
       RRSIG DNSKEY signed by KSK1 only

example.com.    A   10.1.1.1
          RRSIG A signed by ZSK1 only
```

Provider/Signer 2:

```
example.com.    DNSKEY    257 <proto> 13 <key...> (KSK2)
example.com.    DNSKEY    256 <proto>  8 <key...> (ZSK1)
example.com.    DNSKEY    256 <proto> 13 <key...> (ZSK2)
          RRSIG DNSKEY signed by KSK2 only

example.com.    A   10.1.1.1
          RRSIG A signed by ZSK2 only
```

Status of the draft

Only an individual submission at the moment.

Will be presented for more detailed discussion at the next IETF meeting (IETF 123 in Madrid, July 2025), with the goal of getting it adopted by the DNSOP working group in the near future, and eventually standardized.

Has also been mentioned on the dnsop list.