The future of DNSSEC cryptographic recommendations

AKA draft-ietf-dnsop-rfc8624-~~bis~~ replacement

Wes Hardaker
Warren Kumari

RFC8624 reminder: algorithm implementation recommendations

- A**lgorithm definitions** published in **various documents**
- Added to the various IANA tables
- **RFC with the recommendations** only sporadically updated

3. Algorithm Selection

3.1. DNSKEY Algorithms

The following table lists the implementation recommendations for DNSKEY algorithms [DNSKEY-IANA].

Number	Mnemonics	DNSSEC Signing	DNSSEC Validation
1	RSAMD5	MUST NOT	MUST NOT
3	DSA	MUST NOT	MUST NOT
5	RSASHA1	NOT RECOMMENDED	MUST
6	DSA-NSEC3-SHA1	MUST NOT	MUST NOT
7	RSASHA1-NSEC3-SHA1	NOT RECOMMENDED	MUST

draft-ietf-dnsop-rfc8624-bis

Adds ~~3~~ 6 columns to existing tables:

IANA Table	Column added
Domain Security Algorithm Numbers	Use for DNSSEC Signing
	Use for DNSSEC Validation
	Implement for DNSSEC Signing
	Implement for DNSSEC Validation
Digest Algorithms	Use for DNSSEC Delegations
	Implement for DNSSEC Delegations

Changes from recent list discussions

N	Mnemonics	Use for DNSSEC Signing
8	RSASHA256	**MUST**
13	ECDSAP256SHA256	**MUST**

MUST you use both algorithms?

Changes from recent list discussions

N	Mnemonics	Use for DNSSEC Signing
8	RSASHA256	**RECOMMENDED**
13	ECDSAP256SHA256	**RECOMMENDED**

MUST you use both algorithms?

No, so… MUST ⟹ RECOMMENDED

“When there are multiple RECOMMENDED algorithms in the "use" column, operators should choose the best algorithm according to local policy.”

Recent list discussions

How does this document interact with the proposed algorithm phasing document?

draft-crocker-dnsop-dnssec-algorithm-lifecycle

Answer: dnsop-rfc8624-bis may be the building block for the other

TL;DR:

- Algorithm changes should allow for any/all combinations when needed
- Potential future phasing will require/recommend column value combinations

Next Steps

Last call for final changes/suggestions?

- `draft-ietf-dnsop-rfc8624-bis`
- `draft-ietf-dnsop-must-not-sha1`
- `draft-ietf-dnsop-must-not-gost`

Note: the two algorithm update documents haven’t changed recently