A New Default

Jakob Schlyter

Roy Arends

Matt Larson

RFC6944

Must Implement	Must Not Implement	Recommended to Implement	Optional
RSASHA1	RSAMD5	RSASHA256 RSASHA1-NSEC3-SHA1 RSASHA512 ECDSAP256SHA256 ECDSAP384SHA384	Any registered algorithm not listed in this table

RFC6944

If the status of any algorithm in the table changes, a new document shall make this document obsolete.

That document shall include a replacement of the table.

It is not meant to be a discussion on algorithm superiority.

RFC6944

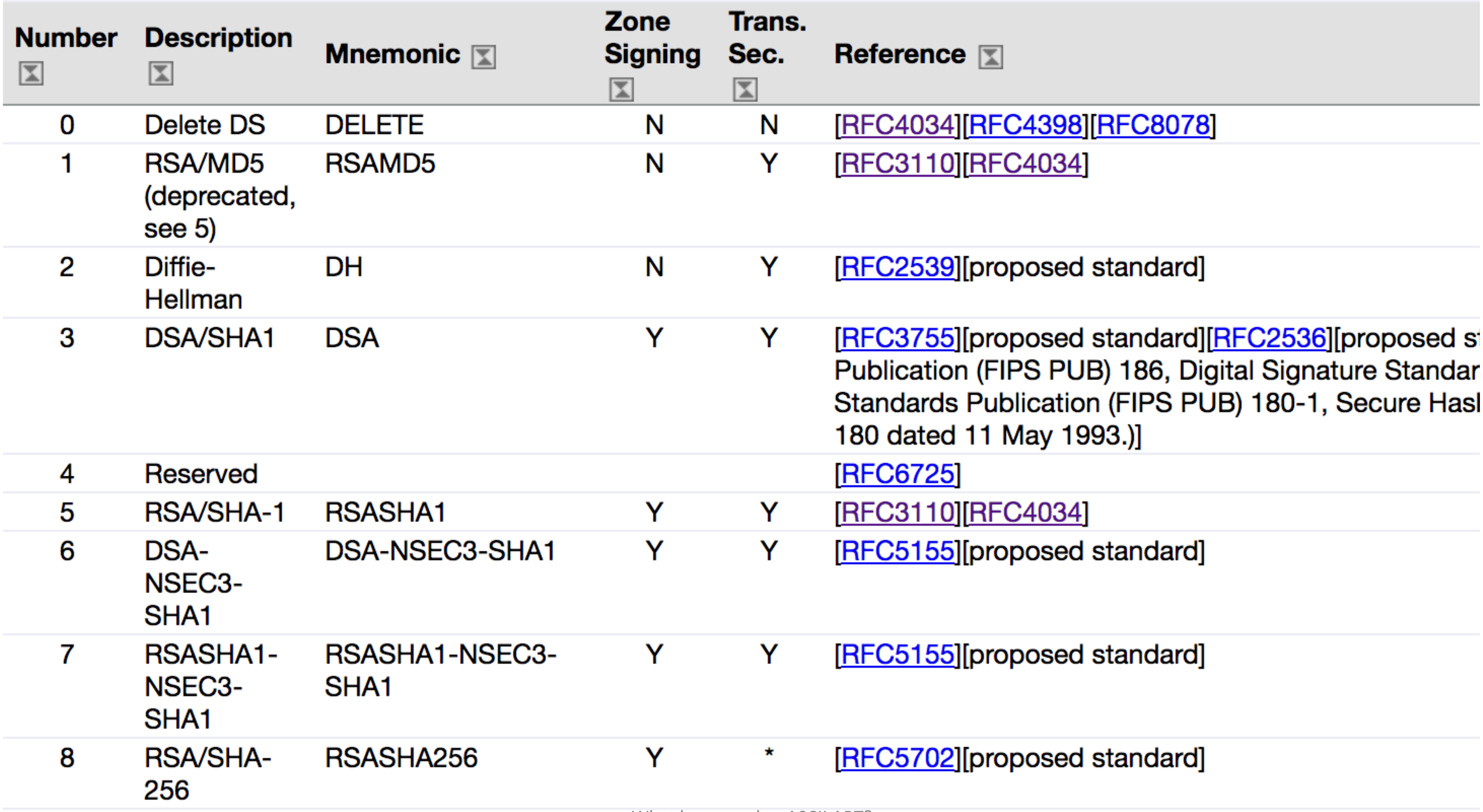
Must Implement	Must Not Implement	Recommended to Implement	Optional
RSASHA1	RSAMD5	RSASHA256 RSASHA1-NSEC3-SHA1 RSASHA512 ECDSAP256SHA256 ECDSAP384SHA384	Any registered algorithm not listed in this table

ASCII ART FTW

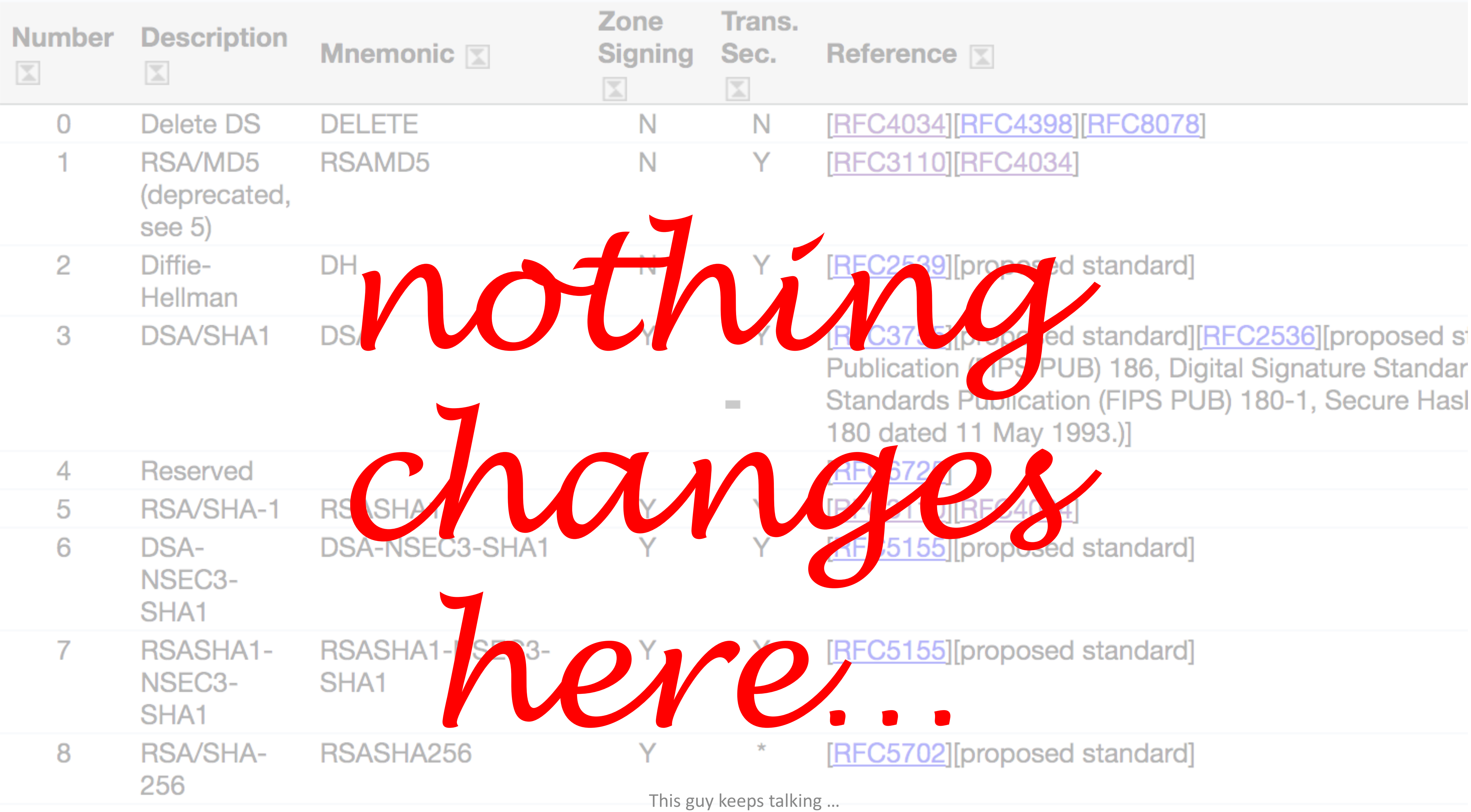
RFC6944

Must Implement	Must Not Implement	Recommended to Implement	Optional
RSASHA256	RSAMD5	RSASHA1 RSASHA1-NSEC3-SHA1 RSASHA512 ECDSAP256SHA256 ECDSAP384SHA384	Any registered algorithm not listed in this table

See what I did here?



Number ☒	Description ☒	Mnemonic ☒	Zone Signing ☒	Trans. Sec. ☒	Reference ☒
0	Delete DS	DELETE	N	N	[RFC4034][RFC4398][RFC8078]
1	RSA/MD5 (deprecated, see 5)	RSAMD5	N	Y	[RFC3110][RFC4034]
2	Diffie-Hellman	DH	N	Y	[RFC2539][proposed standard]
3	DSA/SHA1	DSA	Y	Y	[RFC3755][proposed standard][RFC2536][proposed st Publication (FIPS PUB) 186, Digital Signature Standar Standards Publication (FIPS PUB) 180-1, Secure Hasl 180 dated 11 May 1993.)]
4	Reserved				[RFC6725]
5	RSA/SHA-1	RSASHA1	Y	Y	[RFC3110][RFC4034]
6	DSA-NSEC3-SHA1	DSA-NSEC3-SHA1	Y	Y	[RFC5155][proposed standard]
7	RSASHA1-NSEC3-SHA1	RSASHA1-NSEC3-SHA1	Y	Y	[RFC5155][proposed standard]
8	RSA/SHA-256	RSASHA256	Y	*	[RFC5702][proposed standard]



Number	Description	Mnemonic	Zone Signing	Trans. Sec.	Reference
0	Delete DS	DELETE	N	N	[RFC4034][RFC4398][RFC8078]
1	RSA/MD5 (deprecated, see 5)	RSAMD5	N	Y	[RFC3110][RFC4034]
2	Diffie-Hellman	DH	N	Y	[RFC2539][proposed standard]
3	DSA/SHA1	DSA	Y	Y	[RFC3755][proposed standard][RFC2536][proposed st Publication (FIPS PUB) 186, Digital Signature Standar Standards Publication (FIPS PUB) 180-1, Secure Hasl 180 dated 11 May 1993.)]
4	Reserved				[RFC6725]
5	RSA/SHA-1	RSASHA1	Y	Y	[RFC3110][RFC4034]
6	DSA-NSEC3-SHA1	DSA-NSEC3-SHA1	Y	Y	[RFC5155][proposed standard]
7	RSASHA1-NSEC3-SHA1	RSASHA1-NSEC3-SHA1	Y	Y	[RFC5155][proposed standard]
8	RSA/SHA-256	RSASHA256	Y	*	[RFC5702][proposed standard]

nothing changes here…

This guy keeps talking …

Then why bother?

- A new “mandatory” algorithm allows implementations to shift its DEFAULT algorithm. It paves the way to make SHA1 less utilised.

So it can go the way of RSAMD5

- Any other advice, discussions on algorithm use lifetimes, algorithm choice, algorithm superiority, guidelines on what validators, signers etc., should (-/+) or must (-) do, belongs in a Best Current Practice.

utilised or utilized? (British Spelling wins)

Request to the working group

- Call for adoption of draft-arends-dnsop-algorithm-update
  - Proposed Standard track
  - Updates applicability statement with a minimal change.

- Consider draft-wouters-sury-dnsop-algorithm-update as BCP
  - The WG has already adopted this document.
  - Please consider it for the category: Best Current Practise
  - As it contains guidelines for implementors and deployment discussions

- NOTE: These are complementary, not mutual exclusive.