draft-wouters-sury-dnsop-algorithm-update-02

- Updates Mandatory-To-Implement (“MTI”) algorithms for
  - DNSKEY
  - CDS / DS
- Different MTI for Resolvers (consumers) and Signers (producers)
- Demote and promote algorithms gradually and realistically
- Uses RFC-2119 language with modifiers based on RFC-7321, RFC-7321bis, RFC-4306bis:
    - SHOULD+, SHOULD-, MUST-

draft-wouters-sury-dnsop-algorithm-update-02

DNSKEY algorithm table

Number	Mnemonics	DNSSEC Signing	DNSSEC Validation
1	RSAMD5	MUST NOT	MUST NOT
3	DSA	MUST NOT	MUST NOT
5	RSASHA1	MUST-	MUST-
6	DSA-NSEC3-SHA1	MUST NOT	MUST NOT
7	RSASHA1-NSEC3-SHA1	MUST-	MUST-
8	RSASHA256	MUST	MUST
10	RSASHA512	SHOULD-	MUST
12	ECC-GOST	SHOULD NOT	SHOULD-
13	ECDSAP256SHA256	SHOULD-	MUST-
14	ECDSAP384SHA384	SHOULD NOT	SHOULD-
TBD	ED25519	SHOULD+	SHOULD+
TBD	ED448	SHOULD+	SHOULD+

draft-wouters-sury-dnsop-algorithm-update-02

DS and CDS algorithm table

Number	Mnemonics	DNSSEC Delegation	DNSSEC Validation
0	NULL (CDS only)	MUST NOT [*]	MUST NOT [*]
1	SHA-1	SHOULD NOT	MUST-
2	SHA-256	MUST	MUST
3	GOST R 34.11-94	MAY	SHOULD
4	SHA-384	MAY	SHOULD+

draft-wouters-sury-dnsop-algorithm-update-02

open items

- Some people don't like the RFC-2119 modifiers
- Should there be a "default" directive in addition to the Mandatory-to-implement directive? Or should that go into a separate BCP document?
- IANA and Security Considerations need some work
- Disagreement about MTI level for SHA1
- Only one document should obsolete RFC-6944