draft-ietf-dnsop-algorithm-update

Ondřej Surý & Paul Wouters
IETF 102, Montreal

Goals

- Refresh the list of DNSKEY Algorithms
  - Add more as mandatory
  - Remove the old insecure ones
- Refresh the list of DS/CDS Algorithms

DNSKEY Algoritms

Mnemonics	DNSSEC Signing	DNSSEC Validation
RSAMD5	MUST NOT	MUST NOT
DSA	MUST NOT	MUST NOT
RSASHA1	NOT RECOMMENDED	MUST
DSA-NSEC3-SHA1	MUST NOT	MUST NOT
RSASHA1-NSEC3-SHA1	NOT RECOMMENDED	MUST
RSASHA256	MUST	MUST
RSASHA512	NOT RECOMMENDED	MUST
ECC-GOST	MUST NOT	MAY
ECDSAP256SHA256	MUST	MUST
ECDSAP384SHA384	MAY	RECOMMENDED
ED25519	RECOMMENDED	RECOMMENDED
ED448	MAY	RECOMMENDED

DS/CDS Algorithms

Mnemonics	DNSSEC Signing	DNSSEC Validation
NULL (CDS Only)	N/A	N/A
SHA-1	MUST NOT	MUST
SHA-256	MUST	MUST
GOST R 34.11-94	MUST NOT	MAY
SHA-384	MAY	MUST

ECDSAP256SHA256

DNSKEY Algorithm Recommendation

Document status

- Authors have addressed all comments from the WG
- Authors believe that the document is ready for WG LC