DNSSEC Algorithm Update

Ondřej Surý, CZ.NIC; Paul Wouters, Red Hat

Updating Algorithm Requirements Levels

- MUST NOT, SHOULD NOT, MUST, SHOULD, …
  - RFC-2119 meaning
- MUST-
  - Mandatory now
  - It’s probably going to be SHOULD* in the near future
- SHOULD-
  - It’s probably going to be MAY or MUST NOT in the near future
- SHOULD+
  - It’s probably going to be MUST in the near future

DNSKEY Algorithms

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+

DS and CDS Algorithms

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+