DNSSEC Encryption Algorithm Agility

ICANN 56 DNSSEC Workshop
June 27, 2016
Helsinki, Finland

Dan York, Internet Society

DNSSEC Algorithms

- **Used to generate keys for *signing***
  - DNSKEY
- **Used in DNSSEC signatures**
  - RRSIG
- **Used for DS record for chain of trust**
  - DS
- **Used in *validation* of DNSSEC records**

IANA Registry of DNSSEC Algorithm Numbers

- http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml

Number	Description	Mnemonic
0	Reserved	
1	RSA/MD5 (deprecated)	RSAMD5
2	Diffie-Hellman	DH
3	DSA/SHA1	DSA
4	Reserved	
5	RSA/SHA-1	RSASHA1
6	DSA-NSEC3-SHA1	DSA-NSEC3-SHA1
7	RSASHA1-NSEC3-SHA1	RSASHA1-NSEC3-SHA1
8	RSA/SHA-256	RSASHA256
9	Reserved	
10	RSA/SHA-512	RSASHA512
11	Reserved	
12	GOST R 34.10-2001	ECC-GOST
13	ECDSA Curve P-256 wSHA-256	ECDSAP256SHA256
14	ECDSA Curve P-384 wSHA-384	ECDSAP384SHA384
15-122	Unassigned	
123-251	Reserved	
252	Reserved for Indirect Keys	INDIRECT
253	private algorithm	PRIVATEDNS
254	private algorithm OID	PRIVATEOID
255	Reserved	

Elliptic Curve DNSSEC Algorithms

- **ECDSA – RFC 6605 – April 2012**

Under development:

- **Ed25519:**
  - draft-ietf-curdle-dnskey-ed25519
- **Ed448**
  - draft-sury-dnskey-ed448

(See “New Curves in DNSSEC” from ICANN 55)

Why Do We Care About Newer Algorithms?

- **Faster!**
  - Signing
  - Validation
- **Smaller keys and signatures**
  - Packet size (and avoiding fragmentation)
  - Minimizing potential reflection/DDoS attacks
- **Better cryptography**
  - Move away from 1024-bit RSA

Aspects of Deploying New Algorithms

- Validation
- Signing / DNS Hosting Operators
- Registries
- Registrars
- Developers

(See ICANN 55 Marrakech DNSSEC Workshop archives for more information.)

Discussions To Date

- Mar 2016 - ICANN 55 DNSSEC Workshop, Marrakech
- Apr 2016 – DNS-OARC Workshop, Buenos Aires
- Apr 2016 – IETF 95, Buenos Aires – Discussion in CURDLE and DNSOP working groups
- May 2016 – RIPE 72 session, Copenhagen
- Jun 2016 – ICANN 56 DNSSEC Workshop, Helsinki

- Internet-Draft
  - draft-york-dnsop-deploying-dnssec-crypto-algs

What Have We Learned?

- A conversation with Ondřej Surý

Next Steps

- Help people understand value and need to support new algorithms

- Document these steps in a form that can be distributed (ex. Internet-draft)

- ?

- Need to start NOW as it will take several years to deploy...

Dan York

Senior Content Strategist
Internet Society

york@isoc.org

Thank You!