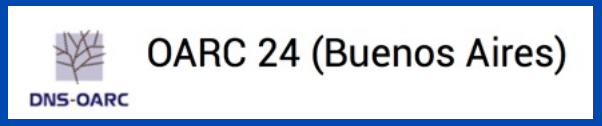
DNSSEC Algorithm Flexibility

DNS-OARC 24
April 1, 2016
Buenos Aires, Argentina



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	

“Newer” DNSSEC Algorithms

- **ECDSA – RFC 6605 – April 2012**
- **GOST – RFC 5933 – July 2010**

- **Future:**
  - Edwards-curve Digital Security Algorithm (EdDSA) with **Ed25519**
    - https://datatracker.ietf.org/doc/draft-ietf-curdle-dnskey-ed25519/
  - Edwards-curve Digital Security Algorithm (EdDSA) with **Ed448**
    - https://datatracker.ietf.org/doc/draft-ietf-curdle-dnskey-ed448/

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**
  - Moving away from 1024-bit RSA

Aspects of Deploying New Algorithms

- **Validation**
  - Need to be updated to use new algorithm
- **Signing Software**
  - Software needs to be updated – and then distributed/deployed
- **DNS Hosting Operators**
  - Need to offer new algorithm to customers
- **Registries**
  - Need to accept DS records with new algorithm
- **Registrars**
  - Need to allow customers to choose new algorithm in web interfaces
- **Developers**
  - Need to modify software to allow new algorithms

More Info

- **New Internet Draft:**
  - **draft-york-dnsop-deploying-dnssec-crypto-algs**
  - https://datatracker.ietf.org/doc/draft-york-dnsop-deploying-dnssec-crypto-algs/
- **Article about ECC and IETF 55 Workshop:**
  - **http://bit.ly/dnssececc**

Internet Society™

OARC 24 Panel: DNSSEC Algorithm Flexibility

- **Ondřej Surý,** representing Debian
- **Paul Wouters,** Red Hat
- **Evan Hunt,** ISC / BIND
- **Benno Overeinder,** NLNet Labs / Unbound
- **Jan Včelák,** CZ.NIC / Knot
- **Ralf Weber,** Nominum

- **Dan York,** Internet Society, *moderator*

Dan York

Senior Content Strategist
Internet Society

york@isoc.org

Thank You!