Challenges To Deploying New DNSSEC Algorithms

ICANN 55 DNSSEC Workshop
March 8, 2016
Marrakech, Morocco

Dan York, Internet Society

ICANN|55
MARRAKECH
5 – 10 MARCH 2016

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:**
  - Ed25519?
    - https://gitlab.labs.nic.cz/labs/ietf/blob/master/draft-sury-dnskey-ed25519.xml
  - ChaCha? (RFC 7539)

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

Validation

- **Resolvers performing validation need to be updated to accept and use the new algorithm.**
- **Software needs to be updated**
  - Can be an issue of getting the underlying libraries updated
- **Updates need to be deployed**
  - Customer-premises equipment (CPE)
- **Problem – RFC 4035, section 5.2:**

"*If the resolver **does not support any of the algorithms** listed in an authenticated DS RRset, then the resolver will not be able to verify the authentication path to the child zone. In this case**, the resolver SHOULD treat the child zone as if it were unsigned**.*"

Signing

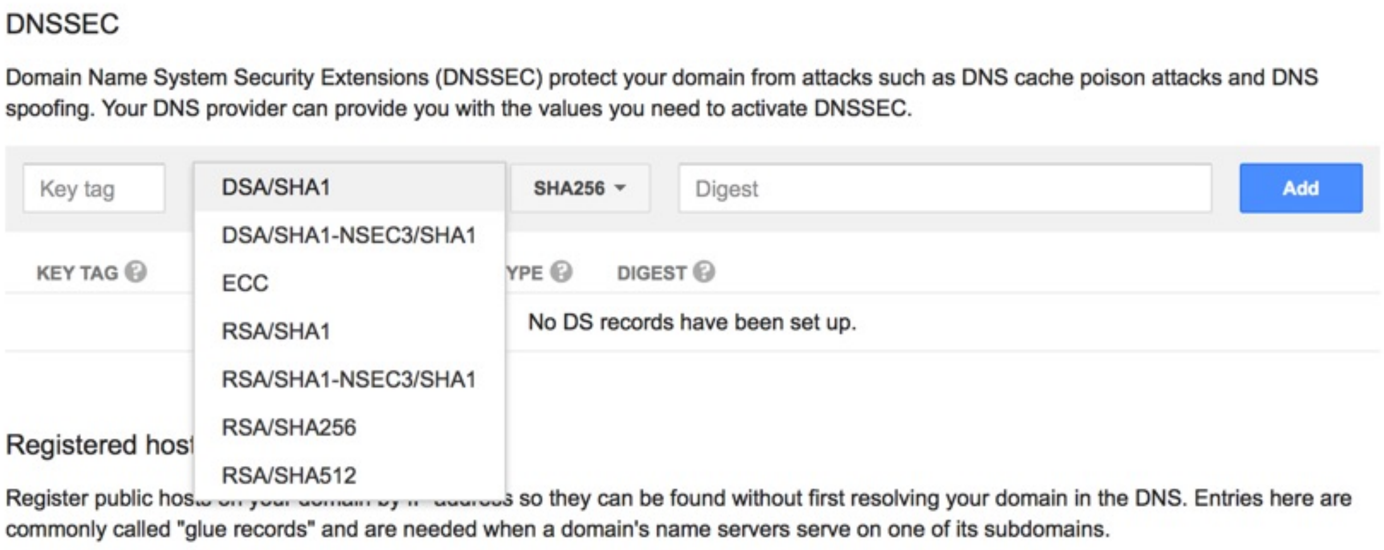
- Software for authoritative DNS servers need updates
- Updated software needs to be deployed to signing servers
- DNS Hosting Operators (which could be Registrars) need to offer new algorithm to customers
- New key with new algorithm needs to co-exist with existing key for some period of time
  - Size impact

Registries

- **Some registries are only accepting DS records with certain algorithms**
  - Not accepting new algorithms
- **No way to know what algorithms registries accept**
  - Update EPP feed to indicate what algorithms are accepted?
- **Question: Why do registries need to check algorithm type?**

Registrars

- **When adding DS records, some registrars only accept certain algorithms in web interface**
- **Example – BEFORE someone asked for ECDSA:**



DNSSEC

Domain Name System Security Extensions (DNSSEC) protect your domain from attacks such as DNS cache poison attacks and DNS spoofing. Your DNS provider can provide you with the values you need to activate DNSSEC.

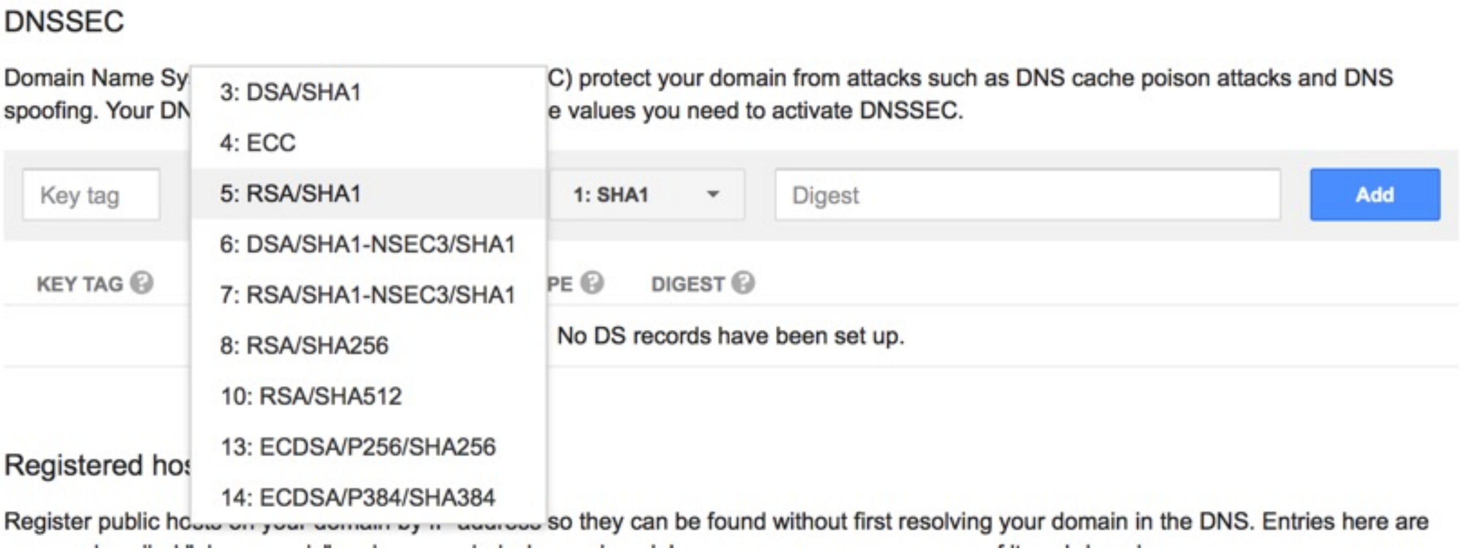
No DS records have been set up.

Registered hos

Register public hos so they can be found without first resolving your domain in the DNS. Entries here are commonly called "glue records" and are needed when a domain's name servers serve on one of its subdomains.

Registrars

- **Good news! – AFTER someone asked for ECDSA:**



DNSSEC

Domain Name Sy C) protect your domain from attacks such as DNS cache poison attacks and DNS spoofing. Your DN e values you need to activate DNSSEC.

Key tag | 1: SHA1 | Digest | Add

3: DSA/SHA1
4: ECC
5: RSA/SHA1
6: DSA/SHA1-NSEC3/SHA1
7: RSA/SHA1-NSEC3/SHA1
8: RSA/SHA256
10: RSA/SHA512
13: ECDSA/P256/SHA256
14: ECDSA/P384/SHA384

KEY TAG | PE | DIGEST

No DS records have been set up.

Registered hos

Register public ho so they can be found without first resolving your domain in the DNS. Entries here are

- **But this requires someone asking registrars to support new algorithms... and the registrars making the appropriate updates.**

Registrars

- **Question: why do registrars *need* to check the algorithm type?**
- **What is the harm in advertising an “unknown” algorithm type?**

- **Answer: Stop restricting and just accept all DS records.**
    - Does this come down to a user interface issue?

Developers

- **Give developers a list, they will check it!**
- **Sooo... IANA DNSSEC algorithm list:**
- http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml
- **But... in this case bounds-checking is not necessary (if we accept idea that registrars/registries should accept all algorithms).**
- **Need to modify software to allow all algorithms (or simply not check algorithm type).**

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)**
- **Identify and act on actions. Examples:**
  - Understand implications of registrars/registries simply NOT doing any checking on algorithm types.
  - Survey registries to find out which restrict algorithms in DS records
    - Explore idea of communicating accepted algorithms in EPP
  - Encourage registrars to accept wider range of algorithms (or to stop checking)
  - Encourage developers to accept all IANA-listed algorithms (or to stop checking)

Dan York

Senior Content Strategist
Internet Society

york@isoc.org

Thank You!