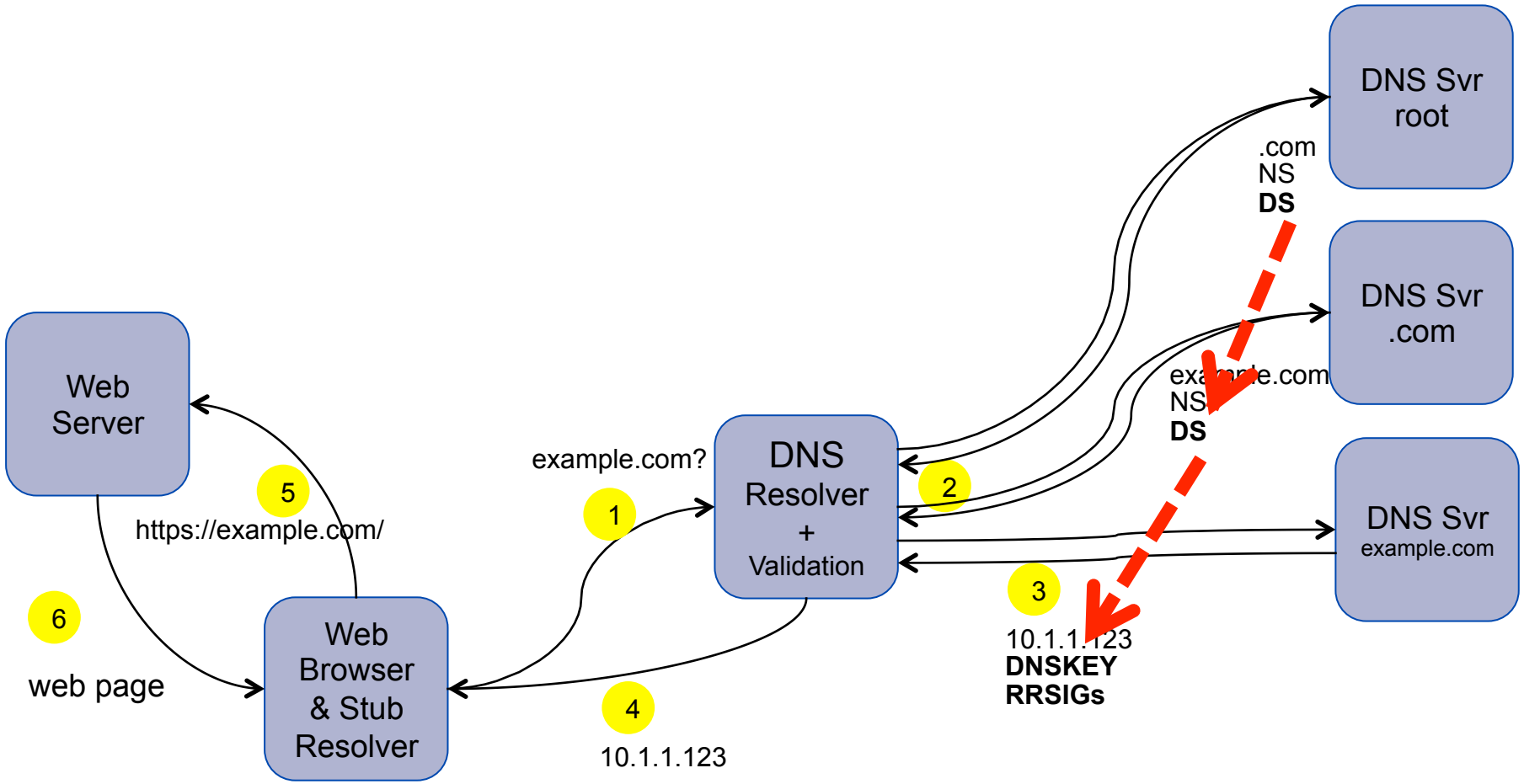
Deploying New DNSSEC Algorithms

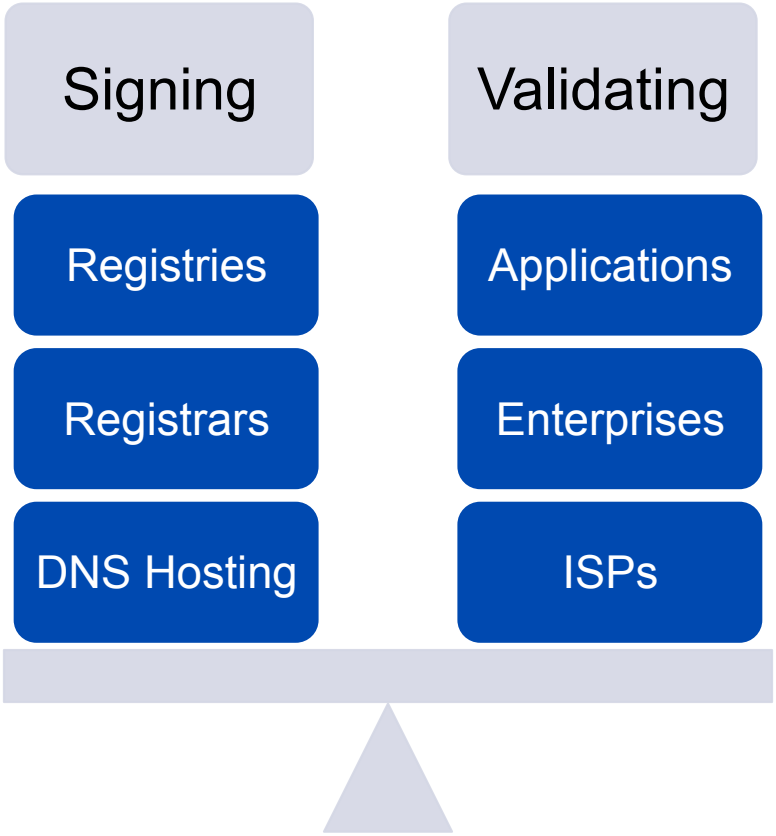
IEPG at IETF 93
19 July 2015
Prague, Czech Republic

Dan York, Internet Society

A Reminder of How DNSSEC Works



The Two Parts of DNSSEC



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**
  - DNS resolvers

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	

BUT... DNSSEC is an RSA world... (part 1)

- **Ed Lewis (ICANN) presenting at CENTR, June 2015**
- **Breakdown of DNSSEC names**

⊙682 thousand DS-owning names
⊙ 11 thousand RSA-SHA-1
⊙562 thousand RSA-SHA-1-NSEC3
⊙146 thousand RSA-SHA-256

⊙453 RSA-SHA-512
⊙ 16 GOST
⊙ 38 ECC-256T
⊙ 14 ECC-384T
⊙ 6 DSA-SHA-1

- https://centr.org/system/files/agenda/attachment/rd7-lewis-dnssec_cryptographic_demographics-20150603.pdf

BUT... DNSSEC is an RSA world... (part 2)

- **Ed Lewis (ICANN) presenting at CENTR, June 2015**
- **Top algorithms (raw keys, not names)**

```
1 million RSA-SHA1-N@1024
208 thousand RSA-SHA256@1024
154 thousand RSA-SHA1-N@2048
152 thousand RSA-SHA256@2048
 10 thousand RSA-SHA1@1024
 10 thousand RSA-SHA1@2048
1497 RSA-SHA1-N@4096
1124 RSA-SHA256@1280
 761 RSA-SHA256@4096
...
...
...
```

```
 80 EC-SHA256T@512
 36 EC-SHA384T@768
 33 ECC-GOST@512
  7 DSA-SHA1@3168
  2 DSA-SHA1@3166
  2 DSA-SHA1@2432
  1 DSA-SHA1@3167
```

Non-RSA algorithms

- https://centr.org/system/files/agenda/attachment/rd7-lewis-dnssec_cryptographic_demographics-20150603.pdf

“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)
  - Others coming out of CFRG?

Why Do We Care About Newer Algorithms?

- **Smaller keys and signatures**
  - Packet size (and avoiding fragmentation)
  - Minimizing potential reflection/DDoS attacks
  - Enable large-scale deployment
    - Ex. CDNs
- **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**.*"

Validation - measurement

- **Geoff Huston at IEPG at IETF 92 (March 2015):**
  - http://blog.apnic.net/2015/03/23/ietf92-geoff-presents-on-ec-dsa-at-iepg/
  - 1 in 5 validating resolvers would *not* support ECDSA

- **Pier Carlo Chiodi using RIPE Atlas probes (Jan 2015):**
  - http://blog.pierky.com/dnssec-ecdsa-aware-resolvers-seen-by-ripe-atlas/
  - "*512 probes received an authenticated response for RSA-signed zone, 63 of those (12,3 %) missed the AD flag for the ECDSA-signed one.*"

Signing

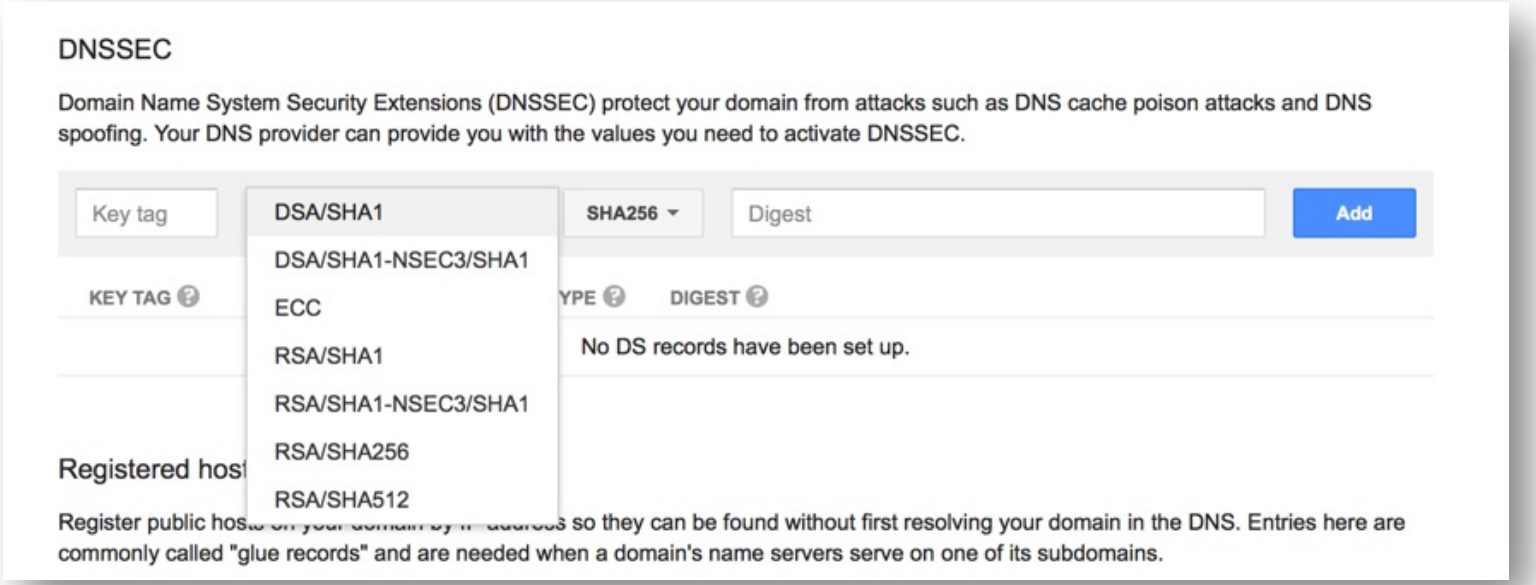
- **Software for authoritative DNS servers need updates**
- **Updated software needs to be deployed to signing servers**
- **DNS Hosting Operators (which could be Registrars) need to offer new algorithm to customers**
- **New key with new algorithm needs to co-exist with existing key for some period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

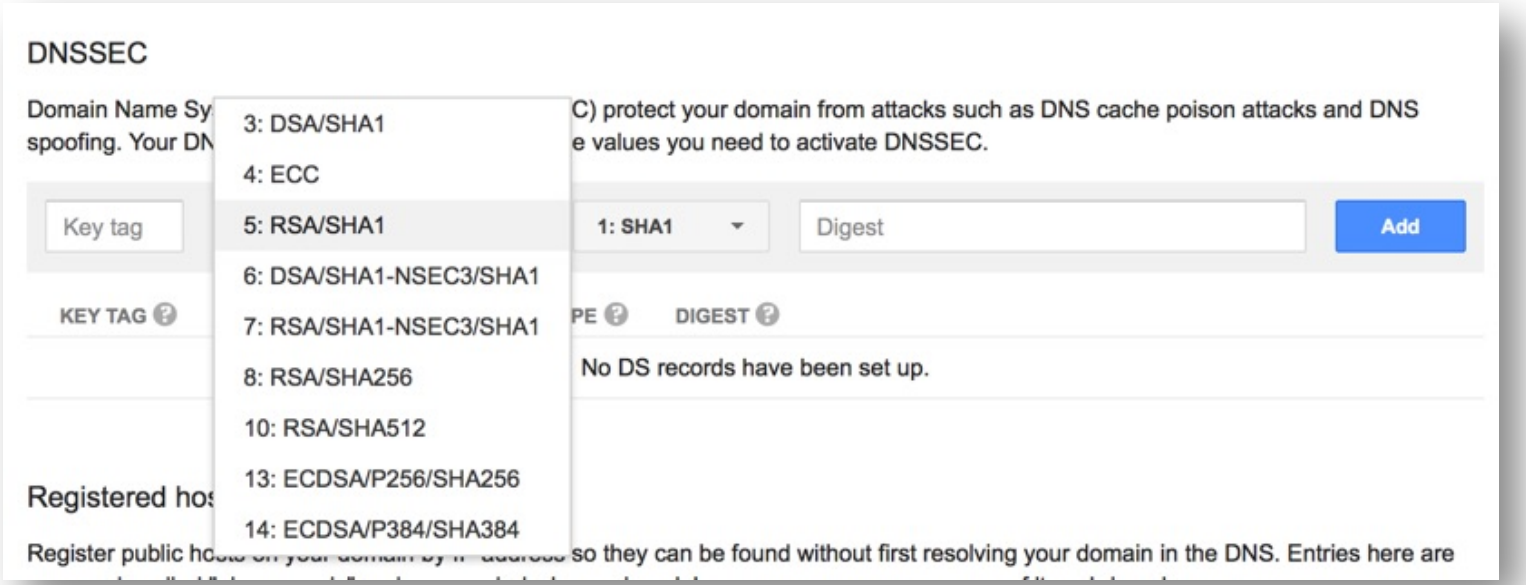
Registrars

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



Registrars

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



- **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?**
  - Is this attempting to protect users from themselves? Minimize support calls?
- **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
  - or check IANA registry on some periodic interval

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)

Draft IAB Statement on Crypto Algorithm Agility

- **https://tools.ietf.org/html/draft-iab-crypto-alg-agility**

Many IETF protocols use cryptographic algorithms to provide confidentiality, integrity, authentication or digital signature. Communicating peers must support a common set of cryptographic algorithms for these mechanisms to work properly. This memo provides guidelines to ensure that protocols have the ability to migrate from one mandatory-to-implement algorithm suite to another over time.

Dan York

Senior Content Strategist
Internet Society

york@isoc.org

Thank You!