“SHA-1 y la rotación de algoritmo en DNSSEC”

Carlos Martínez, LACNIC
Hugo Salgado, .CL

Foro Técnico LACNIC 33, Webinar.

nic chile
SOMOS EL PUNTO CL

lacnic 33
online meeting

lacnic

DNSSEC y los algoritmos

- DNSSEC es criptografía asimétrica para el DNS
- Se necesitan llaves
  - RSA
  - DSA
  - GOST
  - ECDSA
- Se necesitan firmas
  - MD5
  - SHA1, SHA256, SHA384, SHA512

¿Por qué es necesario rotar? (rollover)

- Los algoritmos pueden sufrir ataques
  - fuerza bruta
  - replay
  - pre-computation
- Debe refirmarse y cambiar llaves
  - Técnica KSK-ZSK
- También cambiar algoritmo cuando se vuelva criptográficamente inseguro.

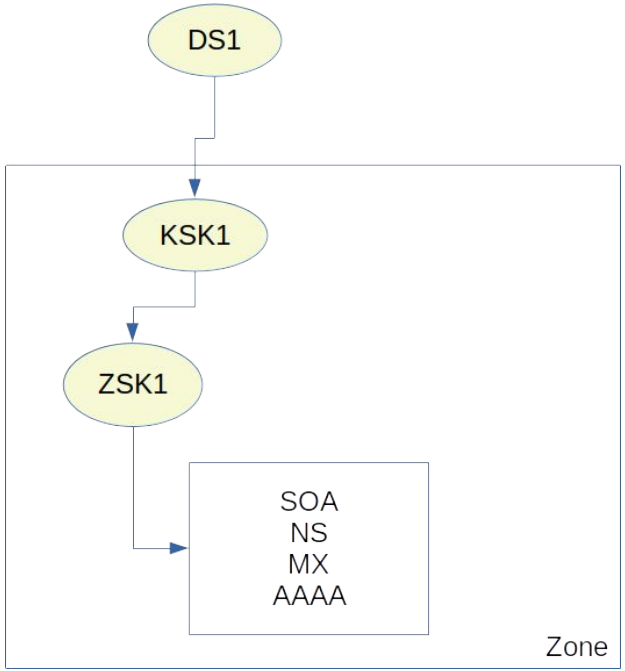
SHA-1 End-of-Life

- MD-5 ya estaba muerto y sin uso
- SHA-1 aproximándose a morir:
  - ataque de pre-computación
  - nuevo de enero 2020
- Cambio de status de implementación
- Dar de baja en software firmador
- Escribir recomendaciones

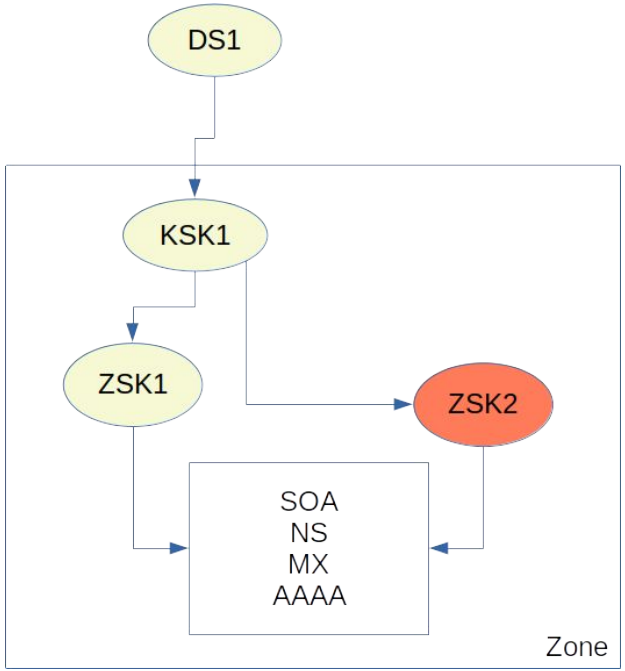
¿Cómo hacer una rotación de algoritmo?

- Paso a paso (modo hacker)
- Comandos de firma y timeline
- Verificación
  - dig
  - dnsviz
  - zonemaster, dnssec-debugger, etc
- Más información: https://hugo.salga.do/post/61550193327864217 6/c%C3%B3mo-hacer-un-rollover-de-algoritmo-en-dnssec

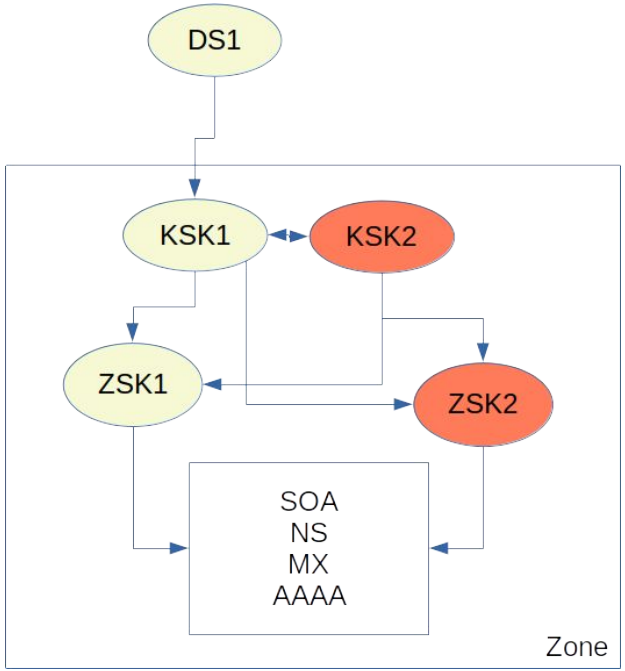
¿Cómo hacer una rotación de algoritmo? - paso 1



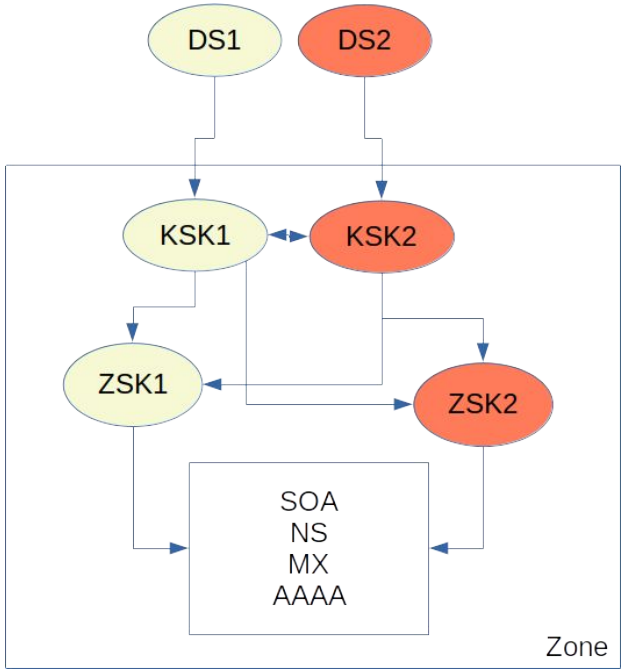
¿Cómo hacer una rotación de algoritmo? - paso 2



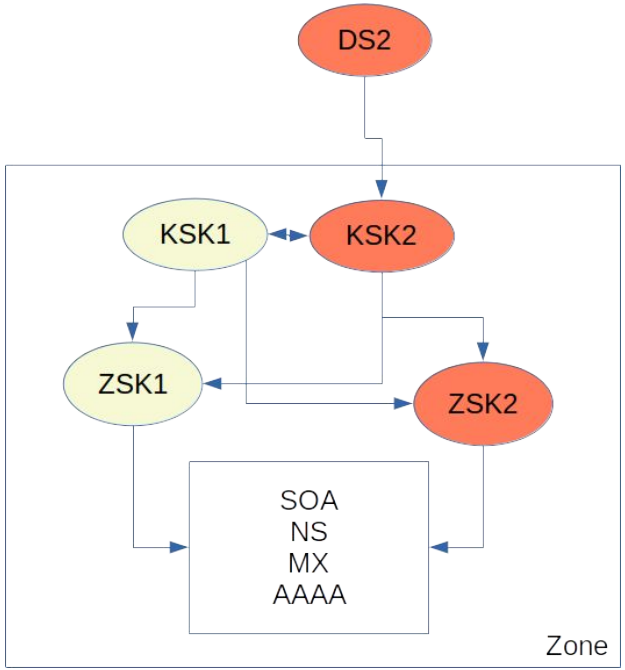
¿Cómo hacer una rotación de algoritmo? - paso 3



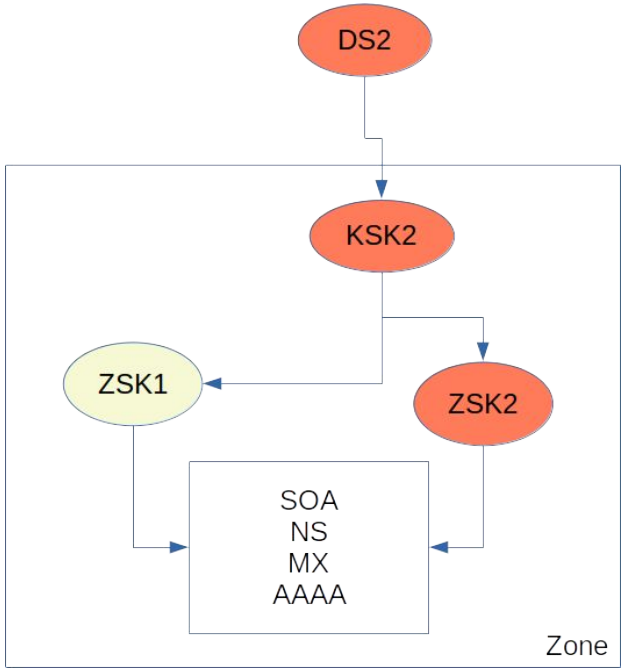
¿Cómo hacer una rotación de algoritmo? - paso 4



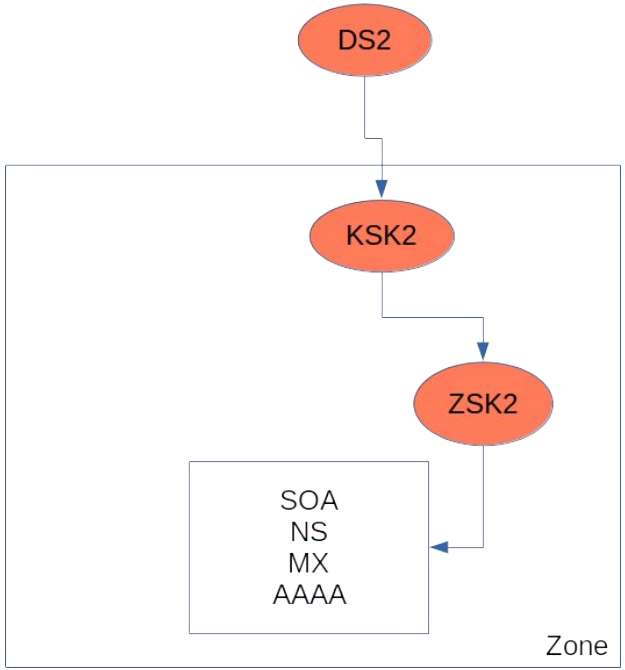
¿Cómo hacer una rotación de algoritmo? - paso 5



¿Cómo hacer una rotación de algoritmo? - paso 6



¿Cómo hacer una rotación de algoritmo? - paso 7



… con OpenDNSSEC?

- Change the <Algorithm> field in the KASP (make sure to do this for both KSK and ZSK)

- Run policy import:
  - ods-enforcer policy import
  - ods-enforcer enforce

Source: https://wiki.opendnssec.org/pages/viewpage.action?pageId=10125376#HowdoI...?-Changethesigningalgorithm

… con Bind?

- Generate new keys
  - dnssec-keygen -L 24h -a 13 -f ksk <dominio>
  - dnssec-keygen -L 24h -a 13 <dominio>
- Then get named to reload the keys:
  - rndc loadkeys botolph.cam.ac.uk
- Update parent with new DS record
- Decommission old algorithm
  - dnssec-settime -D now -I now <KEY>

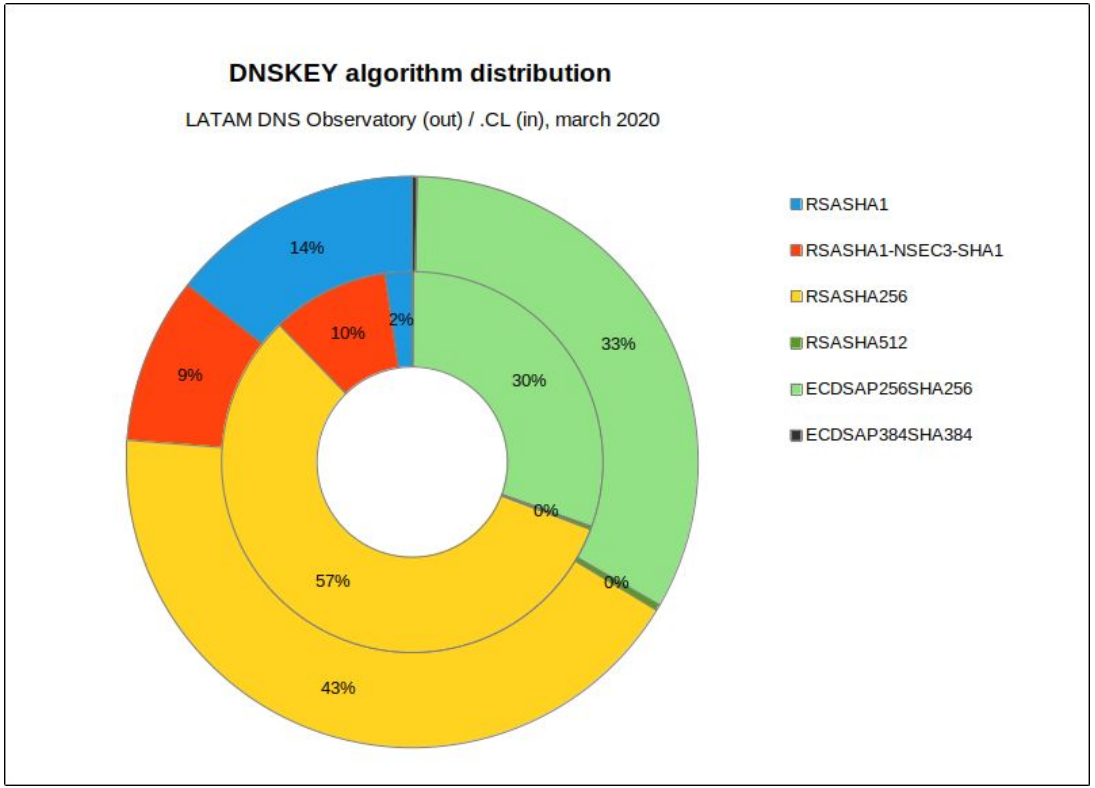
Source: https://www.dns.cam.ac.uk/news/2020-01-15-rollover.html

… con Knot?

- Change “algorithm” in “policy” section
- Reload server

Source:
https://www.knot-dns.cz/docs/2.7/html/operation.html#dnssec-key-rollovers

Algorithms in-the-wild



Llamado a acción

- Verifique su algoritmo y planee su cambio si es SHA-1
  - $ dig <dominio> dnskey +short
    256 3 8 AwEAAb+TgVyeaGob…
    257 3 8 AwEAAfEG/xIgexdUN...

- Aún hay tiempo para planificar, pero no sabemos hasta cuándo.
- Si no lo hacemos a tiempo, los validadores pueden decidir dejar de dar soporte.

¡Gracias!

Carlos Martínez, carlos@lacnic.net
Hugo Salgado, hsalgado@nic.cl

Grupo DNS de LACNOG
https://www.lacnog.org/wg-dns/

nic chile
SOMOS EL PUNTO CL

lacnic

lacnic 33
online meeting