



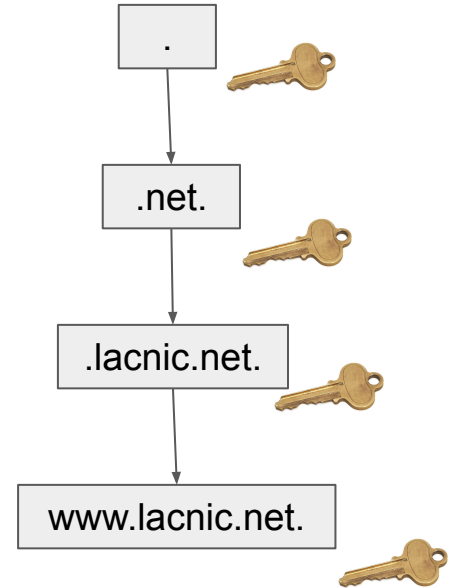
# La rotación 2026 de la llave de la raíz del DNS

Hugo Salgado - LACNOG  
Foro Técnico de LACNIC 23  
Sao Paulo - mayo 2025

**lacnic43**  
5-9 de Mayo 2025 / São Paulo, Brasil

# ¿Qué es la llave KSK de la raíz?

- Cómo funciona DNSSEC
- Por qué es importante la llave de la raíz
- La cadena de confianza
  - para obtener la llave de un dominio, debo preguntarle al padre
  - la raíz es el padre último



# ¿Por qué hay que rotar la KSK?

- Razones para cambiarla
  - criptográficas
  - operativas
- Existe un mecanismo automático dentro del protocolo
  - RFC 5011
- Es parte de la configuración inicial en servidores

# ¿Cómo se firma la raíz?

- Ceremonias IANA
  - Dos sedes en costas opuestas de USA
  - Con medidas de seguridad y control
  - Dentro de cajas fuertes
  - En dispositivos HSM, se activa con llaves de los CO (3 de 7)

# ¿Cómo se firma la raíz?

- Ceremonias IANA
  - Dos sedes en costas opues
  - Con medidas de seguridad
  - Dentro de cajas fuertes
  - En dispositivos HSM, se act



HSM First slot: HSM9E\_KSK-2024

HSM ManufacturerID:

HSM Model: Luna G7

HSM Serial: 1658876115494

Generate key

Generated key: key\_label=Kmyv6jo alg=RSA bits=2048 exp=65537

Generated key Kmyv6jo has key tag 38696 for algorithm=AlgorithmDNSSEC.RSASHA256, flags=0x101

Generated key Kmyv6jo has key tag 38824 with the REVOKE bit set (flags 0x181)

DS record for generated key:

. IN DS 38696 8 2 683D2D0ACB8C9B712A1948B27F741219298D0A450D612C483AF444A4C0FB2B16

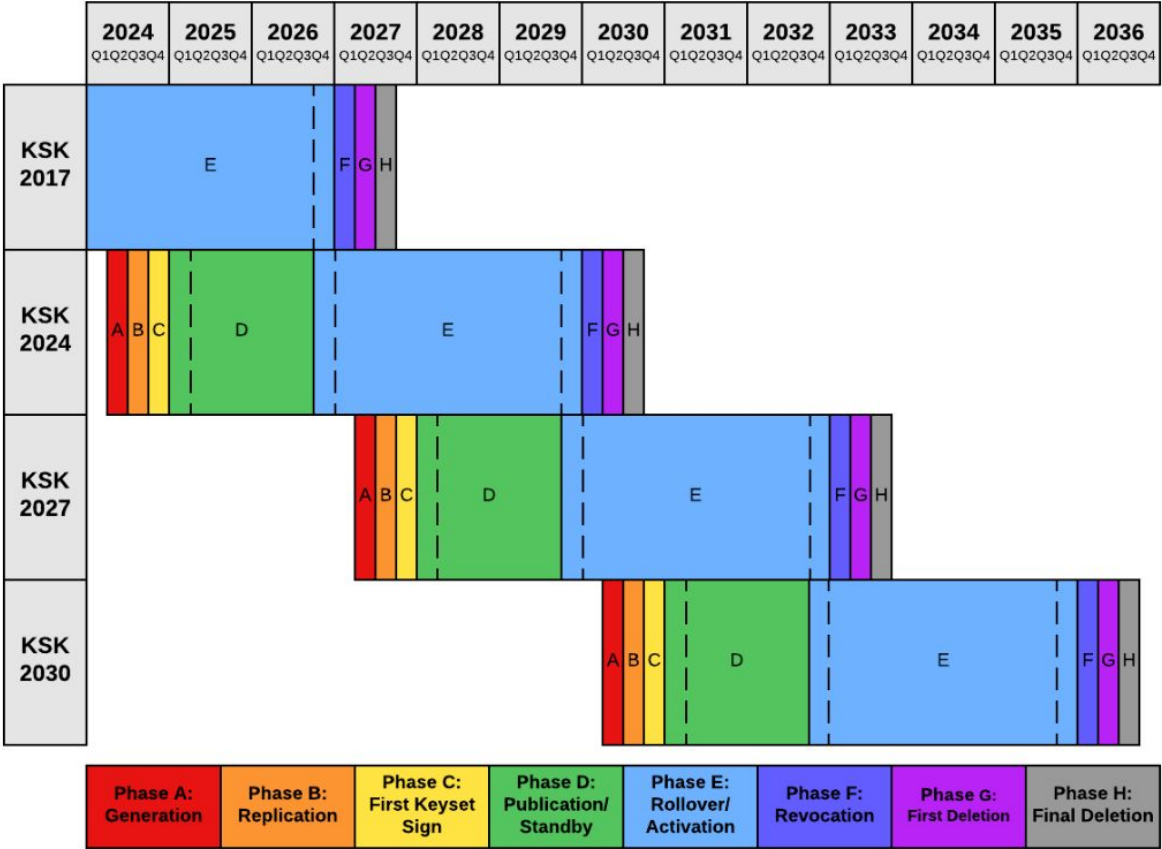
33 freighter crucifix button Apollo spheroid megaton puppy hideaway brickvard bottomless deadbolt pion

# Nueva llave de la raíz: KSK2024

- Tercera llave, segunda rotación (KSK2010, KSK2017)
- Generada el 26 de abril de 2024
  - Key tag 38696
- Actualmente en estado pre-publicación:
  - Es parte del DNSKEY de la raíz, junto a la KSK2017
  - Pero aún no firma. Sigue firmando la actual.
- Siguiente estado: rotación y activación
  - Pasará a ser la única que firme, y la anterior KSK2017 dejará de firmar
  - 11 de octubre 2026

# Nueva llave de la raíz: KSK2024

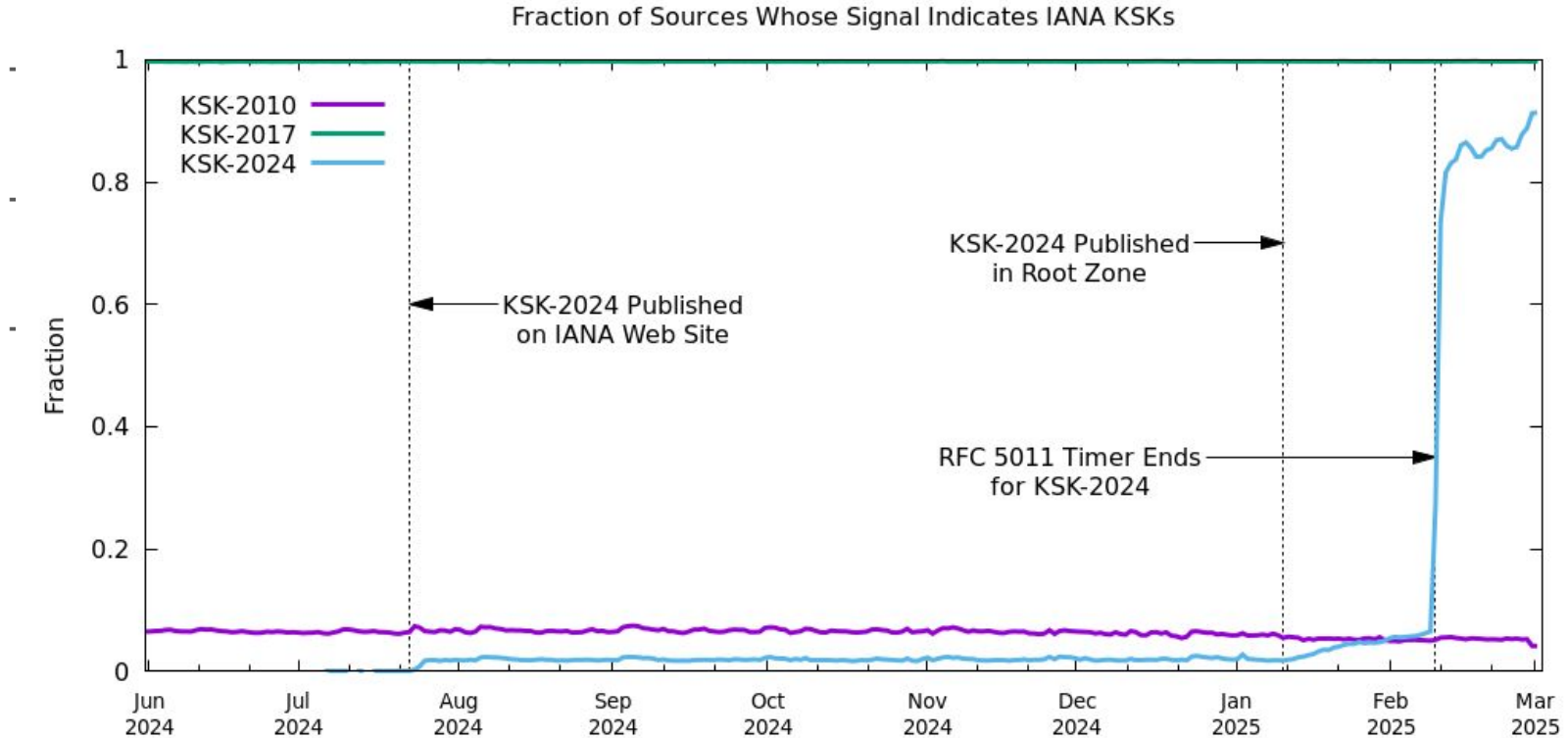
- Terc
- Gen
- 
- Act
- 
- 
- Sign
- 
- 



# ¿Qué podríamos esperar?

- Si usted no la cambia: no le funcionará Internet
- La vez anterior todo fue bien (casi)
  - julio 2010 (primera llave)
    - el riesgo era por introducir nuevos tipos al DNS
    - posibles problemas de parsing, software externo
    - pero nadie validaba!
  - octubre 2018 (primera rotación)
    - no se sabía si estábamos todos preparados
    - software que validaba pero no sabía rotar
    - algunos problemas visibles (ISP de mediano tamaño en Irlanda)

# ¿Qué podríamos esperar?



“The 2024-2026 Root Zone KSK Rollover: initial observations and early trends” - Duane Wessels, Verisign Blog  
<https://blog.verisign.com/security/2024-2026-root-zone-ksk-rollover-initial-observations/>

# ¿Qué puedo hacer ahora?

- Las buenas noticias: el cambio debiera ser automático
  - viene en actualizaciones de software
  - se actualiza automáticamente (RFC5011)
- Asegurarse de tener las últimas versiones de sus software
- Revisar logs de sistemas
- Monitorear
- Estar atento al 11 de octubre de 2026

# ¿Cómo estoy seguro que todo está bien?

- Revisar los trust anchors de mis sistemas
  - Parte de la configuración de paquete
  - Pero actualizado dinámicamente con RFC5011
- Revisar logs de “signaling trust anchors” (RFC8145)
  - `_ta-4f66-9728`.

# Unbound

```
% cat /var/lib/unbound/root.key
```

```
[...]
```

```
.      86400      IN      DNSKEY  257 3 8
```

```
AwEAAaz/tAm8yTn4Mfeh5eyl96WSVexTBAvkMgJzkKTOiW1vklbzxeF3+/4Rg... ;{id = 20326 (ksk),  
size = 2048b} ;;state=2 [ VALID ] ;;count=0 ;;lastchange=1720210748 ;;Fri Jul 5 16:19:08 2024
```

```
.      172800     IN      DNSKEY  257 3 8
```

```
AwEAAa96jeuknZlaeSrvyAJj6ZHv28hhOKkx3rLGXVaC6rXTsDc449/cidltpky... ;{id = 38696 (ksk), size  
= 2048b} ;;state=2 [ VALID ] ;;count=0 ;;lastchange=1739641314 ;;Sat Feb 15 14:41:54 2025
```

```
% sudo journalctl -u unbound -g _ta-
```

```
Feb 17 18:00:00 vulcano unbound[149]: [149:0] info: generate keytag query _ta-4f66-9728. NULL IN
```

# Bind

```
$ cat /var/cache/bind/managed-keys.bind
```

```
[ ... ]
```

```
KEYDATA 20250425033429 20240624224500 19700101000000 257 3 8 (  
    AwEAAaz/tAm8yTn4Mfeh5eyl96WSVexTBAvkMgJzkKTO[...]
```

```
) ; KSK; alg = RSASHA256; key id = 20326
```

```
; next refresh: Fri, 25 Apr 2025 03:34:29 GMT
```

```
; trusted since: Mon, 24 Jun 2024 22:45:00 GMT
```

```
KEYDATA 20250425033429 20250524033429 19700101000000 257 3 8 (  
    AwEAAa96jeuknZlaeSrvyAJj6ZHv28hhOKkx3rLGXVaC[...]
```

```
) ; KSK; alg = RSASHA256; key id = 38696
```

```
; next refresh: Fri, 25 Apr 2025 03:34:29 GMT
```

```
; trust since: Sat, 15 Feb 2025 03:34:29 GMT
```

```
$ sudo journalctl -u named -g _ta-
```

```
Apr 25 20:09:35 vulcano named[59014]: _default: sending trust-anchor-telemetry query '_ta-4f66-9728/NULL'
```

# Knot Resolver

```
$ sudo socat - UNIX-CONNECT:/run/knot-resolver/control/1
```

```
> trust_anchors.summary()
```

```
'          3600 DNSKEY  257 3 8
```

```
AwEAAaz/tAm8yTn4Mfeh5eyl96WSVexTBAvkMgJzkKTOiW1vklbzxeF3+/4RgWOq7HrxRixHIFiExOLAJr5  
emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrj  
yBxWezF0jLHwVN8efS3rCj/EWgvlWgb9tarpVUDK/b58Da+sqqls3eNbuv7p[...]= ; Valid: ; KeyTag:20326
```

```
.          3600 DNSKEY  257 3 8
```

```
AwEAAa96jeuknZlaeSrvyAJj6ZHv28hhOKkx3rLGXVaC6rXTsDc449/cidltpkyGwCJNnOAIFNKF2jBosZBU  
5eeHspaQWomOEIZsjlCMQMC3aeHbGiShvZsx4wMYSjH8e7Vrhbu6irwCzVBAPESjbUdpWWmEnhathW  
u1jo+siFUiRAAxm9qyJNg/wOZqqzL/dL/q8PkcRU5oUKEpU[...]= ; Valid: ; KeyTag:38696
```

```
$ sudo journalctl -u kresd@1.service -g _ta-
```

```
Apr 29 18:32:14 vulcano kresd[209834]: [tassign] signalling query triggered: _ta-4f66-9728.
```

# PowerDNS Recursor

```
$ sudo rec_control get-tas
```

Configured Trust Anchors:

.

```
20326 8 2 e06d44b80b8f1d39a95c0b0d7c65d08458e880409bbc683457104237c7f8ec8d  
38696 8 2 683d2d0acb8c9b712a1948b27f741219298d0a450d612c483af444a4c0fb2b16
```

(conf: allow-trust-anchor-query=yes)

```
$ dig @127.0.0.1 trustanchor.server CH TXT +rec +short
```

```
". 20326 38696"
```

# ÚLTIMO MINUTO: Revise si su resolver está preparado

<https://test.kskroll.vulcano.cl>

Advertencia:

- solo funciona en Bind, NSD y Knot de últimas versiones
- versión Beta, puede tener errores
- no se porta muy bien con los cachés

# ÚLTIMO MINUTO: Revise si su resolver está preparado

[https](https://test.kskroll.vulcano.cl)

Adve

-

-

-



← → ↻ test.kskroll.vulcano.cl ☆ ⬇ 👤 📄 ☰

**Root KSK Sentinel tests**

This page helps to test your DNS resolvers if they're ready for the next DNSSEC root key rollover.

The technique is based on and IETF standard "RFC8509: A Root Key Trust Anchor Sentinel for DNSSEC", which is work-in-progress and there's not yet so much deploy in DNS resolvers.

[Launch tests for my DNS resolvers](#)

[ debug... ]

is-ta-KSK2017

is-ta-KSK2026

[Click for Results](#)

Congratulations! your resolver is ready for rollover.

Copyright Hugo Salgado 2025 - <https://hugo.salga.do>

# Más información

- Sitio oficial de la raíz:
  - <https://www.iana.org/dnssec>
- Mi blog con información de cada ceremonia <https://hugo.salga.do>
- Lista de correo DNS - LACNOG



# Obrigado / Gracias / Thanks

Hugo Salgado - Grupo de Trabajo DNS de LACNOG

ICANN DNSSEC Trusted Community Representative (Cryptographic Officer 6-East)

**lacnic43**

5-9 de Mayo 2025 / São Paulo, Brasil