

tucows/domains

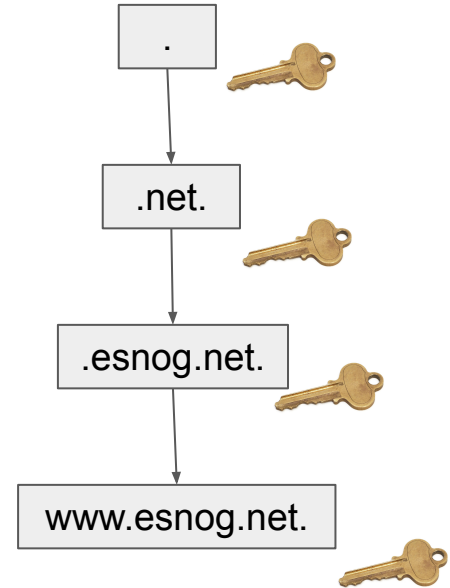
Las rotaciones de la llave raíz del DNS

Hugo Salgado, Tucows Domains
Oficial Criptográfico de la raíz del DNS (IANA)

ESNOG-36, octubre 2026

¿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

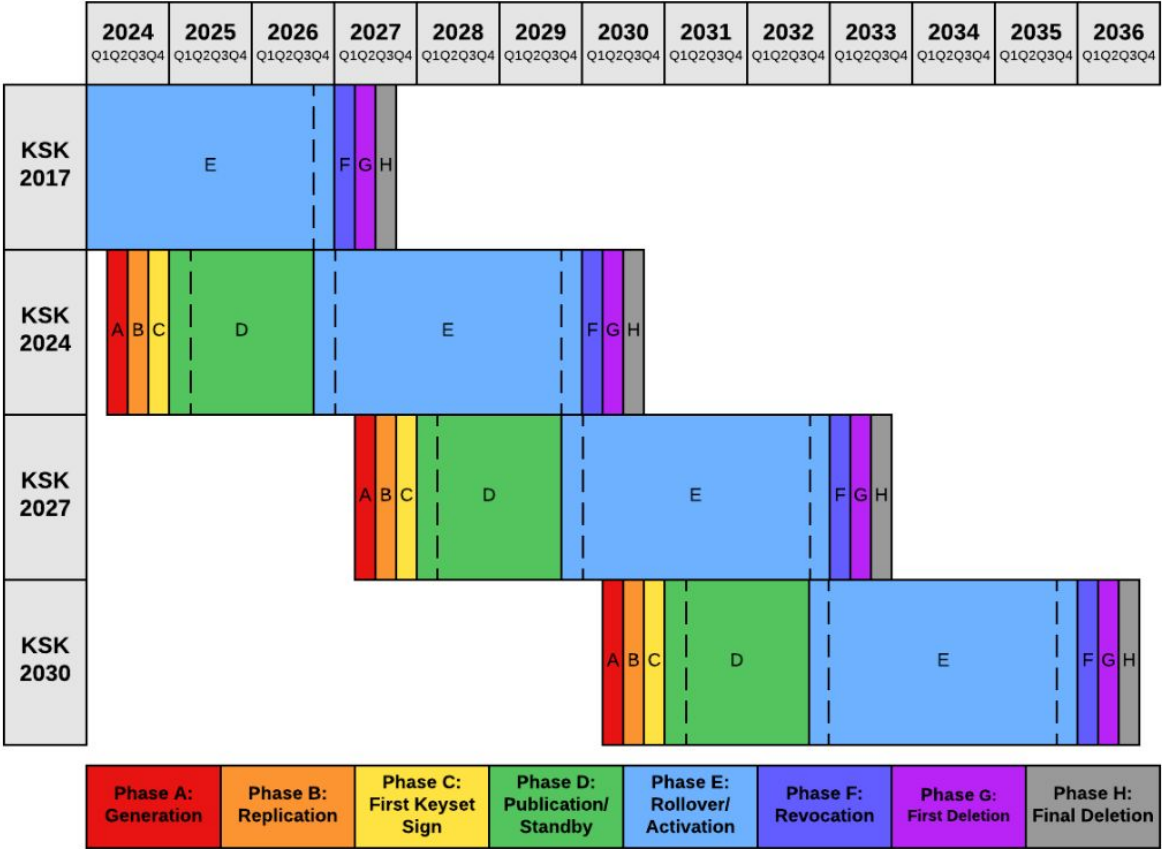
freighten crucifix button Apollo spheroid megaton puppy hideaway brickvard bottomless deadbolt pion5

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 de rotación/activación:
 - Es parte del DNSKEY de la raíz, junto a la KSK2017
 - Es la única que firma el DNSKEY set. Ya no firma la anterior.
- Siguiente estado: revocación y eliminación de KSK2017
 - La KSK2017 se seguirá publicando, pero pasará a tener el bit de revocada
 - Se eliminará finalmente a mediados de 2027

Nueva llave de la raíz: KSK2024

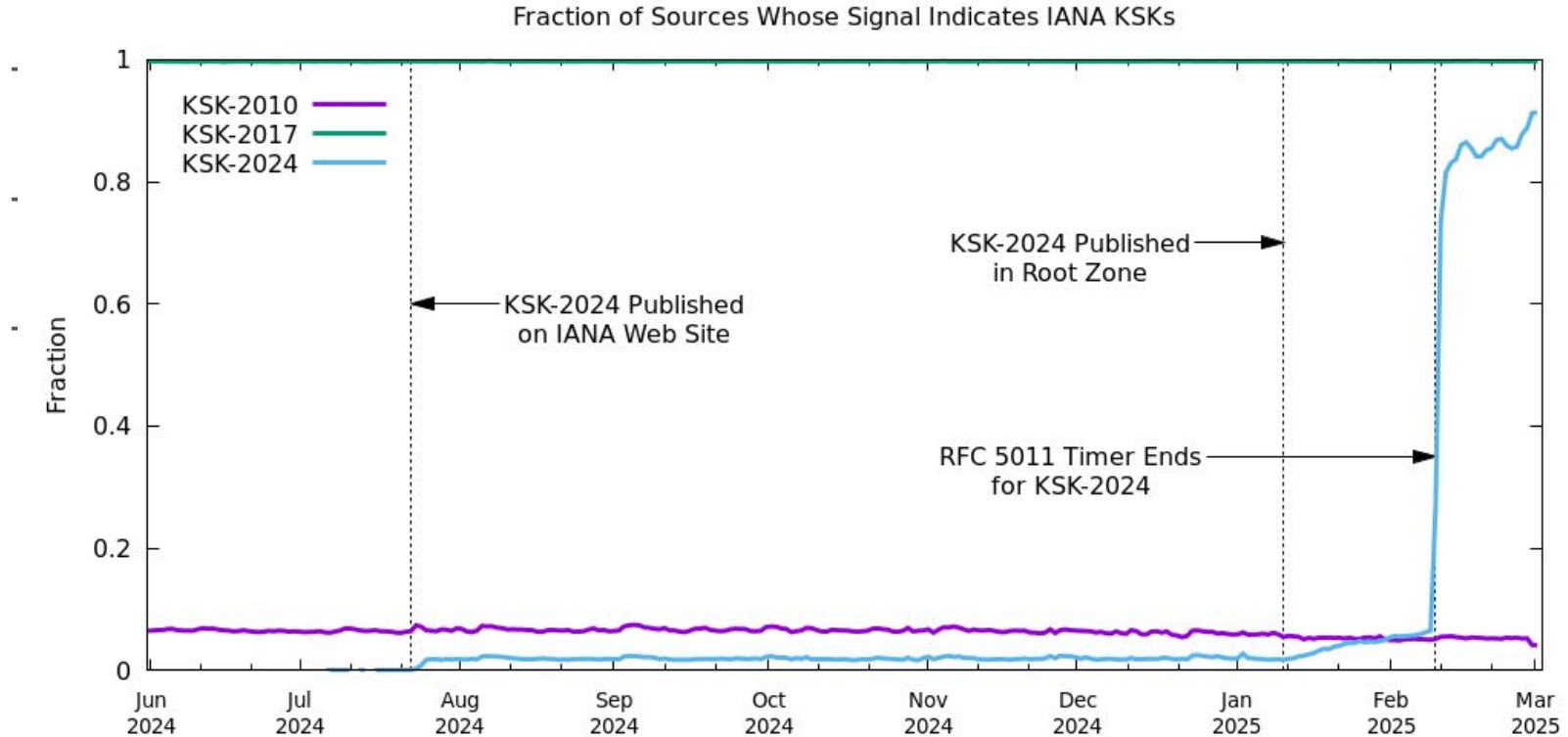
- Terc
- Gen
-
- Act
-
-
- Sig
-
-



¿Qué podría haber pasado?

- 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 podría haber pasado?



“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/cidltphy... ;{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]: [tasign] 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
```

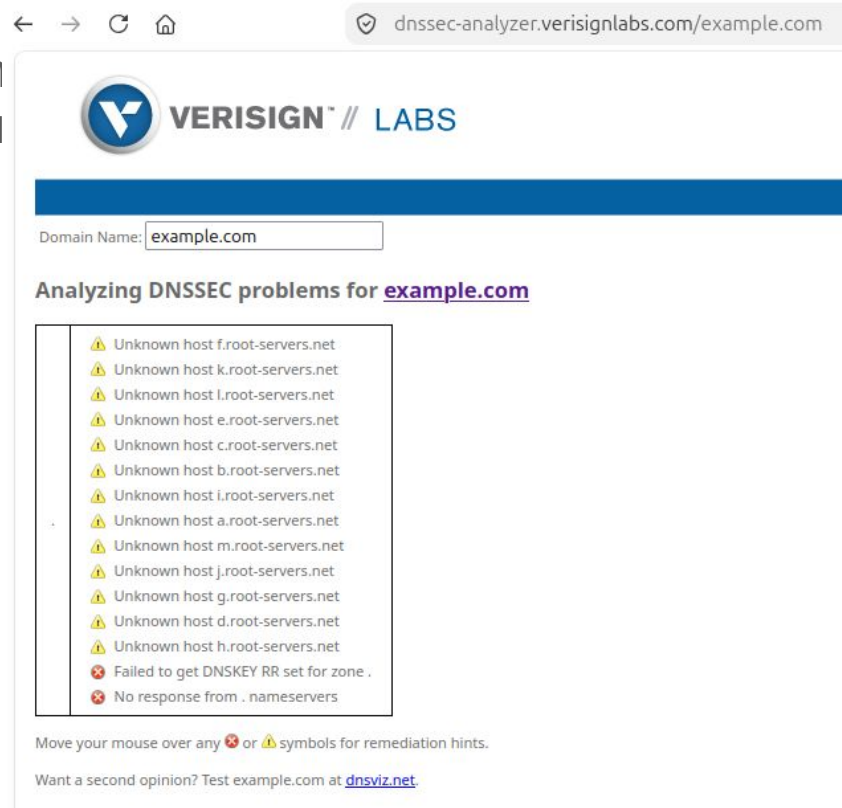
```
". 20326 38696"
```

¿Y qué efectivamente pasó?

- Nada importante
 - validador DNSSEC de Verisign

¿Y qué efectivamente pasó?

- Nada importante
- validador DN



The screenshot shows a web browser window with the address bar displaying `dnssec-analyzer.verisignlabs.com/example.com`. The page header features the Verisign Labs logo. Below the header, the domain name `example.com` is entered in a text field. The main heading reads "Analyzing DNSSEC problems for [example.com](#)". A list of errors is displayed, each preceded by a yellow warning icon:

- Unknown host f.root-servers.net
- Unknown host k.root-servers.net
- Unknown host l.root-servers.net
- Unknown host e.root-servers.net
- Unknown host c.root-servers.net
- Unknown host b.root-servers.net
- Unknown host i.root-servers.net
- Unknown host a.root-servers.net
- Unknown host m.root-servers.net
- Unknown host j.root-servers.net
- Unknown host g.root-servers.net
- Unknown host d.root-servers.net
- Unknown host h.root-servers.net
- Failed to get DNSKEY RR set for zone .
- No response from . nameservers

Below the list, a note states: "Move your mouse over any  or  symbols for remediation hints." At the bottom, it says: "Want a second opinion? Test example.com at [dnsviz.net](#)."

¿Y qué efectivamente pasó?

- Nada importante
 - validador DNSSEC de Verisign
 - bug en systemd-resolved de Ubuntu 24.04

¿Y qué efectivamente pasó?

- Na



Ubuntu
systemd package

-

-

Overview

Code

Bugs

Blueprints

Translations

Answers

Ubuntu 24.04: systemd-resolved DNSSEC fails after root KSK rollover; built-in trust anchor lacks key 38696

Bug #2170538 reported by  Ian Packer on 2026-10-12

This bug affects 16 people

 88

Affects	Status	Importance	Assigned to	Milestone
 systemd (Ubuntu)	Fix Released	Undecided	 Sudhakar Verma	

Bug Description

Ubuntu 24.04: systemd-resolved DNSSEC fails after root KSK rollover; built-in trust anchor lacks key 38696

System just stops resolving. When doing a terminal lookup it reports a key missing message.

Fuente: <https://bugs.launchpad.net/ubuntu/+source/systemd/+bug/2170538>

¿Y qué efectivamente pasó?

- Nada importante
 - validador DNSSEC de Verisign
 - bug en systemd-resolved de Ubuntu 24.04
 - bug en dnsmasq para Debian 12

¿Y qué efectivamente pasó?

- Nada importante

- validad
- bug en
- bug en

Debian Bug report logs - [#1150730](#)

dnsmasq-base 2.90-4~deb12u2 ships with outdated DNSSEC trust anchor

Package: [dnsmasq-base](#); Maintainer for [dnsmasq-base](#) is [Simon Kelley <simon@thekelleys.org.uk>](#); Source for [dnsmasq-base](#) is [dnsmasq-base](#)

Reported by: [Jason Bolger <jbolger@techcore.com.au>](#)

Date: Mon, 12 Oct 2026 23:47:02 UTC

Severity: normal

Tags: bookworm

Merged with [1150731](#)

Found in version [dnsmasq/2.90-4~deb12u2](#)

[Reply](#) or [subscribe](#) to this bug.

☐ Display info messages

View this report as an [mbox folder](#), [status mbox](#), [maintainer mbox](#)

[Message #5](#) received at [submit@bugs.debian.org](#) ([full text](#), [mbox](#), [reply](#)):

From: Jason Bolger <jbolger@techcore.com.au>

To: submit@bugs.debian.org

Subject: dnsmasq-base 2.90-4~deb12u2 ships with outdated DNSSEC trust anchor

Date: Tue, 13 Oct 2026 10:06:22 +1100

Package: dnsmasq-base

Version: 2.90-4~deb12u2

Long time user, first time caller.

This package is shipping with outdated dns trust anchor information in /usr/share/dnsmasq-base/trust-anchors.conf causing all DNSSEC validations to fail.

Rather than correcting it I suggest making the package dependent on dns-root-data which appears to be the Debian package for maintaining DNS data.

Fuente: https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1150730&pow_referer=

¿Y qué efectivamente pasó?

- Nada importante
 - validador DNSSEC de Verisign
 - bug en systemd-resolved de Ubuntu 24.04
 - bug en dnsmasq para Debian 12
 - ISPs salvados en el último minuto (reporte APNIC)

¿Y qué efectivamente pasó?

- Nada i

- val

- bu

- bu

- ISF

AS	CC	KSK-2024	Tests	Validating	RFC8509	KSK-2024	NOT KSK-2024	Name
262202	CR	49.40%	9,441	9,343	2,201	469	481	Telefonica de Costa Rica, Costa Rica
328169	SZ	48.90%	4,694	4,687	1,199	276	288	Swazi Mobile, Swaziland
328341	ZA	48.90%	2,551	2,522	1,352	284	297	Capricorn Networks , South Africa
17470	LK	48.70%	15,011	11,749	2,952	717	756	Hutchison Telecoms, Sri Lanka
9335	TH	48.40%	4,905	4,877	1,355	299	319	National Teleco, Thailand
45925	BD	48.20%	7,886	7,811	2,046	465	499	Teletalk, Bangladesh
29544	MR	47.90%	41,149	40,758	8,032	1,842	2,003	Mauritanian Telecommunication, Mauritania
30990	DJ	47.40%	9,472	9,393	2,701	641	711	Dibjouti Telecom, Djibouti
329129	LY	46.80%	7,879	7,843	1,790	384	436	Libya Tech, Lybia
136336	IN	46.00%	8,113	6,972	1,818	353	414	Thamizhaga, India
9658	PH	45.60%	6,920	6,293	2,062	555	661	Eastern Telecoms, Philippines
135300	MM	45.40%	5,813	4,600	1,150	228	274	Myanmar Broadband, Myanmar
205368	AM	38.60%	4,227	4,209	2,349	536	852	Fnet, Armenia
24812	UA	32.00%	10,791	3,437	1,322	205	436	HomeNet, Ukraine

Fuente: <https://ispcol.potaroo.net/2026-10/kskroll.html>

¿Y qué efectivamente pasó?

- Nada importante
 - validador DNSSEC de Verisign
 - bug en systemd-resolved de Ubuntu 24.04
 - bug en dnsmasq para Debian 12
 - ISPs salvados en el último minuto (reporte APNIC)
 - Agentes de ThousandEyes

¿Y qué efectivamente pasó?

- Nada importante
- validado
- bug en s
- bug en d
- ISPs sal
- Agentes

Cloud and Enterprise Agents showing DNSSEC failures.

Incident Report for ThousandEyes

Resolved

This incident is now resolved.

Please follow the instructions using one of the options below if any of your Enterprise Agents cannot automatically update themselves.

Option 1: Add the New DNSSEC Key

Adding the new DNSSEC key can restore the Agent's connection to the ThousandEyes platform. After the

Fuente: <https://status.thousandeyes.com/incidents/t3j5l8mwnv88>

¿Qué se viene en el futuro?

- Rotación cada tres años
 - Ya se generará la nueva en abril 2027

¿Qué se viene en el futuro?

- Rotación cada tres años
 - Ya se generará la nueva en abril 2027
- Cambio de algoritmo!
 - ECDSA en vez de RSA

¿Qué se viene en el futuro?

- Rotación cada tres años
 - Ya se generará la nueva en abril 2027
- Cambio de algoritmo!
 - ECDSA en vez de RSA
- Mejoras en campaña de visibilización

¿Qué se viene en el futuro?

- Rotación cada tres años
 - Ya se generará la nueva en abril 2027
- Cambio de algoritmo!
 - ECDSA en vez de RSA
- Mejoras en campaña de visibilización
- Mejoras de usabilidad DNSSEC
 - Automatización CDS

¿Qué se viene en el futuro?

- Rotación cada tres años
 - Ya se generará la nueva en abril 2027
- Cambio de algoritmo!
 - ECDSA en vez de RSA
- Mejoras en campaña de visibilización
- Mejoras de usabilidad DNSSEC
 - Automatización CDS
- Futuro: criptografía post-cuántica

Más información

- Sitio oficial de la raíz:
 - <https://www.iana.org/dnssec>
- Mi blog con información de cada ceremonia <https://hugo.salga.do>
- ICANN KSK rollover mailing list
<https://lists.icann.org/hyperkitty/list/ksk-rollover@icann.org/>

Questions?

/domains

Thank you!

tucows/domains