

Estado de la rotación de la llave KSK para la raíz

...ya casi lo logramos!

Mauricio Vergara Ereche

LACNIC 27 & LACNOG 2017

22 Sep 2017



Agenda

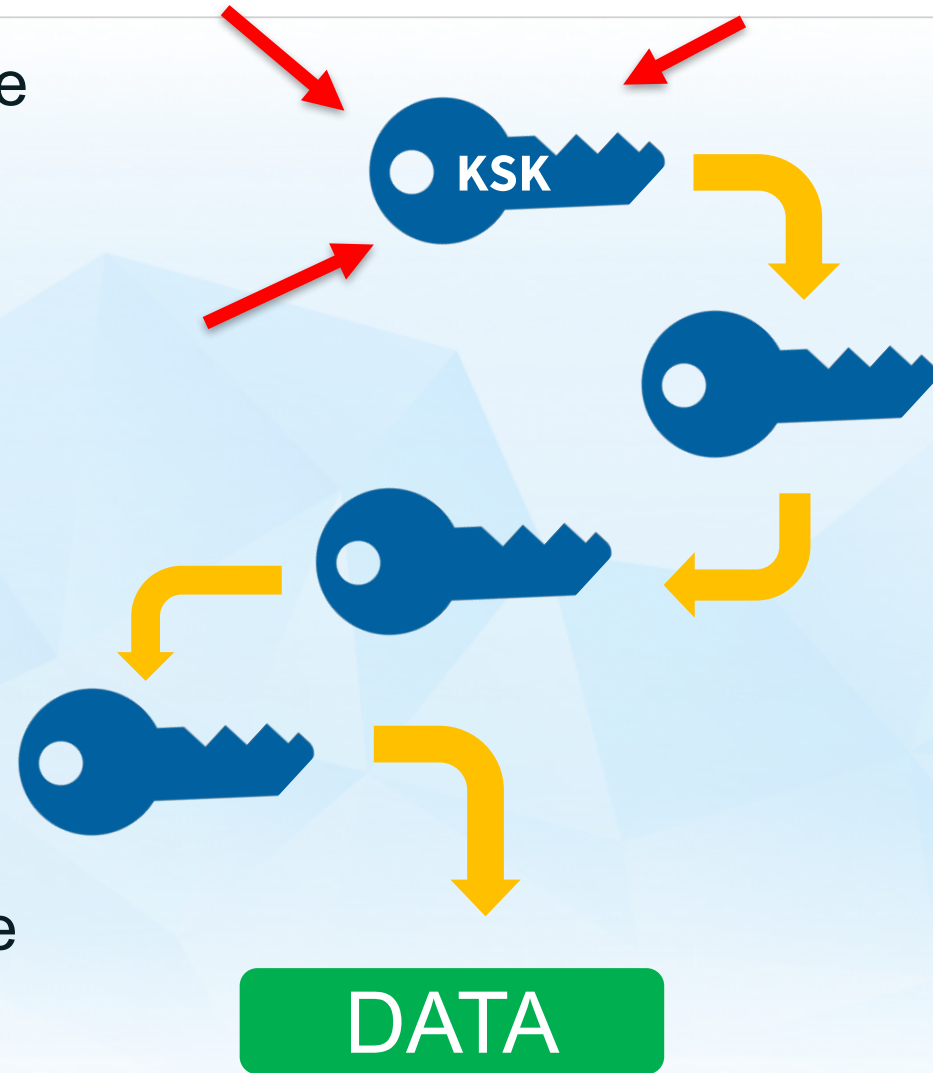
- KSK Rollover: En qué etapa del proyecto estamos
- Verificando que todo funciona en los *resolvers* y se ven las llaves correctas
- Qué hacer si algo está fallando
- Todo va a estar bien

KSK Rollover

En qué etapa del proyecto
estamos

La KSK en la zona raíz

- La **KSK** (Key Signing Key) de la zona Raíz es la llave criptográfica de mayor nivel en la jerarquía de DNSSEC
- La parte **pública** de la llave KSK es un **parámetro** de configuración de los DNS recursivos (*resolvers*) que ofrecen validación DNSSEC
- El otro "rol" es el de una llave llamada **ZSK** (Zone Signing Key)



Por qué hacer un rollover de la KSK

- **Hasta ahora, sólo ha existido una llave KSK operando en la zona raíz del DNS**
 - Esa llave la llamamos **"KSK-2010"**
 - Existe desde el 2010, no hubo nada antes de eso.
- **Una nueva llave KSK será puesta en producción en menos de 1 mes**
 - Esa llave la llamamos **"KSK-2017"**
 - Para mantener la operación estable, ordenada y sin contratiempos, necesitamos asegurar su rotación
- **Operadores de servidores DNSSEC recursivos con validación activada pueden tener trabajo**
 - Tal vez, sólo implique revisar algunas configuraciones
 - Tal vez tengan que instalar manualmente la KSK-2017

Hitos importantes

Event	Date
Creation of KSK-2017	October 27, 2016
Production Qualified	February 2, 2017
Out-of-DNS-band Publication	Now , onwards
In-band (<i>Automated Updates</i>) Publication	July 11, 2017 and onwards
Sign (Production Use)	October 11, 2017 and onwards
Revoke KSK-2010	January 11, 2018
Remove KSK-2010 from systems	Dates TBD , 2018

Verificando que todo funcione

Está bien configurado mi
servidor DNS resolver?

Paso 1: identificar la KSK-2017

- La KSK-2017 tiene el Key Tag (definida por el parámetro del protocolo):
 - **20326**
- Los registros DS (Delegation Signer) para la KSK-2017 son:

```
. IN DS 20326 8 1 AE1EA5B974D4C858B740BD03E3CED7E  
BFCBD1724
```

```
. IN DS 20326 8 2 E06D44B80B8F1D39A95C0B0D7C65D084  
58E880409BBC683457104237C7F8EC8D
```


Paso 1: identificar la KSK-2017

- El DNSKEY de la llave KSK-2017:

```
IN DNSKEY 257 3 8 (  
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTO  
iW1vkIbzxeF3+/4RgW0q7HrxRixHlFlExOLAJr5emLvN  
7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5  
LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF0jLHwVN8  
efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuV7  
pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLY  
A4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnXGXws  
9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=  
) ; KSK; alg = RSASHA256; key id = 20326
```

RFC 5011: Actualización automática

- Actualización automática de los *Trust Anchors*
 - Usa actuales trust anchors para **aprender** los nuevos
 - Basado en **períodos de tiempo** – si una nueva llave aparece y nadie reclama por su inclusión, entonces puede confiarse en ella
 - El período para "darse cuenta" es de **30 días**.
 - En algunos meses, este método se usará para **revocar** KSK-2010
 - Los operadores pueden **elegir** no usar las actualizaciones automáticas.

Paso 2: Mi resolver caché valida DNSSEC?

- Probar enviando una consulta a "***dnssec-failed.org***" con los parámetros DNSSEC activados
 - Si la respuesta retorna **SERVFAIL**, quiere decir que DNSSEC **sí está funcionando**.
 - Si la respuesta entrega una **dirección IPv4**, entonces la validación DNSSEC **no está funcionando**

Paso 2: Mi resolver caché valida DNSSEC?

```
$ dig @$server dnssec-failed.org a +dnssec
```

```
; <<>> DiG 9.8.3-P1 <<>> dnssec-failed.org a +dnssec  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 10492  
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags: do; udp: 4096  
;; QUESTION SECTION:  
;dnssec-failed.org. IN A  
  
;; Query time: 756 msec  
;; SERVER: 10.47.11.34#53(10.47.11.34)  
;; WHEN: Tue Sep 5 19:04:04 2017  
;; MSG SIZE rcvd: 46
```

DNSSEC is on!

Paso 2: Mi resolver caché valida DNSSEC?

```
$ dig @$server dnssec-failed.org a +dnssec
```

```
; <<>> DiG 9.8.3-P1 <<>> dnssec-failed.org a +dnssec  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5832  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags: do; udp: 512  
;; QUESTION SECTION:  
;dnssec-failed.org. IN A
```

DNSSEC is off!

```
;; ANSWER SECTION:
```

```
dnssec-failed.org. 7200 IN 69.252.80.75
```

```
;; Query time: 76 msec  
;; SERVER: 192.168.1.1#53(192.168.1.1)  
;; WHEN: Tue Sep 5 18:58:57 2017  
;; MSG SIZE rcvd: 62
```

Paso 3: Cómo sé si puedo confiar en KSK-2017

- **BIND**
 - 9.11.x "rndc managed-keys status"
 - 9.9.x and 9.10.x "rndc secroots"
- **Unbound**
 - Inspect the configured root.key file
- **PowerDNS**
 - "rec_control get-tas"
- **Knot-resolver**
 - Inspect the configured root.keys file
- **Microsoft Server**
 - "Administrative Tools"->"DNS"->"Trust Points"

**[https://www.icann.org/
dns-resolvers-
checking-current-
trust-anchors](https://www.icann.org/dns-resolvers-checking-current-trust-anchors)**

Qué se debería ver en las pruebas

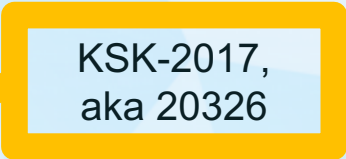
- **2 llaves listadas como trust anchors para la zona raíz:**
 - **KSK-2017 con key-id 20326**
 - Si usted no ve eso, significa que su resolver cache validador VA A COMENZAR A FALLAR el 11 de Octubre
 - **KSK-2010 con key-id 19036**
 - Si usted no ve eso, significa que su resolver cache validador no está funcionando ahora
- **Eventualmente KSK-2010 va a desaparecer**
 - Pero falta aún para eso.

Ejemplo: BIND

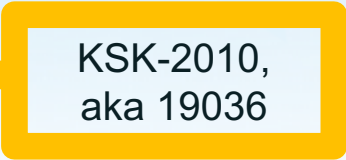
```
bind-9.9.5 $ rndc -c rndc.conf secroots  
bind-9.9.5 $ cat named.secroots  
05-Sep-2017 09:24:06.361
```

```
Start view _default
```

```
./RSASHA256/20326 ; managed  
./RSASHA256/19036 ; managed
```



KSK-2017,
aka 20326



KSK-2010,
aka 19036

Ejemplo: Unbound

```
unbound $ cat root.key
; autotrust trust anchor file
;;id: . 1
;;last_queried: 1504239596 ;;Fri Sep 1 00:19:56 2017
;;last_success: 1504239596 ;;Fri Sep 1 00:19:56 2017
;;next_probe_time: 1504281134 ;;Fri Sep 1 11:52:14 2017
;;query_failed: 0
;;query_interval: 43200
;;retry_time: 8640
. 172800 IN DNSKEY 257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiWlvkIbzxef3+4RgWOq7HrxR...xHlF
lExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5...KyWbRd2n9V...Ge2R8
PzgCmr3EgVLRjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58D...qqls3eN...uv7pr
+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIidsIXxuOLYA4/ilBmSVIzuDWfdRU...hHdY6+...8HFRm
+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU= ;{id = 20326 (ksk),
size = 2048b} ;;state=2 [ VALID ] ;;count=0 ;;lastchange=1502438004
;;Fri Aug 11 03:53:24 2017
. 172800 IN DNSKEY 257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW008gcCjFFVQUTf6v5...fLjwBd0Y
I0EzrAcQqBGCzh/RStIo08g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnM...oxP/VHL49
6M/QZxkjf5/Efucp2gaDX6RS6CXpoY68LsvpVjR0ZSwzz1apAzvN9dlzEheX7IC...tuA6G3LQ
pzW5hOA2hzCTMjJPJ8Lbqf6dsV6DoBQzgul0sGICGOYl70yQdXfz57relSQageu...lpAdTTJ25A
sRTAoub8ONGcLmqrAmRLKBPldfwhYB4N7knNnulqQxA+Uklihz0= ;{id = 19036 (ksk),
size = 2048b} ;;state=2 [ VALID ] ;;count=0 ;;lastchange=1459820836
;;Mon Apr 4 21:47:16 2016
```

KSK-2017,
Key-id: 20326

KSK-2010,
Key-id: 19036

Si ambas llaves KSKs se ven "trusted"

TODO ESTA BIEN!



Qué hacer si algo falla?

Algunos consejos

Cómo lo arreglo?

- Si uno no ve **AMBAS** KSKs como "trusted", entonces hay que hacer ajustes
- Cada "How-To" depende de la realidad de cada uno

**[https://www.icann.org/
dns-resolvers-
updating-latest-trust-
anchor](https://www.icann.org/dns-resolvers-updating-latest-trust-anchor)**

Obtener la KSK Manualmente

- Via IANA:

<https://data.iana.org/root-anchors/root-anchors.xml>

- Via DNS:

```
dig @1.root-servers.net . DNSKEY +multi
```

- Via Software Update

- Más opciones, se pueden ver:

<https://www.icann.org/dns-resolvers-updating-latest-trust-anchor>

- Una herramienta que recibe los Trust-Anchors y los valida:

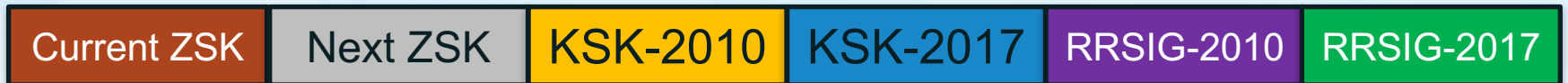
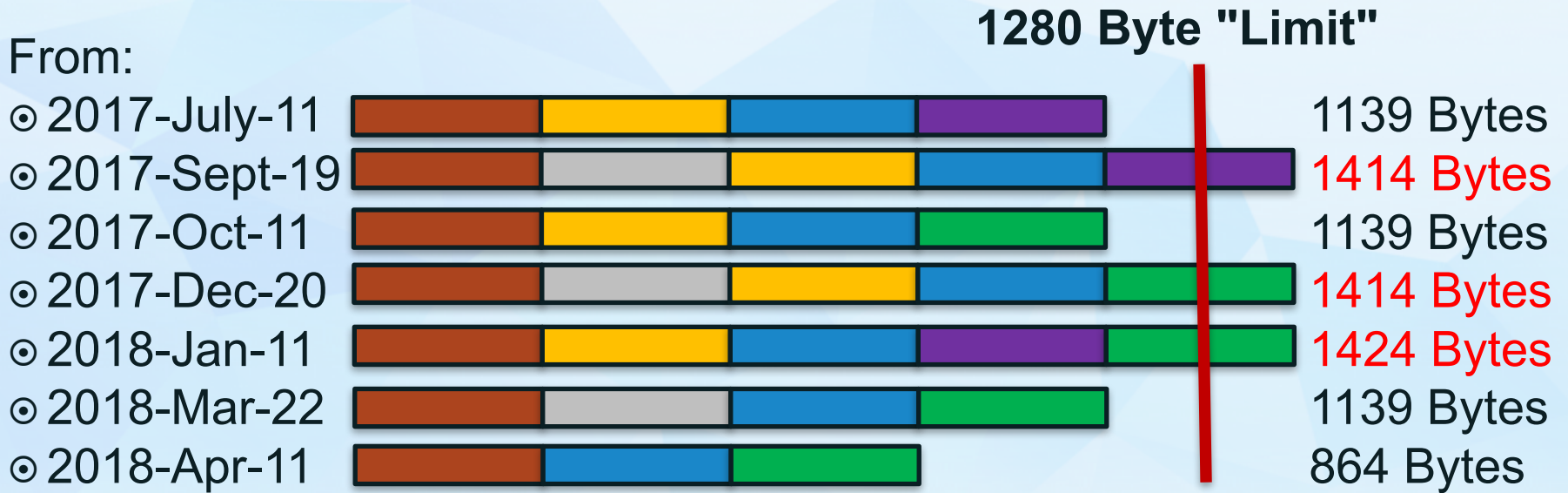
<https://github.com/iana-org/get-trust-anchor>

Síntomas o cosas relacionadas al Rollover

- **Si los problemas causan "fragmentación"**
 - Validación DNSSEC puede fallar por todas las cosas que impliquen el no poder alcanzar la DNSKEY de la zona Raíz seteada para KSK-2017
 - Revise si hay un **número mayor** de consultas saliendo desde el *resolver* o **re-intentando** la misma pregunta.
- **Si hay problemas causados por usar el trust-anchor equivocado.**
 - Validación DNSSEC fallará, ya que será imposible construir la cadena de confianza.
 - Busque en sus logs, por **"validation failure"** (cada implementación tiene su propio forma de nombrar)

Fragmentación, IPv4, IPv6 y DNS

Visualizing Packet Sizes (response to root DNSKEY query)



Recomendación para IPv6 e IPv4

- Asegúrese que sus servidores pueden realizar y recibir consultas sobre TCP (especialmente en IPv6)
- Testee y verifique que puede recibir sets de DNSKEYs de gran tamaño:

<http://keysizetest.verisignlabs.com>

<https://www.dns-oarc.net/oarc/services/replysizetest>

- Estas soluciones deben ser "arreglos permanentes", no sólo para el KSK rollover. TCP es una pieza importante del funcionamiento del DNS.

Más información

<https://icann.org/kskroll>

<https://lacnog.org/wg-dns-ksk-rollover>

Consultas en la región?

Lista de correos dns-esp:

<https://listas.nic.cl/mailman/listinfo/dns-esp>



One World, One Internet

Visit us at icann.org



[@icann](https://twitter.com/icann)



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin/company/icann



slideshare/icannpresentations



soundcloud/icann