Traspaso de la KSK en las Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC)

Daniel Fink, ICANN

LAC-i Roadshow Montevideo

16 de Agosto, 2018

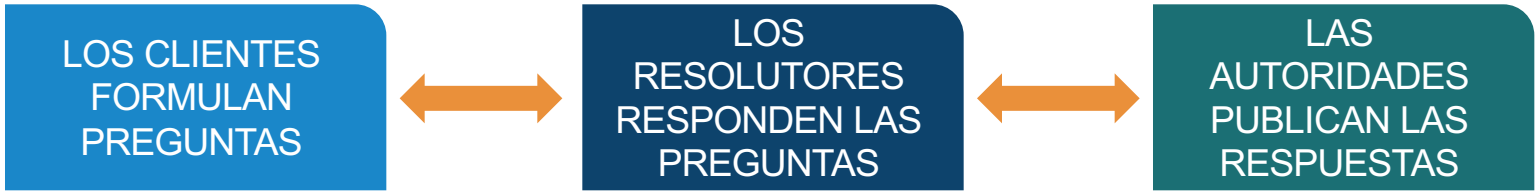
DNSSEC

¿Qué son las DNSSEC?

DNSSEC es una sigla en inglés que significa **Extensiones de Seguridad del Sistema de Nombres de Dominio (DNS).**

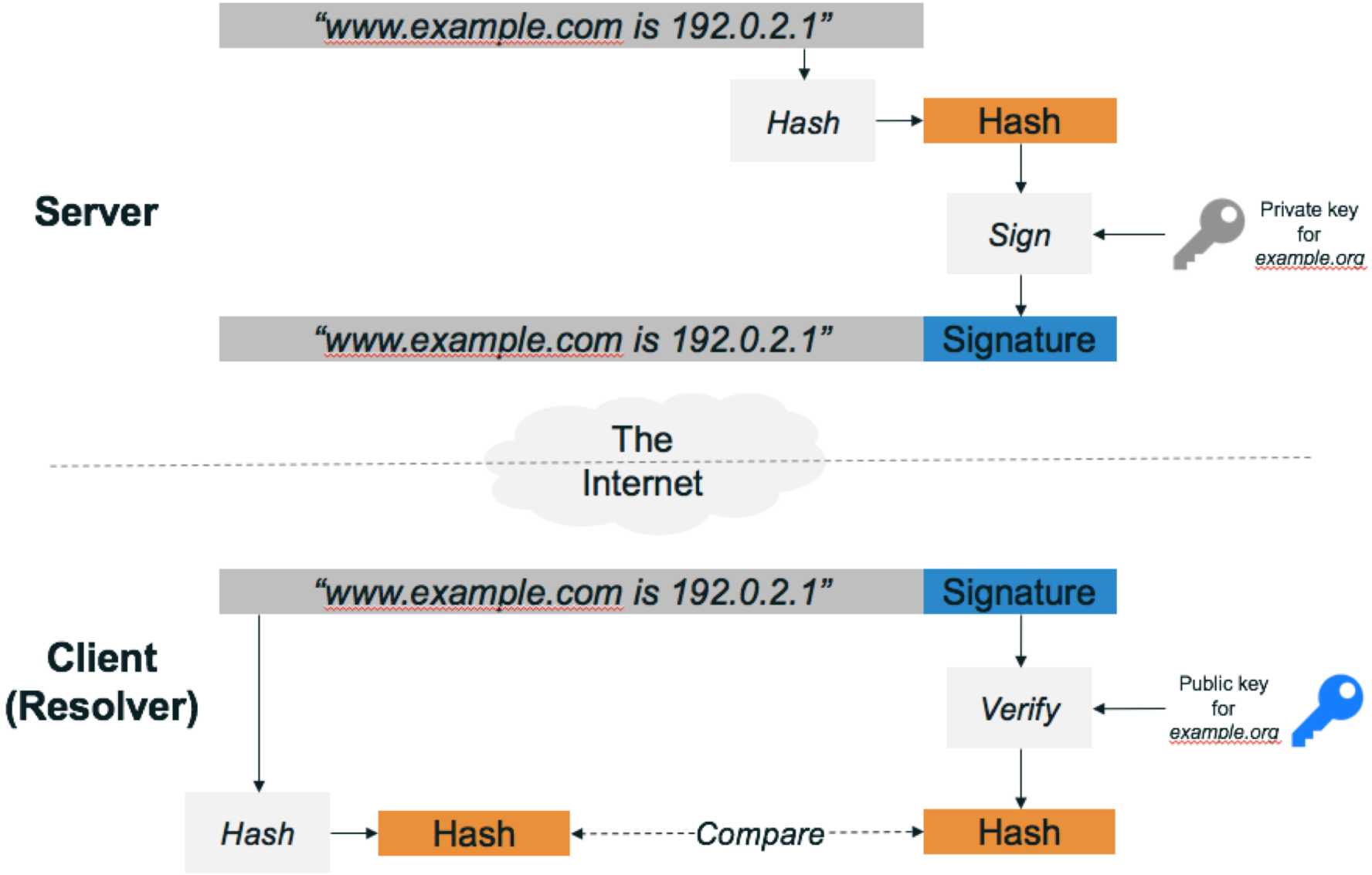
- Las DNSSEC constituyen un protocolo que se está implementando actualmente para proteger al DNS.
- Las DNSSEC agregan seguridad al DNS incorporando criptografía de clave pública en la jerarquía del DNS, lo cual da lugar a una Infraestructura de Clave Pública (PKI) única y abierta para los nombres de dominio.
- Las DNSSEC son el resultado de más de una década de desarrollo de normas abiertas originadas en la comunidad.

Elementos del DNS vulnerables a los ataques

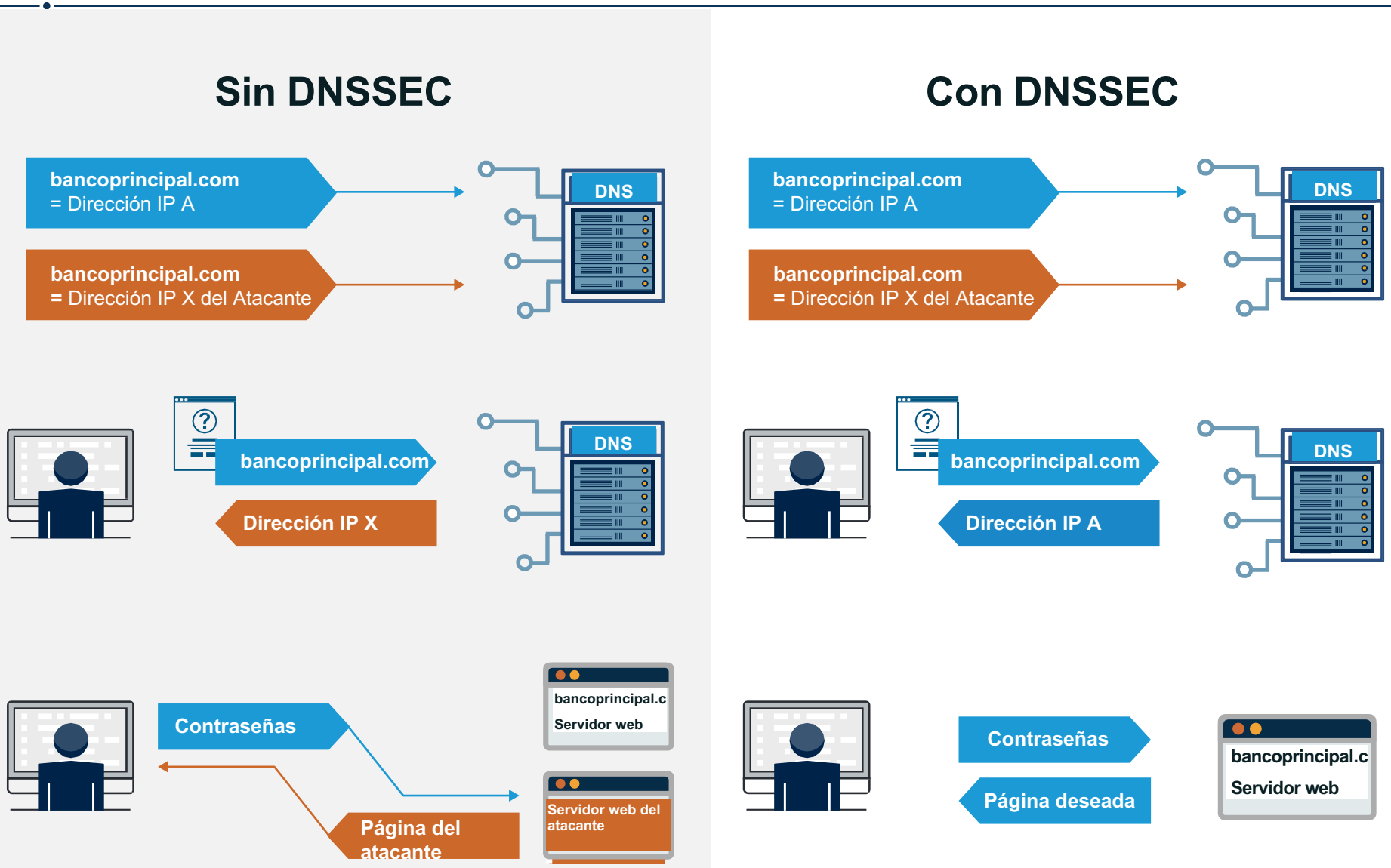


- **Los servidores de nombres autoritativos** alojan datos de zona: el conjunto de datos del DNS que publica el registratario.
- **Los resolutores de nombres recursivos** (resolutores) son sistemas que encuentran respuestas a consultas de datos del DNS.
- **Los resolutores caché** encuentran y almacenan las respuestas localmente durante un período de Tiempo de Vida Útil (TTL).
- **Los resolutores cliente o mínimos** son software en aplicaciones, aplicaciones móviles o sistemas operativos que consultan al DNS y procesan las respuestas.

Public Key Cryptography y DNSSEC



¿Cómo funcionan las DNSSEC?



¿Quién se beneficia con las DNSSEC?

Usuario final

Adquiere confianza respecto de llegar al sitio web deseado.

Registratario

Mitiga el fraude y aumenta la protección de las marcas.

Registrador

Cumple con los estándares de la industria y con las demandas de los registratarios para brindar mayor seguridad.

Registro

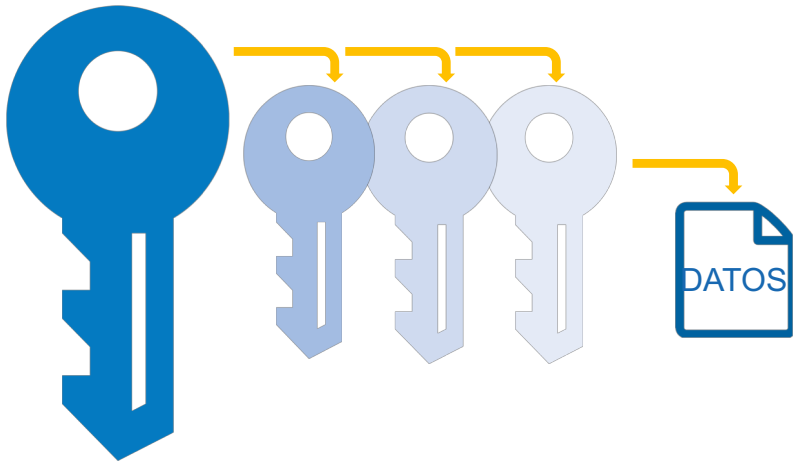
Cumple con las prácticas recomendadas de la industria y las demandas de los registradores para aumentar la seguridad del dominio.

Traspaso de la KSK

Traspaso de la KSK: descripción general

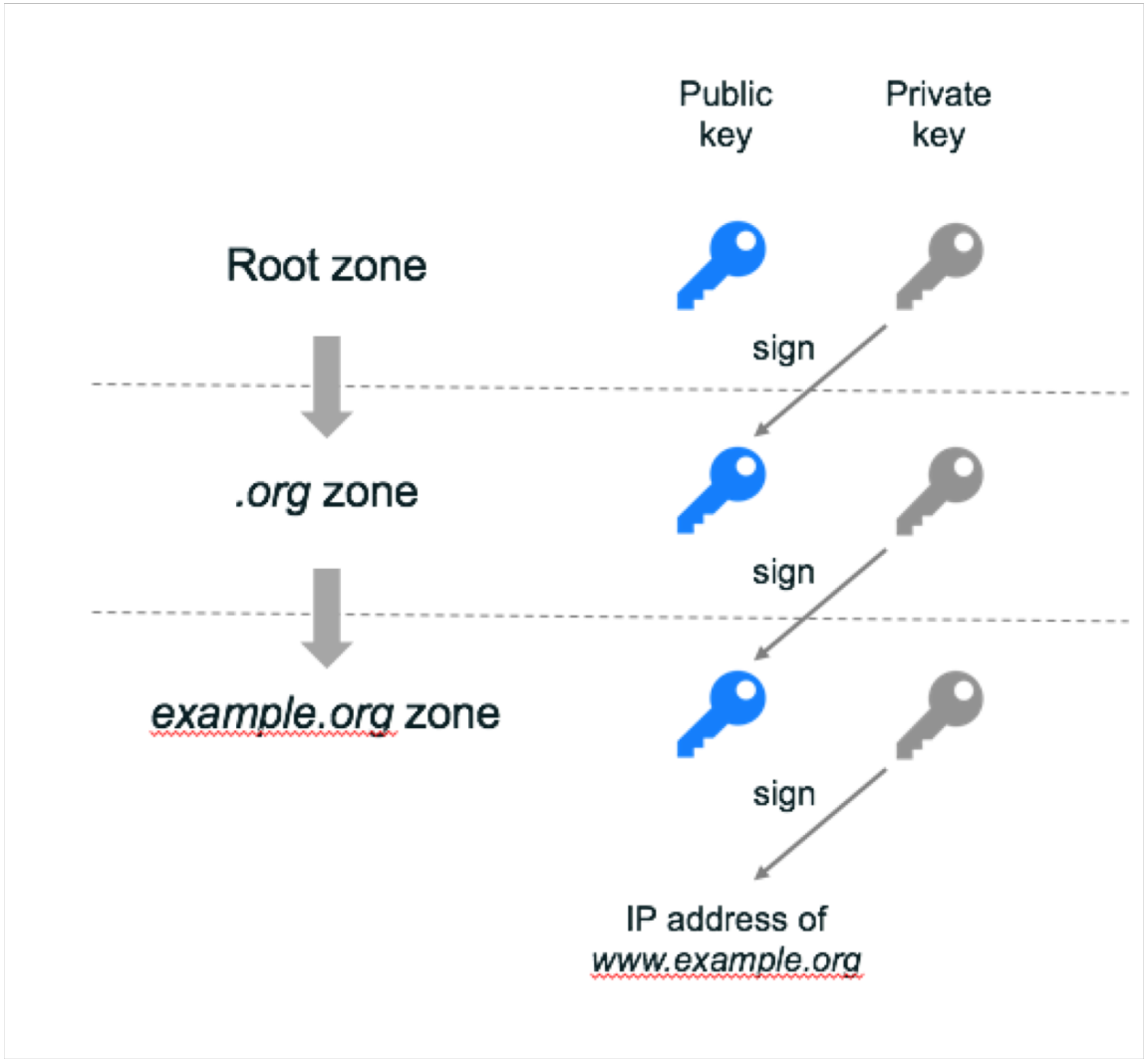
La ICANN se encuentra en medio del proceso de traspaso de la clave para la firma de la llave de la zona raíz (KSK) para las Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC).

- La KSK es la clave criptográfica más alta en la jerarquía de las DNSSEC.
- La KSK es un par de claves criptográficas con un componente público y uno privado.
  - La parte pública es el punto de partida de confianza para la validación de las DNSSEC.
  - La parte privada firma la clave para la firma de la llave de la zona raíz (ZSK).
- La KSK genera una “cadena de confianza” de claves y firmas sucesivas para validar la autenticidad de los datos firmados en las DNSSEC.



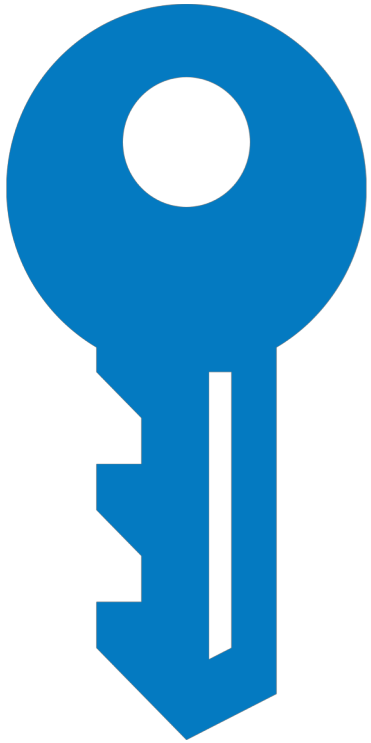
Ver video:
https://youtu.be/cAPyLI1qowY

La KSK es el punto de partida de confianza



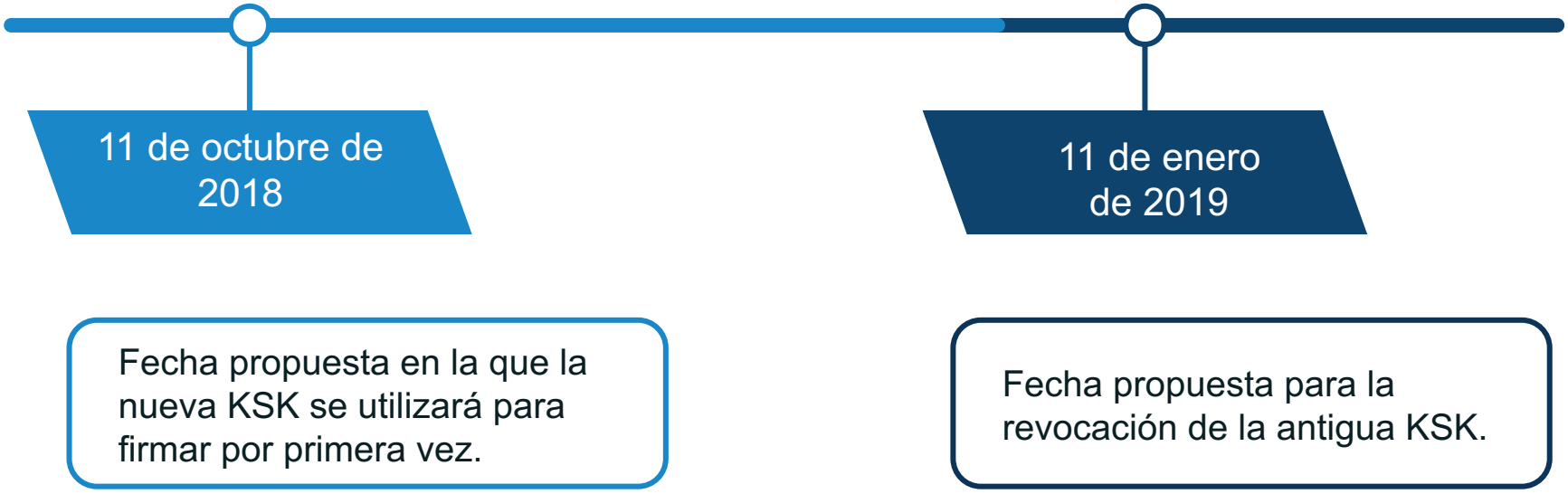
¿Por qué la ICANN está traspasando la KSK?

- Al igual que con las contraseñas, las claves criptográficas utilizadas en los datos del DNS para la firma de las DNSSEC deben cambiarse periódicamente.
  - Garantiza que la infraestructura pueda soportar el cambio de claves en caso de emergencia.
- Nunca antes se ha realizado este tipo de cambio a nivel de la raíz.
  - Desde el 2010, hay una KSK de las DNSSEC de la zona raíz operativa y funcional.
- El traspaso de la KSK debe ser coordinado de manera amplia y cuidadosa para garantizar que no interfiera con las operaciones normales.



¿Cuándo tendrá lugar el traspaso de la KSK?

El traspaso de la KSK es un proceso, no es un evento único. Las siguientes fechas son hitos clave en el proceso en las que los usuarios finales pueden sufrir interrupciones en los servicios de Internet:



http://data.iana.org/root-anchors/

¿Quién se verá afectado?

Desarrolladores y distribuidores de software del DNS

Integradores de sistema

Operadores de redes

Operadores de servidores raíz

Proveedores de Servicios de Internet

Usuarios finales

(Si los operadores de resolutores no realizan ninguna acción)

Por qué es necesario prepararse

Si ha habilitado la validación de las DNSSEC, debe actualizar sus sistemas con la nueva KSK para contribuir a que los usuarios de Internet puedan acceder a Internet sin inconvenientes.

- Actualmente, el 25 por ciento de los usuarios de Internet a nivel mundial, o **750 millones de personas**, utilizan resolutores de validación de DNSSEC que podrían verse afectados por el traspaso de la KSK.
- Si los resolutores de validación no tienen la clave nueva cuando se realice el traspaso de la KSK, los usuarios finales que dependen de dichos resolutores encontrarán errores y **no podrán tener acceso a Internet.**

¿Qué deben hacer los operadores?

Saber si las DNSSEC están habilitadas en sus servidores.

Conocer cómo se evalúa la confianza en sus operaciones.

Probar/verificar sus configuraciones.

Inspeccionar los archivos de configuración: ¿están (también) actualizados?

Si la validación de DNSSEC está habilitada o planificada en su sistema:

- Tener un plan para participar en el traspaso de la KSK.
- Conocer fechas, síntomas y soluciones.

Cómo actualizar su sistema

Si su software admite actualizaciones automáticas de los anclajes de confianza de las DNSSEC (RFC 5011):

- La KSK se actualizará automáticamente en el momento adecuado.
- No es necesario llevar a cabo ninguna acción adicional.
  - Los dispositivos que están fuera de línea durante el traspaso tendrán que actualizarse de forma manual si vuelven a estar en línea tras la finalización del traspaso.

Si su software no admite actualizaciones automáticas de los anclajes de confianza de las DNSSEC (RFC 5011) o no está configurado para utilizarlo:

- El archivo del anclaje de confianza del software debe actualizarse en forma manual.
- Obtenga la nueva KSK de la zona raíz aquí:

Anclajes de la raíz ▶

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

Recursos

KSK-2017 en un registro de recurso DNSKEY

- **El registro de recurso DNSKEY será:**

```
. IN DNSKEY  257 3 8
 AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3
    +/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv
    ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF
    0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e
    oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd
    RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN
    R1AkUTV74bU=
```

"Raíz"

Nota: se tomaron algunas licencias de formato a los fines de la presentación

Reconocimiento de la KSK-2017

- **La etiqueta clave de la KSK-2017 es**

  20326

- **El registro del recurso del Firmante de Delegación (DS) para la KSK-2017 es**

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

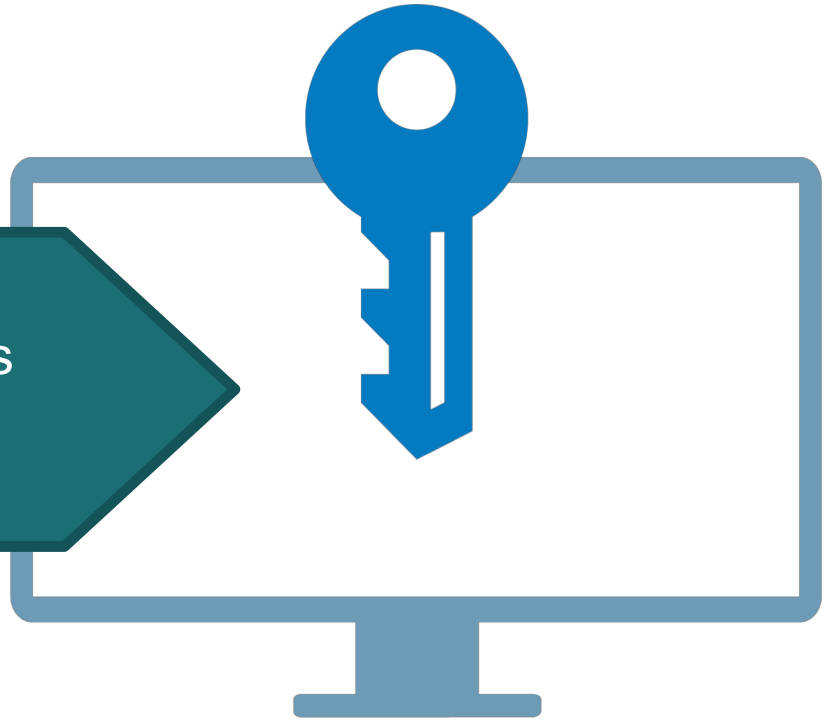
"Raíz"

Nota: se tomaron algunas licencias de formato a los fines de la presentación

Verifique que sus sistemas estén listos

La ICANN ofrece un **banco de pruebas** para que los operadores o toda parte interesada confirmen que sus sistemas manejan el proceso actualizado automáticamente de manera correcta.

Visite la siguiente página para asegurarse de que sus sistemas están listos:
go.icann.org/KSKtest



Si la validación de las DNSSEC falla después del cambio de clave

Detenga los tickets

Está bien desactivar la validación de las DNSSEC mientras lo soluciona (¡pero recuerde volver a activarla!).

Depuración

Si el problema es el anclaje de confianza, determine por qué no es correcto.

- ¿Falló el RFC 5011? ¿Las herramientas de configuración no actualizaron la clave?
- Si el problema está relacionado con la fragmentación, asegúrese de que el TPC esté habilitado y/o realice otros ajustes de transporte.

Compruebe la recuperación

Asegúrese de que se apliquen las correcciones.

Para más información

Participe en la conversación en línea

- Utilice la etiqueta #KeyRoll
- Regístrese en la lista de correo electrónico **https://mm.icann.org/listinfo/ksk-rollover**

Envíe una pregunta por correo electrónico a globalsupport@icann.org

- Asunto: “Traspaso de la KSK”

Participe en un evento

- Visite **https://features.icann.org/calendar** para enterarse de las próximas presentaciones sobre el traspaso de la KSK en su región

Ver más información

https://icann.org/kskroll

Participen en la ICANN – ¡Gracias! ¿Preguntas?

One World, One Internet

Visítenos en **icann.org**

- @icann
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- slideshare/icannpresentations
- soundcloud/icann