Plan de traspaso de la clave para la firma de la llave de la Zona Raíz

Informe preliminar del Equipo de Diseño, actualizado el 4 de agosto de 2015

1 Descripción general

La ICANN está preparando un plan para llevar a cabo un traspaso de la clave para la firma de la llave (KSK) de las DNSSEC de la Zona Raíz. La operación de traspaso está a cargo de la ICANN, en su función como Operador de las funciones de la IANA y en cooperación con otros socios de Gestión de la Zona Raíz (RZM). Los socios son Verisign, como Encargado de la Zona Raíz, y la Administración Nacional de Telecomunicaciones e Información (NTIA) del Departamento de Comercio de los Estados Unidos, como Gestor de la Zona Raíz.[1]

El cambio de la clave para la firma de la llave de la Zona Raíz refiere al cambio de la clave que se ha utilizado desde 2010, cuando la Zona Raíz se firmó por primera vez de acuerdo con la definición de las Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC)[2]. El cambio de la clave implica la generación de un componente secreto criptográfico nuevo y la distribución de un componente público nuevo. La distribución adecuada del componente público nuevo es el aspecto más crítico de la operación de traspaso de la clave.

El presente documento está disponible para Comentario Público y es un informe preliminar de las deliberaciones de un Equipo de Diseño que está formado por un panel de expertos voluntarios en DNS y DNSSEC, junto con los socios de Gestión de la Zona Raíz. La condición del presente documento es preliminar, será enmendado con los aportes de la comunidad de Internet durante el Comentario Público abierto de la ICANN y posteriores deliberaciones. Se emitirá un informe final tras la serie de debates que tendrá lugar más adelante.

2 Índice

[1] Este plan preliminar se elabora a partir de y en reconocimiento de la estructura de gestión de la zona raíz actual tal cual lo indicado en el contrato de funciones de la IANA y el Acuerdo de Cooperación entre la NTIA y Verisign. El Equipo de Diseño y los socios de RZM reconocen que los esfuerzos en curso para la transición de la custodia de la IANA pueden tener implicancias para el plan de traspaso de KSK y la participación de la NTIA en cualquier proceso futuro. Sin embargo, los detalles técnicos y las consideraciones dependen en su mayor parte del esfuerzo de transición y de su resultado final.

[2] Véase RFC 4033, RFC 4034 y RFC 4035.

3 Resumen Ejecutivo

La ICANN, como Operador de las funciones de la IANA, en colaboración con Verisign, como Encargado de la Zona Raíz, y la Administración Nacional de Telecomunicaciones e Información (NTIA) del Departamento de Comercio de los Estados Unidos, como Gestor de la Zona Raíz, conocidos como socios de Gestión de la Zona Raíz (RZM) han perseguido la elaboración de un plan para cambiar la Clave para la firma de la llave de la zona raíz (KSK).

Según las DNSSEC, la KSK de la Zona Raíz se utiliza para firmar el conjunto de registros de recursos DNSKEY de la Zona Raíz. Ese conjunto incluye la Clave para la firma de la Zona (ZSK), que se utiliza para firmar todos los demás conjuntos de registros de recursos (RRsets) en la Zona Raíz. El cambio de la clave para la firma de la llave de la Zona Raíz refiere al cambio de la clave que se ha utilizado desde 2010 (cuando la Zona Raíz se firmó por primera vez de acuerdo con la definición de las DNSSEC). El cambio de la clave implica la generación de un componente secreto criptográfico nuevo y la distribución de un componente público nuevo. La distribución adecuada del componente público nuevo es el aspecto más crítico del traspaso de la clave.

En diciembre de 2014, la ICANN solicitó que voluntarios de la comunidad participaran con los socios de RZM en un Equipo de Diseño para elaborar el plan de traspaso de la clave para la firma de la llave de la zona raíz, como se presenta en este documento. Los resultados de este trabajo fueron un conjunto integral de recomendaciones técnicas y operativas, cuya intención era orientar a los socios de RZM en la elaboración de un plan de implementación detallado para llevar a cabo el primer traspaso de la clave para la firma de la llave de la zona raíz. Este documento deberá pasar por etapas de revisión como un plan preliminar orientado a proporcionar dichos resultados.

3.1 Terminología del Sistema de Nombres de Dominio

Este documento se relaciona con los detalles técnicos sobre el DNS y las DNSSEC. A fin de que ya estén disponibles las definiciones de los términos relacionados con las DNSSEC (jerga), en Tabla 1 a continuación se incluyen definiciones de algunos términos relevantes.

Término	Abreviatura	Explicación
Conjunto de registros de recursos	RRSet	Una unidad de datos almacenada en el DNS, la unidad más pequeña que una clave de DNSSEC puede firmar.
Clave para la firma de la llave de la zona raíz	KSK	Un par de claves público-privadas[3] cuya función es producir una firma verificable del conjunto de claves que están en uso en la zona del DNS. Esta función es especial ya que las DNSSEC requieren que este tipo de clave pública se distribuya de forma externa al protocolo de DNS.
Clave para la firma de la zona	ZSK	Un par de claves público-privadas cuya función es producir firmas para todos los demás conjuntos de datos en una zona del DNS. Esta clave no se distribuye fuera del protocolo del DNS.
DNSKEY RRset		El conjunto de claves que se utiliza en una zona, incluso los roles de las KSK y ZSK, un conjunto de registros de recursos de DNSKEY.
Traspaso de clave		El acto de cambiar de una clave criptográfica a otra de forma ordenada.
Validador (DNSSEC)		Software que realiza comprobaciones de seguridad en las respuestas de DNSSEC, incluso la verificación de firmas en los datos como un solo paso.

[3] Ferguson, Niels; Schneier, Bruce (2003). *Practical Cryptography* (Criptografía práctica). Wiley. ISBN 0-471-22357-3.

Término	Abreviatura	Explicación
Anclajes de confianza		Una KSK pública almacenada en la que un validador confía plenamente.
Actualizaciones automáticas de los anclajes de confianza de DNSSEC	RFC 5011	Un método para actualizar de forma automática los anclajes de confianza en un validador.
Doble firma		La inclusión de dos firmas para un RRset, en general, la clave antigua y la nueva involucradas en un traspaso. Comúnmente, solo una firma es suficiente para un RRset.
Comité Asesor del Sistema de Servidores Raíz	RSSAC	Conformado según los estatutos de la ICANN, proporciona asesoramiento sobre el Sistema de servidor raíz a la comunidad de la ICANN.
Mecanismos de extensión para el DNS	EDNS o EDNS(0)	Actualmente se definen en RFC 6891, proporcionan un medio de extensión o ampliación del formato de protocolo DNS original. EDNS(0) refiere al primer conjunto de extensiones.
Registro de recursos del Firmante de Delegación	DS	El registro de DNSSEC indica la KSK que una subdelegación tiene en uso (o para la Zona Raíz, la KSK de un dominio de alto nivel).
Respuesta negativa	NSEC o NSEC3	Los registros de recursos definidos por DNSSEC que se utilizan para indicar que no existen datos para la pregunta que se formuló.
Declaración de Prácticas de Extensiones de Seguridad para el Sistema de Nombres de Dominio	DPS	Un documento que describe los aspectos específicos del procesamiento de DNSSEC para una zona.

Término	Abreviatura	Explicación
Ceremonias de clave		Eventos en los que se utiliza la clave privada, dentro de un Módulo de Seguridad de Hardware, para generar firmas. Se utiliza un proceso formal cuando hay testigos que desean observar las prácticas.

Tabla 1. Terminología sobre DNS y DNSSEC

3.2 Otros términos de seguridad

Término	Abreviatura	Explicación
OpenPGP	OpenPGP	Un medio para gestionar las claves público-privadas. RFC 4880: *Formato de mensaje OpenPGP*
Estándar de sintaxis de mensajes criptográficos	PKCS#7	RFC 2315: *PKCS #7: Sintaxis de mensajes criptográficos, versión 1.5*
El directorio: marcos de clave pública y certificados de atributos	X.509	El estándar del Sector de Normalización de Telecomunicaciones de la Unión Internacional de Telecomunicaciones (ITU-T) para gestionar las claves público-privadas. Recomendación ITU-T X.509 | ISO/IEC 9594-8
Solicitud para la firma de la llave de la zona raíz	KSR	Una estructura de datos que contiene solicitudes de firmas para claves, en particular conjuntos DNSKEY que debe firmar la KSK.
Respuesta de clave firmada	SKR	Una estructura de datos que contiene firmas generadas por claves privadas, en particular firmas KSK para conjuntos DNSKEY.

Tabla 2. Otros términos de seguridad

3.3 Otros términos de red

Se utilizan algunos otros términos que pueden requerir una definición para la mejor comprensión del público en general.

Término	Abreviatura	Explicación
Protocolo de Nivel de Transporte	UDP	Un protocolo de transporte del mejor esfuerzo y libre de contexto para enviar datos mediante Internet.
Protocolo de Control de Transmisión	TCP	Un protocolo de transporte con orden de octetos garantizado y orientado a la conexión para enviar datos mediante Internet.
Unidad de transmisión máxima	MTU	La cantidad máxima de octetos que pueden contener los datos que se envían a una porción de Internet. La ruta MTU refiere a la MTU más baja de todas las porciones que se utilizan en un recorrido de punto a punto en Internet.

Tabla 3. Otros términos de red

3.4 Resumen de Recomendaciones

Recomendación 1: El traspaso de la clave para la firma de la llave de la zona raíz debe seguir los procedimientos que se describen en RFC 5011 para actualizar los anclajes de confianza durante el traspaso de KSK.

Recomendación 2: La ICANN debe identificar los proveedores de software de DNS clave y trabajar con ellos en la formalización de los procesos para garantizar que la distribución de los anclajes de confianza a través de los canales específicos de los proveedores sea sólida y segura.

Recomendación 3: La ICANN debe identificar los integradores de sistemas de DNS clave y trabajar con ellos en la formalización de los procesos para garantizar que la distribución de los anclajes de confianza a través de los canales específicos de los integradores sea sólida y segura.

Recomendación 4: La ICANN debe adoptar un rol activo en la promoción de autenticación adecuada de anclaje de confianza de la Zona Raíz, que incluya una forma de destacar la información que se publica en el sitio web de la IANA de la ICANN.

Recomendación 5: El traspaso de la clave para la firma de la llave de la zona raíz no requiere cambios importantes a la gestión de KSK y procesos de uso

existentes para mantener los estándares altos de transparencia a los que se los asocia.

Recomendación 6: Todos los cambios que se realicen en los conjuntos RRset DNSKEY de la Zona Raíz deben estar alineados con espacios de 10 días que se describen en la DPS del operador de KSK.

Recomendación 7: Se debe mantener el algoritmo existente y el tamaño de la clave para la KSK entrante para el primer traspaso de la clave para la firma de la llave de la zona raíz.

Recomendación 8: La elección del algoritmo y el tamaño de clave deberán revisarse en el futuro, para los subsiguientes traspasos de claves para la firma de la llave de la zona raíz.

Recomendación 9: La ICANN, en cooperación con los socios de RZM, debe diseñar y ejecutar un plan de comunicaciones para generar conciencia sobre el traspaso de la clave para la firma de la llave de la zona raíz, que incluya la difusión a la comunidad técnica global mediante reuniones técnicas adecuadas y "socios de canal" como los que se definen en el presente documento.

Recomendación 10: La ICANN debe solicitar al Comité Asesor del Sistema de Servidores Raíz que coordine una revisión del cronograma detallado para el período de traspaso de KSK antes de su publicación. Asimismo, debe incorporar las solicitudes razonables para modificar el cronograma ante la eventualidad de que el operador de servidor raíz identifique motivos operativos para hacerlo.

Recomendación 11: La ICANN debe coordinarse con el RSSAC y los socios de RZM a fin de garantizar la utilización de los canales de comunicaciones en tiempo real para generar conciencia operativa sobre el sistema de servidor raíz en cada cambio de la Zona Raíz que implique la adición o remoción de una KSK.

Recomendación 12: La ICANN debe coordinarse con el RSSAC para solicitar que los operadores de servidor raíz realicen una recopilación de datos que brindará información a los análisis subsiguientes y permitirá caracterizar el impacto operativo del traspaso de la KSK. Además, deberán solicitar que los planes y productos de dicha recopilación de datos estén disponibles para el análisis de terceros.

Recomendación 13: Los socios de RZM deben garantizar que cualquier aumento del tamaño de la clave para la firma de la zona raíz que se realice a futuro se coordinará cuidadosamente con otros traspasos de KSK, de modo que no se lleven a cabo los dos ejercicios de manera simultánea.

Recomendación 14: Para reducir el tiempo de recuperación debido a dificultades que involucren a la KSK entrante, se generará un SKR generado solo por la KSK titular en paralelo con el SKR generado por la KSK entrante.

Recomendación 15: Los socios de RZM deben elaborar y documentar el proceso de utilización de la KSK titular generada por SKR.

3.5 Destinatarios

El presente documento está destinado a una audiencia técnica, en especial, a una audiencia familiarizada con los protocolos de DNS y DNSSEC, con los aspectos operativos del DNS y con los procesos asociados con el uso de DNSSEC en la Zona Raíz.

3.6 Alcance del documento

El presente documento tiene como objetivo dar un marco y proporcionar una serie de recomendaciones que guiarán a los socios de RZM en el desarrollo de un plan de implementación detallado para cambiar la clave para la firma de la llave de la zona raíz.

4 Historia abreviada

4.1 Desarrollo de las DNSSEC en la Zona Raíz

En 2009, los socios de RZM colaboraron[4] para implementar Extensiones de Seguridad del Sistema de Nombres de Dominio en la Zona Raíz, lo que culminó con la primera publicación de una Zona Raíz firmada y validable en el mes de julio de 2010. La KSK de la Zona Raíz actualmente en uso fue generada en la primera ceremonia de KSK que se llevó a cabo en la instalación en la cual se administra la clave (KMF), a cargo de la ICANN en Culpeper, Virginia, Estados Unidos. Los materiales clave se transportaron posteriormente a una segunda KMF de la ICANN en El Segundo, California, Estados Unidos y, luego de verificar que se hubieran transportado de forma segura, se publicó la porción pública de la KSK en la Zona Raíz y en los anclajes de confianza.

[4] En http://www.root-dnssec.org/ se publican los detalles de la implementación de DNSSEC en la Zona Raíz.

Los requisitos para generar y mantener la KSK de la Zona Raíz, así como las respectivas responsabilidades de cada socio de RZM, fueron especificados por la NTIA[5]. Los procedimientos a partir de los cuales el Encargado de la Zona Raíz y el Operador de las funciones de la IANA cumplen con estos requisitos se publicaron en Declaraciones de Prácticas (DPS) y de Política de DNSSEC independientes[6].

El Contrato de funciones de la IANA entre la NTIA y la ICANN se modificó en julio de 2010 para incorporar las responsabilidades asociadas con la gestión de KSK de la Zona Raíz, así como también aquellos requisitos que se habían aplicado en posteriores revisiones de aquel contrato[7]. El Acuerdo de Cooperación entre la NTIA y Verisign también se enmendó en julio de 2010 a fin de incluir las responsabilidades del operador de ZSK de la Zona Raíz de Verisign.[8]

El Contrato de funciones de la IANA requiere que la ICANN lleve a cabo un traspaso de KSK de la Zona Raíz, aunque no determina un período detallado ni un plan de implementación. La Declaración de Prácticas del operador de KSK de la Zona Raíz contiene esta declaración y establece el requisito de traspaso en la Sección 6.5:

“Toda KSK de la Zona Raíz realizará un traspaso mediante una ceremonia de clave según lo requerido por cronograma o cada cinco años de operación”.

4.2 Comentario público sobre el traspaso de la clave para la firma de la llave de la Zona Raíz

El 8 de marzo de 2013, la ICANN abrió un período de Comentario Público en busca de comentarios sobre la ejecución de un traspaso de KSK de la Zona Raíz[9]. Respondieron seis organizaciones y 15 personas. En el resumen de las respuestas[10], la ICANN identificó siete recomendaciones para que los socios de RZM consideren:

1. Se debe establecer una serie de pruebas y mediciones, con un banco de pruebas, antes de embarcarse en un traspaso de KSK, según se describe en

[5] "Testing and Implementation Requirements for the Initial Deployment of DNSSEC in the Authoritative Root Zone" (Requisitos de prueba e implementación para la implementación inicial de DNSSEC en la Zona Raíz acreditada), 29 de octubre de 2009, http://www.ntia.doc.gov/files/ntia/publications/dnssec_requirements_102909.pdf
[6] https://www.iana.org/dnssec, https://www.verisigninc.com/en_US/repository/index.xhtml
[7] http://www.ntia.doc.gov/page/iana-functions-purchase-order
[8] http://www.ntia.doc.gov/files/ntia/publications/amendment31_07062010.pdf
[9] https://www.icann.org/public-comments/root-zone-consultation-2013-03-08-en
[10] https://www.icann.org/en/system/files/files/report-comments-root-zone-consultation-08apr14-en.pdf

RFC 5011. Se deben establecer líneas de comunicación durante las fases y métodos de prueba para garantizar el éxito de la evaluación elaborada.
2. El traspaso de KSK debe llevarse a cabo en cuanto sea factible, poniendo énfasis en la preparación.
3. Las mediciones y la supervisión son los modos clave que se destacan para medir el impacto [técnico y de usuario final] de un traspaso de KSK, en caso de que debiera implementarse uno.
4. El traspaso de KSK debe realizarse periódicamente.
5. Los grupos de partes interesadas múltiples y diversos deben recibir notificaciones públicas sobre los eventos de traspaso de KSK con mucha antelación.
6. Es necesario seguir investigando la estabilidad operativa, los traspasos de KSK repetitivos y [la probabilidad y el impacto de] el incumplimiento de RFC 5011.

4.3 Debate preliminar sobre el traspaso de KSK de la Zona Raíz en 2013

Los socios de RZM acordaron una reunión a fines de julio de 2013 para discutir las opciones de cambio de KSK de la Zona Raíz. El equipo identificó la necesidad de contar con un procedimiento de traspaso clave que se llevaría a cabo en distintos pasos durante un período conservador. También identificó los beneficios de un amplio alcance a la comunidad y la noción de un cronograma de traspaso de RFC 5011 modificado con revocación demorada. Estos principios de alto nivel se presentaron en la reunión N.° 87 del IETF del grupo de trabajo sobre Operaciones del DNS (DNSOP) perteneciente al IETF[11].

4.4 Asesoramiento del SSAC sobre sustitución de claves DNSSEC en la zona raíz

En noviembre de 2013, el Comité Asesor de Seguridad y Estabilidad (SSAC) de la ICANN publicó el informe SAC063[12], acerca del traspaso de KSK. El informe abarcó los riesgos implicados y el estado de la base de códigos en ese período (las implementaciones del DNS de código abierto, en particular). Asimismo, el informe recomendó una acción de comunicación para publicar la implementación de la clave de KSK de la Zona Raíz; fomentó la realización de pruebas para recopilar y analizar los comportamientos del resolutor, la creación de métricas para lo que serían niveles aceptables de “quiebre” en una implementación de la llave de la raíz, definición de medidas de reversión en caso de “quiebre” excesivo y la recopilación de información para futuros ejercicios de cambio de clave de esta naturaleza.

[11] http://www.ietf.org/proceedings/87/slides/slides-87-dnsop-6.pdf
[12] https://www.icann.org/en/system/files/files/sac-063-en.pdf

El informe del Comité Asesor de Seguridad y Estabilidad destacó tres temas que se analizarán más adelante. Primero, una estimación aproximada del 1,1 % de quienes confían en el DNS habilitado por DNSSEC puede sufrir un impacto negativo, incluso de un traspaso de KSK de la Zona Raíz bien gestionado. Segundo, el estado de respaldo para las actualizaciones automáticas del anclaje de confianza de DNSSEC, también conocido como RFC 5011, está presente pero es impredecible. Y, tercero, se ha creído que el tamaño de las respuestas de DNS puede representar una inquietud cuando se relaciona con la ocurrencia de fragmentación y reversión de los paquetes de UDP subyacentes a las consultas de TCP.

4.5 La ICANN reúne un Equipo de Diseño del Traspaso de la KSK de la Zona Raíz

En diciembre de 2014, la ICANN solicitó que voluntarios de la comunidad participaran con los socios de RZM en un Equipo de Diseño para elaborar el plan de traspaso de la clave para la firma de la llave de la zona raíz, como se presenta en este documento.

5 Descripción de alto nivel del cambio de KSK

El plan derivado en julio de 2013, que no está muy lejos de los planes de cambio de cualquier otra KSK, sigue estos pasos:

1) Se genera un par de claves KSK entrantes (pública y privada).

2) La clave pública KSK entrante se coloca en la Zona Raíz o se pone a disponibilidad de los usuarios de confianza.

3) En una desviación de otras zonas, la nueva clave pública KSK de la Zona Raíz se encuentra en un estado de aceptación por parte de aquellos que estén preocupados de que sea, en efecto, la próxima KSK. Además de ser aceptada de forma pasiva, la nueva clave pública KSK de la Zona Raíz está disponible en distintos medios electrónicos y no electrónicos para permitir que los operadores de resolutores y los desarrolladores que tienen servidores que no admiten RFC 5011 tengan tiempo para incluir el anclaje de confianza nuevo en sus sistemas y productos. (Para “otras zonas”, este paso se reemplaza al informar al titular del registro DS que hay una KSK entrante.)

4) El proceso de firma pasa de utilizar la clave privada KSK titular a utilizar la clave privada KSK entrante.

5) El KSK entrante ahora se encuentra en un estado de transición dado que las firmas generadas por la KSK titular caducan o desaparecen de la vista operativa.

6) La clave pública KSK titular se elimina de la Zona Raíz (sin revocación).

7) En otra desviación de las operaciones normales, la KSK de la Zona Raíz titular se vuelve a ingresar para marcarla como revocada de acuerdo con las pautas de RFC 5011. Este paso independiente está diseñado para incorporar las operaciones de ZSK, que incluyen cambios de la clave sin respuestas de DNS sobredimensionadas para el conjunto de claves completo de la Zona Raíz.

6 Enfoque del Equipo de Diseño

El Equipo de Diseño consideró varios aspectos de un traspaso de KSK de la Zona Raíz y elaboró recomendaciones para cada área de estudio a fin de que los socios de la Zona Raíz puedan guiar el desarrollo de un plan de implementación.

- Consideraciones operativas: el impacto sobre los usuarios finales de Internet y los operadores de los sistemas de DNS, así como los servicios utilizados por los usuarios finales.

- Consideraciones de protocolo: la medida en que los elementos de protocolo documentados y existentes son suficientes para incorporar un traspaso de KSK de la Zona Raíz.

- Impacto sobre la gestión de KSK de la Zona Raíz: el impacto sobre los procesos implicados en la Gestión de la Zona Raíz por parte del operador de funciones de la IANA.

- Consideraciones criptográficas: garantizar que la totalidad del sistema tenga suficiente fuerza criptográfica.

- Comunicación y coordinación con todas las partes involucradas.

Cada una de estas áreas se analiza de forma individual en las secciones subsiguientes. También se proporcionó una solución detallada de traspaso técnico para ilustrar la manera en que se pueden seguir las recomendaciones, y como un punto de partida para los socios de RZM a medida que concluyan su plan de implementación.

6.1 Consideraciones operativas

Se anticipa que el impacto sobre los usuarios finales de Internet y los operadores de sistemas de DNS tendrá lugar durante dos de los pasos antes descritos. Cuando se

agregue la clave pública KSK entrante a la Zona Raíz, crecerá el tamaño de la respuesta para el conjunto DNSKEY raíz. Cuando la clave privada KSK titular ya no genere firmas, la validación con esa clave pública dejará de funcionar de la forma esperada.

Con una respuesta a DNSKEY más grande, es posible que la fragmentación de los paquetes de UDP ocurra con resultados levemente diferentes en IPv4 y en IPv6. En efecto, ya existen componentes de Internet que consideran a los fragmentos como anomalías y los filtran. Para el DNS, que no mantiene un estado respecto del envío de respuestas, esto significa que un cliente puede no recibir una respuesta esperada. También existe la posibilidad de una respuesta de UDP mayor que exceda el tamaño del búfer de cargas del DNS especificado en la consulta, lo que incrementa el nivel de respuestas truncadas y la posterior reformulación de consultas con TCP.

Cuando la KSK titular ya no firma la clave para la firma de la zona, con la implicancia de que la KSK entrante genera firmas, un validador de DNSSEC con solo la KSK titular configurada como anclaje de confianza dejará de validar las respuestas de DNSSEC firmadas. El validador se “cerrará al fallar”, lo que significa que todas las respuestas de DNS firmadas se considerarán inválidas.

Un cliente final que utilice resolutores de validación de forma exclusiva que no pueden tomar la KSK entrante o bien no pueden recibir respuestas más grandes durante el proceso de cambio de clave no serán capaces de validar ninguna respuesta de DNS firmada. Para el cliente final, esto aparecerá como un corte de Internet, en el que no se pueden resolver los nombres de dominio. Cuando ya han ocurrido situaciones semejantes, el efecto secundario es el aumento de las llamadas a los centros de atención al cliente, lo que impone cargas adicionales en los roles de gestión operativa y atención al cliente del ISP.

La ICANN debe planificar las comunicaciones, para que se coordinen con la introducción de la KSK entrante, así como con el cambio de la KSK titular a la entrante para la generación de firmas (véase la Recomendación 8).

6.2 Consideraciones de protocolo

6.2.1 Configuración del anclaje de confianza de la Zona Raíz

Hay dos clases de configuraciones de anclaje de confianza para tener en cuenta:

- Anclajes de confianza en resolutores de validación en línea
- Anclajes de confianza en dispositivos/sistemas que están fuera de línea durante el traspaso y se conectan más adelante

Los resolutores de validación en línea pueden utilizar *Actualizaciones automáticas de los anclajes de confianza de seguridad del Sistema de Nombres de Dominio (DNSSEC)* como se describen en RFC 5011, si el software de DNS utilizado admite este mecanismo y está configurado para utilizarlo en la actualización de la Clave para la firma de la llave de la Zona Raíz.

Los resolutores de validación en línea que no pueden o no desean utilizar las Actualizaciones automáticas de los anclajes de confianza de seguridad del DNS deberán actualizar de forma manual durante el traspaso de la KSK. La actualización manual debe respetar los tiempos del mecanismo RFC 5011 – el anclaje de confianza nuevo debe agregarse a la configuración del resolutor de validación en el período PUBLISH del traspaso (véase la Sección 11 para obtener más detalles) – y el anclaje de confianza titular no debe eliminarse antes de que la Zona Raíz esté firmada con la KSK de la Zona Raíz entrante. Más aún, para que la práctica operativa sea cautelosa, el anclaje de confianza titular no debe eliminarse antes de la revocación de la KSK de la Zona Raíz titular. Los mecanismos para recuperar el anclaje de confianza nuevo son iguales para los dispositivos fuera de línea y se describen a continuación.

Recomendación 1: El traspaso de la clave para la firma de la llave de la zona raíz debe seguir los procedimientos que se describen en RFC 5011 para actualizar los anclajes de confianza durante el traspaso de KSK.

Los dispositivos que están fuera de línea durante el traspaso de KSK de la Zona Raíz tendrán que actualizarse de forma manual si vuelven a estar en línea tras la finalización del traspaso. En esencia, es necesario arrancar estos dispositivos como si recién se instalaran.

Generalmente, el proceso por el cual cualquier dispositivo se prepara para poder llevar a cabo la validación de DNSSEC debe seguir un enfoque que reduce las posibilidades de utilizar un anclaje de confianza incorrecto. Actualmente, en un Borrador de Internet, titulado "*DNSSEC Trust Anchor Publication for the Root Zone*" (Publicación de anclajes de confianza de DNSSEC para la Zona Raíz) en el IETF[13], circulan consejos generales para estos dispositivos, pero es necesario seguir analizando el tema para llegar a un documento consensuado estable que proporcione asesoramiento a los implementadores.

El Equipo de Diseño respalda el debate de la comunidad y la revisión del Borrador de Internet en el IETF, con el objetivo de publicar una especificación estable, revisada por los pares en la serie de documentos RFC.

[13] http://tools.ietf.org/html/draft-jabley-dnsop-validator-bootstrap-00

Existen varios casos de uso sobre recuperación de anclajes de confianza actualizados que exploraremos brevemente a continuación.

6.2.1.1 Más discusión sobre RFC 5011

En el texto anterior se menciona a los resolutores “que no pueden o no desean” confiar en el enfoque de RFC 5011. Esta sección pretende proporcionar cierto contexto sobre esta fase.

El espíritu del temporizador agregar/retener de RFC 5011 es importante. El temporizador se incluye para evitar que una clave con presentación falsa gane aceptación. En otras palabras, si una entidad desea presentar una KSK falsa, podrían tener éxito en la publicación de la clave. En ese caso, la autoridad verdadera podrá presentar un descargo contra la clave falsa antes de que se genere confianza en ella.

La resistencia al RFC 5011 de los resolutores no se basa en las preguntas relacionadas con el diseño del mecanismo de actualización; por el contrario, tiene su origen en algunas realidades operativas. La gestión de configuración es una inquietud muy importante cuando se opera una flota de servidores y se confía en el “empuje hacia el exterior” de los archivos de configuración gestionados. El mecanismo de actualización de RFC 5011 va en contra de esto, con equipos de flotas configurados que aprenden datos nuevos y se desvían de la configuración gestionada de forma central.

Con esto en mente, los grandes operadores pondrán en práctica un proceso manual, que les permitirá usar varios mecanismos automatizados. Un sistema automatizado puede ser una herramienta que sigue el mecanismo de actualización de RFC 5011. En una encuesta informal breve, los grandes operadores señalaron que para establecer la confianza contarán con el veto de la KSK de la Zona Raíz nueva mediante algunas diversas formas, incluida la comunicación entre personas. Este es el motivo por el que se proponen alternativas a RFC 5011.

Cuando se indagó más en el funcionamiento de RFC 5011, se identificaron algunas brechas. La primera brecha alude a la verificación remota de un proceso de RFC 5011 exitoso. La segunda brecha alude a la capacidad de evaluar las implementaciones en pos del temporizador agregar/retener.

Lo que se necesita es un medio para que el código de confianza conozca los anclajes de confianza en uso en un resolutor. Dado el contexto de supervisión generalizada, la intención no es tener conocimiento de las capacidades y configuración de un resolutor específico, sino primero confirmar que el proceso de

RFC 5011 se siguió en su mayor parte y saber en qué momento es aceptable comprometerse con la KSK de la Zona Raíz.

Se identificó también la necesidad de acelerar la capacidad de realizar una prueba funcional, que muestre los pasos de RFC 5011 que están en curso sin adherirse a la necesidad de contar con un modelo de seguridad. En particular, las herramientas necesarias para anular el temporizador agregar/retener especificado a fin de permitir una configuración más breve durante la prueba. Lo deseable es proporcionar un mecanismo de "prueba segura" que garantice que no se utilice el temporizador agregar/retener en la producción. Esta es solo una sugerencia que está orientada a los desarrolladores de herramientas y a los proveedores de software de DNS.

6.2.1.2 Otros formatos de anclajes de confianza

Desde la firma inicial de la Zona Raíz, la ICANN ha puesto a disponibilidad el anclaje de confianza en formatos distintos al DNS en un sitio web[14]. Estos anclajes de confianza proporcionan un medio de ruta no crítica para distribuir y recibir el anclaje de confianza de la zona raíz, es decir, un medio fuera de las operaciones del DNS. (El sitio web no requiere acceso al DNS para obtener los archivos.) Gracias a la consideración de ruta no crítica, se pueden distribuir nuevos anclajes de confianza. En algún momento del futuro, es posible agregar anclajes de confianza a algoritmos criptográficos de DNSSEC diferentes[15] para enfatizar la necesidad de contar con capacidades nuevas. Esto puede también ser un medio para componer resolutores con antelación ante la eventualidad de realizar un traspaso de emergencia.

6.2.1.3 Proveedores de software de DNS

Los proveedores pueden incorporar anclajes de confianza a los paquetes de software de DNS (como código abierto o propietario/comercial). El proveedor de software deberá emitir una versión nueva del conjunto de anclaje de confianza para mantener el software actualizado.

Es importante que los anclajes de confianza que se distribuyen de esta forma sean auténticos y aprovechen todos los mecanismos de verificación existentes para garantizar la integridad del software en un sistema final. Los proveedores de software requieren un método sólido y eficiente para garantizar que los anclajes de confianza que distribuyen con su software sean auténticos, dado que el impacto de distribuir claves no auténticas es muy importante, en especial, si están firmados con

[14] https://www.iana.org/dnssec/files
[15] https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml#dns-sec-alg-numbers-1

claves de firma de código como parte de una estrategia de actualización de software del proveedor.

Recomendación 2: La ICANN debe identificar los proveedores de software de DNS clave y trabajar con ellos en la formalización de los procesos para garantizar que la distribución de los anclajes de confianza a través de los canales específicos de los proveedores sea sólida y segura.

6.2.1.4 Integradores de sistema

Un método de distribución de los anclajes de confianza de DNSSEC es a través de un integrador de sistemas, por ejemplo, un encargado de paquetes o un proveedor de sistemas operativos. En este caso, el integrador de sistema proporcionará paquetes actualizados para todas las copias de anclajes de confianza que haya en el sistema. Se están realizando algunos esfuerzos en varias distribuciones de Linux para proporcionar un paquete con una copia acreditada del anclaje de confianza.

Recomendación 3: La ICANN debe identificar los integradores de sistemas de DNS clave y trabajar con ellos en la formalización de los procesos para garantizar que la distribución de los anclajes de confianza a través de los canales específicos de los integradores sea sólida y segura.

6.2.1.5 Administradores de sistemas

Los administradores de sistemas pueden descargar los anclajes de confianza de DNSSEC de forma manual en el sitio web de la IANA de la ICANN, mientras instalan o descargan software. El Operador de las funciones de la IANA proporciona los anclajes de confianza de Zona Raíz actuales en un sitio web dedicado[16] para obtener información sobre DNSSEC en la Zona Raíz. La determinación de la autenticidad de los anclajes de confianza que se descargan es fundamental para establecer la confianza en las Extensiones de Seguridad del Sistema de Nombres de Dominio. Para respaldar la verificación de autenticidad de diversos tipos de firmas digitales en la forma de OpenPGP, también se publican PKCS#7 y un certificado X.509 que contiene la clave raíz, en el mismo sitio web dedicado.

Si bien la determinación de autenticidad es sumamente importante, se la suele ignorar y no especificar correctamente. Cuando los procesos para respaldar las pruebas de autenticidad se pusieron a disponibilidad para revisión pública, la cantidad de comentarios sustantivos que se recibió fue baja. Esto socava el esfuerzo de respaldar la autenticidad de forma correcta. Es posible que se necesite realizar una revisión adicional (con los cambios compatibles con sus versiones

[16] La lista se encuentra en https://www.iana.org/dnssec/files.

previas, según corresponda). Como se mencionó antes, el Equipo de Diseño respalda el debate y revisión de la comunidad sobre el Borrador de Internet titulado "*DNSSEC Trust Anchor Publication for the Root Zone*" (citado anteriormente) en el IETF, con el objetivo de publicar una especificación estable y revisada por los pares en las series de documentos RFC.

Más aún, las recuperaciones observadas de las firmas de autenticación y respaldo digital sugieren que unos pocos usuarios de confianza, si los hubiese, han estado usando las firmas digitales. La confianza no se gana solo con la provisión de firmas digitales, sino también con la promoción activa.

Recomendación 4: La ICANN debe adoptar un rol activo en la promoción de autenticación adecuada de anclaje de confianza de la Zona Raíz, que incluya una forma de destacar la información que se publica en el sitio web de la IANA de la ICANN.

6.3 Impacto sobre la gestión de KSK de la Zona Raíz

Como se describe en *DNSSEC Practice Statement for the Root Zone KSK Operator* (Declaración de Prácticas de DNSSEC para el Operador de KSK de la Zona Raíz), el operador de KSK de la Zona Raíz firma cada RRset DNSKEY adjunto a la Zona Raíz mediante un KSR provisto por dicho operador. El resultado es un SKR que contiene un conjunto de RRset DNSKEY firmado provisto al Encargado de la Zona Raíz.

Estos procesos están bien documentados y, en el caso de las acciones que se realizan durante las ceremonias de KSK, están sujetos a auditorías externas y observación extendida. El Equipo de Diseño considera que es muy ventajoso evitar cualquier cambio sustantivo en los procesos como resultado del cambio de la KSK, a fin de evitar la interrupción de un proceso que, en su forma actual, se comprende correctamente.

Recomendación 5: El traspaso de la clave para la firma de la llave de la zona raíz no requiere cambios importantes a los procesos existentes para mantener los estándares altos de transparencia a los que se asocia.

Cada KSR abarca un ciclo de tiempo de un trimestre calendario (tres meses o aproximadamente 90 días) y se divide en nueve espacios de diez días cada uno. Si el ciclo de tiempo supera los 90 días, el último espacio del ciclo se amplía para completar el período. Debido a esto, todos los cambios en el RRset DNSKEY de la Zona Raíz (por ejemplo adición o eliminación de claves según lo requerido por un

traspaso de clave) deben estar alineados con estos períodos de diez días para reducir al mínimo cualquier cambio sustantivo en los procesos que se utilizan para publicar una Zona Raíz firmada.

Recomendación 6: Todos los cambios que se realicen en los conjuntos RRset DNSKEY de la Zona Raíz deben estar alineados con espacios de 10 días que se describen en la DPS del operador de KSK.

Con los períodos estándar, el tamaño de respuesta del paquete RRset DNSKEY raíz aumenta con el primer y el último espacio en cada ciclo de tiempo. El primer espacio contiene la última ZSK publicada en el ciclo de tiempo anterior, mientras que el último espacio contiene la ZSK publicada antes en el próximo ciclo de tiempo.

Para reducir al mínimo la posibilidad de que surjan cuestiones relacionadas con los tamaños de respuestas de DNS más grandes, se recomienda programar un traspaso que pueda mantener el tamaño de respuesta de RRset DNSKEY lo más pequeño posible. Más adelante en este documento, se presenta un examen detallado de las cuestiones de tamaño de respuesta, con recomendaciones. También se incluye in cronograma de traspaso de KSK de la Zona Raíz elaborado a partir de las consideraciones antes mencionadas.

6.4 Consideraciones criptográficas

El Equipo de Diseño consideró la pregunta sobre si hubo razones lo suficientemente válidas como para considerar un cambio en el tamaño de la clave o en el algoritmo de la KSK. Una razón válida puede derivar de preguntas sobre la fuerza criptográfica del tamaño de la clave o el algoritmo seleccionados.

Con la publicación inicial de SP 800-57, parte 1 (*Recommendation for Key Management* (Recomendaciones para la gestión de claves)) en 2005, el Instituto Nacional de Normas y Tecnología (NIST) de Estados Unidos anunció la intención de aumentar las fuerzas criptográficas mínimas. Sin embargo, en los cinco años que siguieron entre la fecha de publicación y la fecha de finalización propuesta, las técnicas de Factoring no han progresado con la rapidez anticipada. No existe nada que sugiera la urgencia de utilizar longitudes de clave más extensas para la KSK de la Zona Raíz.

6.4.1 Criptografía de campo finita

La clave RSA asimétrica de 2048 bits se considera el equivalente a la clave simétrica de 103 bits en el Informe Anual de 2012 de ECRYPT II sobre Algoritmos y

Tamaños de Claves[17]. El mismo informe recomienda el uso de al menos 96 bits de seguridad para lograr una protección de aproximadamente diez años. Las *Recommendation for Key Management-Part 1: General (Revision 3)*[18] (Recomendaciones para la gestión de claves, parte 1: General (Revisión 3)) consideran que la clave RSA de 2048 bits es el equivalente de 112 bits de seguridad y que esta fuerza es aceptable para utilizar en el período que abarca desde 2014 a 2030. La French Agence nationale de la sécurité des systèmes d'information (ANSSI) *Référentiel Général de Sécurité*[19] también considera que la clave RSA de 2048 bits es segura para utilizar hasta 2030.

El contenido firmado en la Zona Raíz suele ser transitorio dado que los períodos de firma DNSKEY se miden en días (aprox. 15 días) y el Equipo de Diseño cree que la clave RSA de 2048 bits estaría segura por cinco años más, a menos que haya un importante avance tecnológico en el área de factorización de números enteros grandes.

6.4.2 Criptografía de curva elíptica

Otra opción de algoritmo disponible para DNSSEC es el algoritmo de firma digital de curva elíptica (ECDSA) que se define en RFC 6605[20]. El ECDSA tiene algunas propiedades que lo hacen deseable para utilizar como algoritmo para la clave para la firma de la llave de la zona raíz. Las claves son mucho más pequeñas al tiempo que mantienen la fuerza de las claves RSA. Las estimaciones actuales son que el ECDSA con curva P-256 tiene una fuerza equivalente aproximada a RSA con claves de 3072 bits (NIST) o de 3248 bits (ECRYPT II). No obstante, la estandarización del algoritmo para utilizarse solo en DNSSEC es bastante reciente —RFC 6605 se publicó en 2012— y las mediciones que se describen más adelante en este documento han observado que el respaldo a ECDSA en los validadores no está tan generalizado como el respaldo a RSA (véase Sección 7: Consideraciones operativas).

El Grupo de Investigación del Foro Crypto (CFRG) del IETF también trabaja en un nuevo documento RFC *"Elliptic Curves for Security"* (Curvas elípticas para seguridad) que agrega nuevas curvas elípticas de seguridad y también expone algunas inquietudes de la comunidad Crypto sobre la generación y posibles debilidades de las curvas que utiliza el ECDSA. Es recomendable permitir que el CFRG termine de trabajar en el documento antes de cambiar a un nuevo algoritmo de curva elíptica para firmar la Zona Raíz.

[17] http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf
[18] http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf
[19] http://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf
[20] https://tools.ietf.org/html/rfc6605

6.4.3 Conclusión

De acuerdo con la orientación antes presentada, el Equipo de Diseño no halló necesidad apremiante alguna para cambiar el algoritmo o el tamaño de la KSK de RSA de 2048 bits. El Equipo de Diseño también tomó conocimiento de una Implementación de resolutor de validación de DNS que requiere que la Zona Raíz esté firmada por todos los algoritmos que coinciden con los anclajes de confianza configurados, por ende, el traspaso a un algoritmo diferente demandará un enfoque distinto al del cambio de la KSK. Esto proporciona otra motivación práctica para evitar un cambio en el algoritmo en este momento. El Equipo de Diseño se comunicó con el proveedor por esta cuestión y el requisito del proveedor; la expectativa es que será distendido para los futuros traspasos de KSK no programados.

Por estos motivos, la KSK entrante para el primer traspaso de KSK deberá ser una clave RSA de 2048 bits, aunque será mejor considerar los cambios en el algoritmo o en la longitud de la clave en posteriores traspasos de KSK.

Recomendación 7: El Equipo de Diseño recomienda mantener el algoritmo existente y el tamaño de la clave para la KSK entrante para el primer traspaso de la clave para la firma de la llave de la zona raíz.

Recomendación 8: La elección del algoritmo y el tamaño de clave deberán revisarse en el futuro, para los subsiguientes traspasos de claves para la firma de la llave de la zona raíz.

6.5 Coordinación y comunicación

6.5.1 Coordinación con la comunidad técnica y los socios de canal

La ICANN debe elaborar y ejecutar un plan de comunicaciones para generar conciencia acerca del cambio de KSK de la Zona Raíz. La forma de generar conciencia es en foros técnicos, como aquellos en lo que se presentó la implementación original de DNSSEC en la Zona Raíz.

El siguiente término “Socios de canal” refiere a las organizaciones externas que facilitan el uso de DNSSEC de forma independiente a la gestión de la Zona Raíz. Estos socios “canalizan” el valor de firmar la Zona Raíz fuera de los socios de RZM hacia la Internet pública global.

Los Socios de canal se dividen en tres áreas generales. En el primer grupo están los facilitadores, quienes implementan el software de validación de DNSSEC y les interesa, entre otras cosas, la implementación de RFC 5011. En el segundo grupo se encuentran los distribuidores de software y sistemas que incluyen software de

validación de DNSSEC, principalmente interesados en la distribución de copias de la KSK de la Zona Raíz. En el tercer grupo se encuentran los operadores de los sistemas de validación de DNSSEC que utilizan la KSK de la Zona Raíz.

A fin de facilitar la comunicación, el Equipo de Diseño recomienda que para cada Socio de canal, de haber buena disposición, se conserve un archivo de contacto y se les envíe actualizaciones del cambio de la KSK. Esta lista de contacto no pretende ser exclusiva ni servir como vía de intercambio de materiales, por el contrario, la intención es que sea pública. Con ella se pretende proporcionar una muestra del conocimiento de los pasos necesarios para el cambio de la KSK de la Zona Raíz. La lista, sin embargo, debe permanecer cerrada para que los Socios de canal puedan gestionar el conocimiento de su información de contacto seleccionada.

Recomendación 9: La ICANN, en cooperación con los socios de RZM, debe diseñar y ejecutar un plan de comunicaciones para generar conciencia sobre el traspaso de la clave para la firma de la llave de la zona raíz, que incluya la difusión a la comunidad técnica global mediante reuniones técnicas adecuadas y Socios de canal como los que se definen en el presente documento.

6.5.2 Coordinación con operadores de servidor raíz

Todo cambio estructural en los contenidos de la Zona Raíz tiene el potencial de afectar el comportamiento operativo de los servidores raíz individuales. El aprovisionamiento inicial de “registro de pegado” de dirección IPv6 (AAAA) en la Zona Raíz y la posterior implementación de DNSSEC son ejemplos de cambios que se realizaron con consulta y estrecha coordinación con los operadores de servidor raíz, dado que dichos cambios impulsaron cambios en los patrones de consulta. Por lo tanto, la cautela con la infraestructura crítica establece un enfoque conservador hacia cualquier cambio ante la eventualidad de que existan consecuencias inesperadas que puedan afectar el desempeño del sistema de servidor raíz en su totalidad.

Los experimentos realizados como parte de la preparación del presente documento sugieren que un evento de traspaso de KSK no provocará efectos dañinos. Sin embargo, al igual que con los primeros ejemplos de cambio estructural antes mencionados, se recomienda un enfoque conservador.

El Equipo de Diseño sugiere que los operadores de servidor raíz individual puedan tratar los eventos particulares dentro del período de traspaso de KSK tal y como tratarían un evento operativo planificado e importante, con la emisión de notificaciones de estado y la coordinación con otros operadores de servidor raíz,

mediante los canales de tiempo real normales para estos eventos. Los eventos deberán incluir el período en torno a la adición de una KSK entrante nueva al RRSet DNSKEY adjunto a la Zona Raíz y a la eliminación de la KSK saliente del mismo RRSet.

El Equipo de Diseño recomienda que los canales de comunicación en tiempo real entre los operadores de servidor raíz individual y la ICANN, y la ICANN y otros socios de RZM sean semejantes a los que se aplican a los mismos eventos para garantizar la pronta identificación e intercambio de cualquier efecto esperado.

Los operadores de servidor raíz deberán revisar un cronograma detallado para el período de traspaso de KSK antes de su finalización y publicación, a fin de garantizar que este no entre en conflicto con otros planes que puedan reducir la capacidad de un operador de servidor raíz individual para proporcionar el nivel deseado de cobertura operativa. Se deberá intentar, por todos los medios, ajustar los tiempos del traspaso para evitar los conflictos operativos, siempre que sea factible.

Recomendación 10: La ICANN debe solicitar al Comité Asesor del Sistema de Servidores Raíz que coordine una revisión del cronograma detallado para el período de traspaso de KSK antes de su publicación. Asimismo, debe incorporar las solicitudes razonables para modificar el cronograma ante la eventualidad de que el operador de servidor raíz identifique motivos operativos para hacerlo.

Recomendación 11: La ICANN debe coordinarse con el RSSAC y los socios de RZM a fin de garantizar la utilización de los canales de comunicaciones en tiempo real para generar conciencia operativa sobre el sistema de servidor raíz en cada cambio de la Zona Raíz que implique la adición o remoción de una KSK.

La recopilación de datos que los operadores de servidor raíz llevan a cabo durante el curso del traspaso de KSK facilita la comprensión del impacto operativo de un traspaso de KSK sobre los validadores y los servidores raíz. Dado que el sistema de servidor raíz difiere en arquitectura y distribución en Internet, se entiende que las oportunidades de recopilación extensa de datos basados en el tiempo por parte de operadores de servidor raíz individual implicarán varias restricciones difíciles de caracterizar brevemente para el sistema como un todo. Se entiende también que ya existen capacidades de recopilación de datos de línea de base para satisfacer los requisitos tácticos de supervisar las condiciones de servicio en tiempo real, a medida que avanza el traspaso de KSK.

Cuando las Extensiones de Seguridad del Sistema de Nombres de Dominio se implementaron al principio en la Zona Raíz, se realizó un ejercicio de recopilación de datos importante. Los datos resultantes demostraron ser útiles en el análisis fuera de línea de la reacción de todo el DNS a los cambios estructurales que tenían lugar en la Zona Raíz, incluso del análisis de terceros, facilitado por DNS-OARC[21]. Para el primer traspaso de KSK se garantiza un ejercicio similar.

Recomendación 12: La ICANN debe coordinarse con el RSSAC para solicitar que los operadores de servidor raíz realicen una recopilación de datos que brindará información a los análisis subsiguientes y permitirá caracterizar el impacto operativo del traspaso de la KSK. Además, deberán solicitar que los planes y productos de dicha recopilación de datos estén disponibles para el análisis de terceros.

6.5.3 Coordinación entre el operador de KSK y el operador de ZSK

La responsabilidad por la gestión de la KSK y la ZSK de la Zona Raíz se asigna por separado al Operador de las funciones de la IANA y al Encargado de la Zona Raíz, respectivamente. Los dos roles se gestionan de forma independiente.

Actualmente, la ZSK de la Zona Raíz es una clave RSA de 1024 bits, como se especifica en la Declaración de Prácticas del Encargado de ZSK[22]. Es posible que el Encargado de la Zona Raíz aumente el tamaño de la clave de ZSK en el futuro.

La ZSK cambia cada 90 días y se espera que esto continúe así durante el período de traspaso de la KSK. Se espera que el período de traspaso de KSK supere los 90 días, por eso habrá períodos en los que el RRSet DNSKEY adjunto a la Zona Raíz podría contener cuatro claves, según el plan final.

El aumento del tamaño de la ZSK durante un evento de traspaso de clave puede iniciar un comportamiento diferente en los validadores durante una parte del período de traspaso de la KSK, ya que los tamaños de respuesta aumentarán con el tamaño de la ZSK. Esto puede complicar los intentos de identificación, comprensión y mitigación de cualquier problema operativo que pudiese surgir.

El presente documento no abarca las decisiones que se relacionan con el tamaño de la ZSK. Sin embargo, recomendamos que la ICANN se coordine con el Encargado de la Zona Raíz para garantizar que cualquier aumento del tamaño de la clave para la firma de la zona raíz que se realice a futuro se coordinará

[21] https://www.dns-oarc.net
[22] http://www.verisigninc.com/assets/dps-zsk-operator-1527.pdf

cuidadosamente con otros traspasos de KSK, de modo que no se lleven a cabo los dos ejercicios de manera simultánea.

Recomendación 13: Los socios de RZM deben garantizar que cualquier aumento del tamaño de la clave para la firma de la zona raíz que se realice a futuro se coordinará cuidadosamente con otros traspasos de KSK, de modo que no se lleven a cabo los dos ejercicios de manera simultánea.

7 Impacto sobre los resolutores de validación

7.1 Consideraciones sobre el tamaño de los paquetes

El DNS se define para operar en protocolos de transporte UDP y TCP. En el diseño del protocolo de DNS se prefiere UDP debido a los costos más bajos en comparación con TCP, es especial para el mantenimiento de los estados de conexión en un servidor. Sin embargo, existe una limitación impuesta por esta opción de protocolo. En la definición original de DNS, RFC 1035, las respuestas de UDP estaban restringidas a 512 octetos. El límite de 512 octetos se observa aún hoy en el software en uso, ya sea para cumplir o hacer cumplir el límite.

Gracias al mecanismo de extensión para el DNS, EDNS(0), que se definió originalmente en un documento RFC que se publicó en agosto de 1999 [RFC 2671, actualizado por RFC 6891], un solicitante de DNS puede informar al servidor de DNS que tiene la capacidad de manejar tamaños de respuestas de UDP superiores a 512 octetos. El solicitante indica su tamaño de carga de UDP máximo (no el tamaño de paquete de IP sino el tamaño de mensaje de DNS) en la consulta y el servidor debe emitir una respuesta de UDP en la que la carga de DNS no supere el tamaño de búfer especificado. Si esto no es posible, entonces el servidor define el bit truncado en la respuesta para indicar que se produjo un truncamiento. Si la respuesta truncada incluye un mensaje de DNS válido, el solicitante puede optar por usar la respuesta truncada. De lo contrario, el solicitante inicia una sesión de TCP en el servidor y repita la consulta en TCP.

Los sistemas de DNS que utilizan las Extensiones de Seguridad del Sistema de Nombres de Dominio deben indicar su capacidad de hacerlo mediante la marca DO (DNSSEC OK) en el seudoencabezado EDNS. Dado que el impacto operativo que se considera en este documento se avoca completamente a los sistemas que admiten DNSSEC, los sistemas implicados admiten EDNS(0) (porque DNSSEC requiere respaldo de EDNS(0)) y, por lo tanto, no están restringidos por el límite de 512 octetos.

Un cliente puede iniciar una transacción en TCP, pero el comportamiento común del solicitante es iniciar la transacción en UDP y utilizar el bit truncado en una respuesta para indicar que el solicitante debe usar TCP para la consulta.

La fragmentación del paquete de UDP recibe un tratamiento diferente en IPv4 y en IPv6. Cuando un paquete es demasiado grande para el medio de transmisión del paquete de IP subyacente, este debe fragmentarse. En este caso, los fragmentos posteriores utilizar el mismo líder de nivel IP, incluso el campo de número de protocolo de UDP, aunque excluyen el seudoencabezado UDP. En IPv4, el remitente original o un enrutador intermediario pueden fragmentar un paquete de IP, a menos que se haya definido la marca de IP *Don't Fragment* (No fragmentar). En IPv6, solo el remitente original puede fragmentar un paquete de IP. Si un enrutador intermediario no puede reenviar un paquete a la siguiente interfaz de salto, en IPv6 el enrutador generará un paquete de diagnóstico ICMPv6 con el tamaño de MTU de la siguiente interfaz de salto y la parte principal del paquete y regresará esta información al remitente del paquete.

Cuando se utiliza UDP, el remitente no puede mantener un búfer de datos no reconocidos, entonces, cuando el remitente IPv6 recibe este mensaje no puede volver a transmitir los datos originales. Los datos empíricos parecen indicar que una respuesta común en muchas implementaciones de IPv6 es generar una entrada de host en la tabla de reenvío IPv6 local y registrar la MTU recibida en esta tabla por algún tiempo de caché determinado de forma local. Esto implica que cualquier intento posterior de enviar un paquete de UDP IPv6 a este destino utilizará este valor de MTU para determinar el modo de fragmentación del paquete saliente.

7.1.1 La experiencia de medición

Se ha diseñado y configurado un experimento para reproducir el entorno de una situación de servidor raíz a fin de evaluar el impacto que los tamaños grandes de paquetes pueden tener en resolutores y usuarios.

Esto se logró mediante una plataforma de anuncio en línea para inducir a los resolutores de DNS a publicar consultas únicas en un servidor de nombre acreditado que se configuró para responder a consultas de dos zonas con distintos tamaños de respuesta. Se cree que los resolutores que presentaron la consulta en el servidor de nombre acreditado para esta prueba son, en su mayoría, los mismos resolutores que harían consultas en la Zona Raíz.

Para evaluar si un resolutor podía recibir una respuesta grande, el anuncio solicitaba un nombre de dominio destinatario. El mismo nombre de dominio destinatario devolvería un tamaño normal de respuesta. Pero, para obtener la respuesta final, el resolutor primero debía recibir una respuesta intermedia grande.

Si el resolutor tenía éxito en pedir la información del nombre de dominio destinatario, entonces la prueba revelaba que el resolutor podía manejar la respuesta intermedia grande.

La prueba también incluyó la recuperación de un objeto web del servidor web del experimento, así fue posible hacer coincidir las direcciones utilizadas en la recuperación web (la dirección IP del usuario final) con las direcciones utilizadas por los resolutores de nombre en la publicación de la consulta de DNS.

En esta prueba, se utiliza una respuesta de DNS de 1444 octetos.

7.1.2 Resultados de las pruebas

En un período de cinco días durante mayo de 2015, alrededor de 7,26 millones de sistemas finales alcanzaron con éxito un pequeño registro de control; algunos de estos, 7,17 millones de sistemas alcanzaron con éxito el registro de prueba, una diferencia de aproximadamente 90 000 usuarios, o 1 % del conjunto de muestra, que no logró alcanzar el registro de prueba de DNS de 1444 octetos.

Estos sistemas finales utilizaron 83 000 direcciones IP de resolutor de DNS diferentes. De estos, el 94 % de los resolutores obtuvo con éxito el registro de control y el registro de prueba. De los 4251 resolutores que recuperaron el registro de control pero fallaron en la recuperación del registro de prueba, 3396 resolutores utilizaron la extensión EDNS(0) con el conjunto de bit DNSSEC OK, que inició la respuesta de 1444 octetos. De estos resolutores que fallaron, 3110 se observaron solo una vez durante el experimento, mientras que 826 mostraron la condición de error más de una vez. Esto implica que el 1 % de los resolutores vistos en este experimento no pudieron recuperar una respuesta grande dos o más veces, mientras que un 3 % de los resolutores que fallaron en la recuperación de la respuesta grande solo se observaron una sola vez, lo que no aporta datos suficientes como para concluir con certeza que fallarían de forma consistente con respuestas grandes. Este 1 % de los resolutores de fallaron dos o más veces de forma consistente fueron utilizados por algo menos que 3000 sistemas finales, o 0,04 % de la población de sistemas finales de muestra.

5237 resolutores utilizaron direcciones IPv6 en esta prueba (6 % del total) mientras que 830 de estos, fallaron en la recuperación del registro de prueba (21 % de los resolutores que fallaron). Estos datos sugieren un posible problema con algunos resolutores IPv6 y su manejo de los tamaños de MTU.

En términos de medir el cambio en la carga de consulta con respuestas grandes, el nombre de control (con un tamaño de respuesta de 93 octetos) se consultó 16,4 millones de veces y 475 consultas se observaron con el uso de TCP. El nombre de

prueba (con un tamaño de respuesta de 1444 octetos) se consultó 18,6 millones de veces, 1,2 millones de estas consultas se realizaron desde TCP, o el 6,5 % del total del conteo de consultas para el nombre de prueba. Hay una diferencia en la cantidad total de consultas realizadas al registro de control frente a la cantidad de consultas que se realizaron al registro de prueba. La diferencia puede explicarse con los resolutores que respondieron a las respuestas truncadas recibidas para el registro de prueba con el envío de otra consulta por TCP. Este resultado tiene una correlación razonable con la distribución de tamaños de búfer de UDP que se ofrece en las extensiones EDNS(0) de las consultas de UDP. Cuando se brindan respuestas más grandes, un servidor acreditado puede anticipar una carga de consulta más elevada y una proporción mayor de consultas por TCP.

7.1.3 Conclusión

Parece que aproximadamente el 1 % de los resolutores que establecieron la marca DNSSEC OK en sus consultas no fueron capaces de recibir una respuesta de DNS de 1444 octetos (los factores de incertidumbre experimental implican que la estimación por lo alto de esta cifra es el 6 % de todos los resolutores). En este conjunto de resolutores, aquellos que utilizaron IPv6 como un protocolo de transporte no están representados de forma proporcionada. Es posible que esta tasa de error se deba a la presencia de varias formas de middleware que intercepta el DNS o bien, en el caso de IPv6, se deba a un posible mal manejo de los mensajes ICMP6: *Packet Too Big* (Paquete demasiado grande). Aun así, con esta metodología experimental, no es posible establecer la naturaleza exacta de los errores.

Los resolutores que fallaron en la recepción de respuestas representan una proporción muy pequeña de usuarios. La cantidad de usuarios que utilizan resolutores de DNS y que no son capaces de resolver un nombre de DNS de forma consistente cuando se incluyen respuestas de DNS de este tamaño, parece ser el 0,04 % de todos los usuarios (los factores de incertidumbre experimental implican que la estimación por lo alto de esta cifra es el 1 % de todos los usuarios).

Estos experimentos evaluaron una respuesta de DNS de 1444 octetos. Se observa que otras partes del DNS ya proporcionan respuestas significativamente más grandes que el tamaño que aquí se contempla; estos tamaños de respuesta no parecen haber atraído la atención del público ni contar con comentarios visibles. Por ejemplo, una consulta DNSKEY comparable para el nombre .org del 6 de junio de 2015 que generó una respuesta de 1625 octetos contiene dos claves para la firma de la llave de la zona raíz RSA de 2048 bits, dos claves para la firma de la zona raíz RSA de 1024 bits y tres firmas, una por cada KSK y una por una de las ZSK. Cualquier resolutor de validación que no pueda recibir respuestas de DNS tan

grandes no podrá validar la firma del registro de DS ni del registro de NSEC3 (que se utilizan para señalar la inexistencia de un registro de DS) para cada delegación en la zona .org, que, en efecto, provocará fallas de resolución de DNS para las delegaciones en .org.

El Equipo de Diseño no está al tanto de ningún problema operativo que los titulares de nombre de dominio en .org puedan tener en relación con el tamaño del paquete de respuesta de DNS DNSKEY para el nombre .org. Incluso tras haber considerado la pequeñísima cantidad de zonas firmadas dentro de .org, la ausencia de informes operativos sobre fallas de resolución en los nombres de dominio .org indicaría que el tamaño de respuesta carece de posibilidades de presentar problemas operativos importantes para el traspaso de KSK de la Zona Raíz.

Una diferencia para tener en cuenta entre el caso de prueba y la situación de .org es que solo los resolutores que realizan validaciones actualmente harán consultas para el RRset DNSKEY grande. En el caso de prueba, todos los resolutores que indicaron DNSSEC OK podrán intentar alcanzar la respuesta grande. Como se describe en la Sección 8.2, al parecer menos del 30 % de los resolutores que indicaron DNSSEC OK en la consulta original realizaron posteriores validaciones de la respuesta. Es posible que esos operadores de resolutor que activaron la validación hayan sido más diligentes en la identificación y corrección de problemas relacionados con la red que podrían evitar la recuperación de paquetes de respuesta grandes, dado que estos resolutores serían más propensos a experimentar este tipo de problemas. Otros resolutores, que no realizaron la validación, solo bajo circunstancias relativamente extrañas encontraron paquetes de respuesta grandes, y es posible que desconocieran las limitaciones impuestas por su entorno de red.

Parece razonable inferir que la gran mayoría de quienes fallaron en la recepción de la respuesta grande en las pruebas sean resolutores que no realizan validaciones y que no se verían afectados por el aumento en el tamaño de registro de recursos DNSKEY de la Zona Raíz.

Resumiendo, las pruebas indican que menos del 0,04 % de los usuarios podrían sufrir el impacto de un tamaño de respuesta grande durante el traspaso de KSK de la Zona Raíz, esto es una estimación con un grado de incertidumbre alto. Las observaciones relacionadas que se extrajeron de TLD con conjuntos de clave grande tienden a indicar que esto es una estimación por lo alto sobre el alcance del impacto que podría tener el tamaño de respuesta más grande.[23]

[23] En http://www.potaroo.net/ispcol/2015-05/ksk.html se describen más detalles sobre el experimento y los resultados.

7.2 Comportamiento de validación de DNSSEC

Hay tres aspectos del comportamiento de validación de DNSSEC para medir. El primero es la recuperación de las firmas digitales de DNSSEC (establecimiento de la marca DNSSEC OK en las opciones EDNS (0) en la consulta); el segundo es la función de validación en la que se crea un cadena de confianza desde la clave raíz hasta el nombre que se está validando; y el tercero es si la configuración de resolución de nombre del usuario aceptará el error de validación de DNSSEC como un error definitivo o si la consulta se derivará a otro resolutor.

7.2.1 Resultados de las pruebas

Con el experimento que se describió anteriormente (Sección 7.1.1), en mayo de 2015 se observó que entre 85 % y 90 % de los usuarios pasaban sus consultas a resolutores; las consultas resultantes observadas en un servidor de nombre acreditado para un nombre sin caché incluían la opción EDNS(0) en la consulta y también tenían la marca DNSSEC OK activada.

El 24 % de la misma población de usuarios de muestra realizó consultas posteriores que demostraron que el resolutor validaba la respuesta con DNSSEC al volver por la cadena de firmas de interbloqueo de la jerarquía de delegación de nombre hasta la KSK de la Zona Raíz.

El 11 % de la misma población de usuarios de muestra corresponde al comportamiento de usuario final que responderá a un error de validación de DNSSEC de la transferencia anterior al pasar la consulta a un resolutor distinto que no realiza la validación de DNSSEC.

Esto sugiere que cualquier cambio en los procedimientos de validación de DNSSEC conlleva la posibilidad de impactar en aproximadamente un cuarto de la población de usuarios de Internet.

De estos, poco menos de la mitad de los usuarios ya interpretaron el error de validación de DNSSEC (indicado por SERVFAIL) como una señal para presentar la misma consulta a un resolutor diferente que no realiza la validación de DNSSEC. Para este grupo del 11 % de usuarios de Internet, el cambio de KSK de la Zona Raíz podría incluir una KSK de la Zona Raíz no reconocida y un error de validación, aunque estos usuarios han demostrado que ya interpretan SERVFAIL con un resolutor alternativo. El resultado podría implicar un mayor tiempo para resolver los nombres firmados por DNSSEC, pero no provocará la incapacidad para resolver el nombre.

El 13 % restante de los usuarios que no volvieron a un resolutor que no valida cuando recibieron una respuesta SERVFAIL está en riesgo de no poder resolver un nombre firmado por DNSSEC si los resolutores utilizados por el usuario no son capaces de seguir las señales provistas mediante el proceso de traspaso de clave RFC 5011.

7.2.2 Conclusión

No es posible utilizar este proceso de medición para evaluar si los resolutores son capaces de seguir un proceso RFC 5011 para seleccionar un nuevo valor de KSK de Zona Raíz de forma automática. La mejor opción aquí es contabilizar la población de usuarios que utiliza resolutores para realizar la validación de DNSSEC y recurrir a aquellos que admitirán RFC 5011 o requerirán intervención manual para cargar la nueva KSK de la Zona Raíz en el momento adecuado.

El 24 % de los usuarios utiliza resolutores que realizan validación de DNSSEC y, por ende, tienen una posibilidad de sufrir el impacto de un cambio de KSK de la Zona Raíz. El error de validación devolverá una respuesta SERVFAIL y el 11 % del total de usuarios utiliza una recopilación de resolutores en los que una respuesta SERVFAIL de uno hará que la consulta se resuelva en un resolutor que no realiza validación. Esto implica que el 13 % de todos los usuarios pueden sufrir el impacto de un cambio de KSK de la Zona Raíz si el resolutor desconoce el documento RFC 5011 y el administrador de resolutores no carga la nueva KSK de la Zona Raíz en el momento adecuado.

Sin embargo, muchos de estos usuarios utilizan uno de los servicios de resolutor de validación de DNSSEC más grandes que se consideran conocedores de RFC 5011 (como los resolutores de DNS de Comcast), por lo que este valor de 13 % representa una estimación por lo alto de la población de usuarios que pueden sufrir un impacto de esta forma.

8 Prueba

Hay dos elementos que se relacionan con la prueba. Uno es la actividad de medir el impacto del cambio de la KSK en las operaciones generales de Internet a fin de evaluar el nivel de impacto negativo que puede suspender la operación. El otro es la actividad relacionada con la preparación de usuarios de confianza para la operación, que incluye recursos con un banco de prueba para autoevaluaciones. Los socios de canal que desarrollan software, los operadores que implementan flotas de servidores o cualquier persona interesada puede llevar a cabo una autoevaluación.

8.1 Prueba de impacto

Las pruebas que se ejecutan para otras partes de este informe que miden el éxito de validación han revelado algunas reacciones a los errores de validación de DNSSEC. Una forma de evaluar el daño puede ser recurrir a evidencia de que algunas consultas comienzan con DNSSEC y luego “fallan” en DNS, aunque esta práctica aumente o disminuya a medida que se cambia la KSK. Daño que puede pasar inadvertido pero ser una métrica valiosa cuando se analiza el impacto de la operación de cambio de clave para la firma de la llave de la zona raíz. Es probable que los usuarios (en una pantalla) no lo detecten y, por ende, nunca generen un comprobante para el departamento de servicio técnico de un proveedor de servicios.

Las pruebas que detectan esto deben realizarse de forma periódica (por mes) desde hoy hasta el final (sea exitoso o no) de la operación de cambio de clave de KSK de la Zona Raíz. Antes del cambio, las pruebas nos proporcionarán una línea de base para comparar.

Además de las pruebas automáticas, es importante comunicarse con los socios de canal durante el cambio de clave de KSK de la Zona Raíz a fin de que proporcionen información explícita y en tiempo real o aproximado. Este es un factor de motivación para enviar notificaciones por adelantado a las partes que sufren el impacto, evitar períodos de tiempo en los que el personal está disperso y favorecer los momentos en los que se puede establecer contacto con facilidad.

8.2 Herramientas de autoevaluación

A fin de permitir que los usuarios de confianza realicen las autoevaluaciones, debe existir una plataforma de evaluación que se asemeje a la plataforma operativa a una velocidad de cambio acelerada. Además de hacer que los servidores ejecuten RFC 5011 a una velocidad acelerada con zonas raíz falsas firmadas, los anclajes de confianza en “otras estructuras de datos” deben estar presentes en los mismos nombres de ruta. Esto fomentará la producción de mejores herramientas, como las que brindan asistencia en el veto de una clave o descubren qué hay en un validador (para consumo local o remoto).

Esto puede contribuir con la formación sobre algoritmos nuevos al permitir la introducción y eliminación de claves de distintos parámetros.

El tiempo es una cuestión importante. Debe ser más rápido que el tiempo real para permitir una observación razonable del proceso; aunque en tiempo real también es beneficioso para reducir los efectos de la prueba.

Finalmente, se debe abordar la fidelidad del sistema raíz, ya sea que la totalidad de la zona raíz se utiliza o no como datos o se considera una zona falsa representativa.

Hay algunos ejemplos existentes de tales bancos de prueba[24, 25] que pueden utilizarse como modelo para futuras pruebas.

8.3 Software de Encargado de KSK y ZSK y Prueba de interoperabilidad de la modificación de procesos

Dado que el proceso de traspaso de KSK requiere modificaciones a los cronogramas, procesos y posiblemente a las operaciones de KSK de soporte de software existentes, es necesario realizar evaluaciones exhaustivas de estos cambios antes de comenzar con el traspaso. Estas evaluaciones deben incluir, entre otras, la generación de claves, la generación de RRset DNSKEY firmados, la validación de DNSSEC, el intercambio KSR/SKR, los mecanismos de respaldo y los ensayos de la ceremonia de clave.

9 Implementación

El proceso de traspaso de clave propuesto se elaboró por primera vez en julio de 2013 y desde entonces ha recibido vetos y perfeccionamientos. El proceso que se describe aquí debe tomarse como una versión preliminar que los socios de RZM seguirán mejorando antes de su implementación.

El proceso se divide en tres fases:

1) publicación de la KSK de la Zona Raíz entrante;
2) cambio de firma con la KSK de la Zona Raíz entrante (“el traspaso”);
3) revocación de la KSK de la Zona Raíz titular.

La revocación de la KSK de la Zona Raíz titular se está demorando deliberadamente para permitir una reversión, en caso de que surjan problemas con la KSK de la Zona Raíz entrante tras la eliminación de la KSK de la Zona Raíz titular del conjunto de claves. El proceso pretende cumplir con RFC 5011, con ventanas ampliadas para agregar la KSK entrante y revocar la KSK titular. El proceso permite de forma explícita la opción de demorar la revocación de la KSK de la Zona Raíz titular por un período indefinido, lo que contempla la eventualidad de que existan cuestiones imprevistas con el proceso de traspaso que pudieren requerir un cambio en el proceso de traspaso de clave planificado.

[24] http://keyroll.systems/
[25] http://icksk.dnssek.info/fauxroot.html

Gráfico 1 a continuación muestra una descripción general de los tres trimestres en los que se llevará a cabo el proceso. Tenga en cuenta que la numeración de los trimestres es relativa al comienzo del proceso, no está ligada al calendario. Por ejemplo, Trimestre 1 y T1 no refieren necesariamente al período entre enero y marzo. La KSK entrante figura como “KSK-NEW” (KSK-NUEVA), la KSK titular es “KSK-2010”.

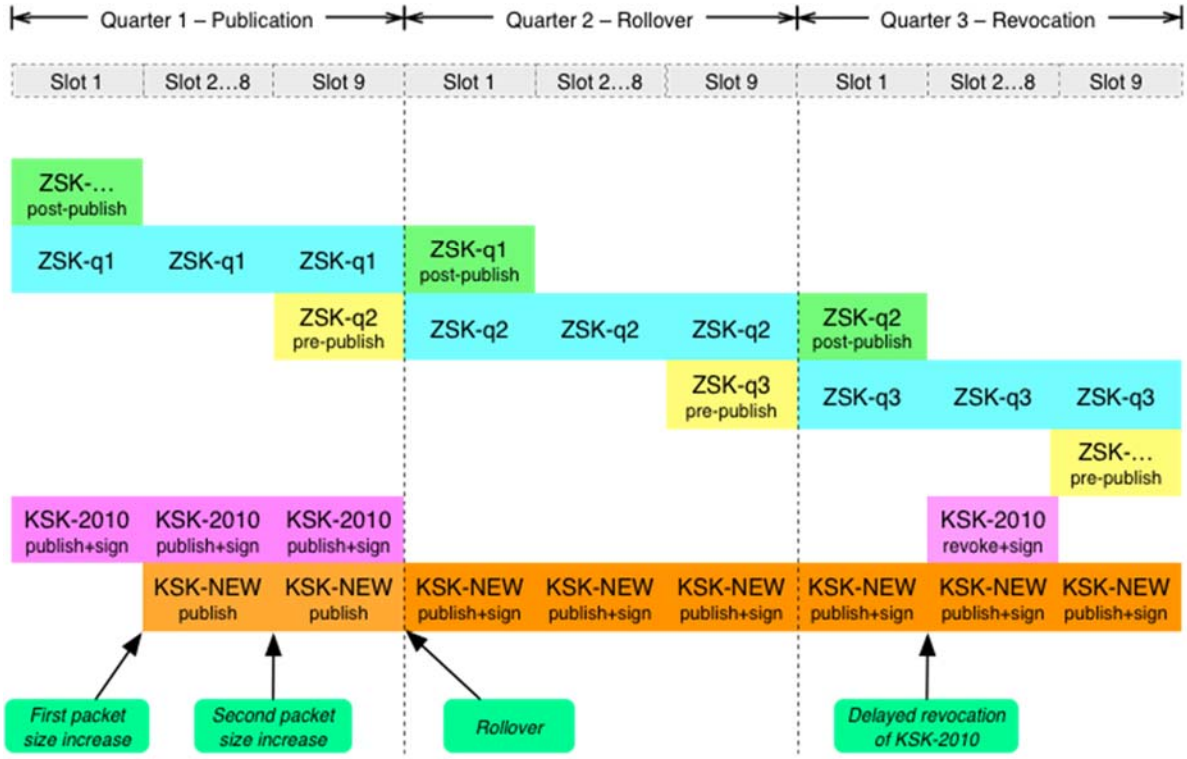

Gráfico 1. Cronograma de traspaso

9.1 Publicación de la KSK entrante

La KSK entrante se agrega al RRset DNSKEY en el T1 espacio 2, pero aún no se utiliza para firmar. Esta es una fase de publicación provisional para que la KSK entrante sea elegida por los validadores que cumplen con RFC 5011. La KSK entrante se publica (y firma por la KSK titular) en la Zona Raíz por un total de 80 días antes de que se utilice para firmar. Se espera que los anclajes de confianza configurados de forma manual se actualicen para incluir la KSK entrante antes de o durante este período.

Un traspaso que cumple con RFC 5011 requiere la publicación de una clave nueva durante un período de al menos 30 días (“tiempo de inactividad agregar/retener”). Si el período de publicación de 80 días propuesto no resulta suficiente, es posible

introducir uno o más trimestres de publicación adicionales antes de cambiar la clave.

Durante el trimestre de publicación de la KSK entrante, los resolutores de validación de DNSSEC verán que el tamaño del paquete de una respuesta a una consulta para el RRset DNSKEY de la Zona Raíz (tamaño de paquete de respuesta) aumentará de 736 octetos a 1011 octetos. (Este aumento teórico se basa en una comparación entre el tamaño de una respuesta de DNS en esta etapa si no hay un traspaso de clave en curso y el tamaño durante el proceso de traspaso de clave). Durante el último espacio de T1, en el traspaso de ZSK, el tamaño de paquete de respuesta aumenta de 833 octetos a 1158 octetos.

9.2 Traspaso de la KSK entrante

Luego de la introducción de la KSK entrante, se la utiliza para firmar el RRset DNSKEY raíz que comienza en T2 espacio 1. Este trimestre es igual a cualquier otro, excepto en que todos los RRset DNSKEY están firmados (únicamente) por la KSK entrante. La única vez que el RRset DNSKEY está firmado por las KSK titular y entrante es durante el período de revocación opcional, que se describe a continuación.

9.3 Revocación de la KSK titular

Si la KSK titular se revoca como se describe en RFC 5011, esta se publica con el bit de revocación y la firman tanto la KSK titular como la KSK entrante.

La revocación de la KSK titular es opcional. Si se desea la revocación, la publicación de la KSK titular revocada se realiza desde el comienzo de T3 espacio 2 hasta T3 espacio 8.

Durante una revocación, el tamaño de paquete de respuesta aumenta de 736 octetos a 1297 octetos.

9.4 Impacto del tamaño de paquete de respuesta

Un objetivo deseable es evitar la fragmentación de UDP tanto como sea posible. A continuación se presentan algunas restricciones de tamaño de respuesta pertinentes:

Tamaño	Umbral
512 octetos	El tamaño de carga de DNS mínimo que debe admitir el DNS
1232 octetos	El tamaño de carga de DNS máximo de un paquete de UDP de

	DNS IPv6 que no se puede fragmentar
1452 octetos	El tamaño de carga de DNS máximo de un paquete de UDP de DNS IPv6 Ethernet sin fragmentar
1472 octetos	El tamaño de carga de DNS máximo de un paquete de UDP de DNS IPv4 Ethernet sin fragmentar

Tabla 4. Umbrales de tamaño de paquetes

Los resultados de las pruebas antes presentadas indican posibles problemas con algunos resolutores de IPv6 y su manejo de respuestas grandes. La primera y más presente restricción de tamaño es, por lo tanto, el umbral de un paquete de UDP de DNS IPv6 que no se puede fragmentar, lo que implica un tamaño de paquete de respuesta DNSKEY de 1232 octetos, como máximo.

Solo se alcanza el primer umbral durante la fase de revocación opcional, donde la KSK de la Zona Raíz titular debe volverse a introducir y marcarse con el bit de revocación. Para el cumplimiento completo con RFC 5011, el RRset DNSKEY debe tener la doble firma de la KSK de la Zona Raíz entrante y de la KSK de la Zona Raíz titular durante la fase de revocación. La doble firma del RRset hará que el tamaño de respuesta exceda los 1232 octetos.

El paquete de respuesta simple más grande para la Zona Raíz es el RRset DNSKEY firmado. La tabla a continuación presenta una descripción general del tamaño de paquete de respuesta DNSKEY durante el cambio propuesto, así como también una comparación entre los tamaños de paquete de respuesta sin cambios.

Tiempo	DNSKEY durante cambio	RRSIG durante cambio	Tamaño de respuesta DNSKEY durante cambio	Tamaño de respuesta DNSKEY sin cambio
T1 espacio 1	1 KSK + 2 ZSK	1 KSK	883 octetos	883 octetos
T1 espacio 2 ... 8	2 KSK + 1 ZSK	1 KSK	1011 octetos	736 octetos
T1 espacio 9	2 KSK + 2 ZSK	1 KSK	1158 octetos	883 octetos
T2 espacio 1	1 KSK + 2 ZSK	1 KSK	883 octetos	883 octetos
T2 espacio 2 ... 8	1 KSK + 1 ZSK	1 KSK	736 octetos	736 octetos

T2 espacio 9	1 KSK + 2 ZSK	1 KSK	883 octetos	883 octetos
T3 espacio 1	1 KSK + 2 ZSK	1 KSK	883 octetos	883 octetos
T3 espacio 2 ... 8	2 KSK + 2 ZSK	2 KSK	1297 octetos	736 octetos
T3 espacio 9	1 KSK + 2 ZSK	1 KSK	883 octetos	883 octetos

Tabla 5. Tamaños de paquetes durante el traspaso

(El código de colores de la tabla anterior corresponde al gráfico que se encuentra a continuación.)

Los riesgos asociados con evitar la revocación de la clave saliente no se analizaron en detalle, pero la fase de revocación puede verse como opcional en esta etapa. Una opción puede ser actualizar el RFC 5011 en este respecto y no necesitar la doble firma para la revocación de la clave saliente. Esta revisión tendría los beneficios agregados de poder revocar una clave que se perdió o destruyó. No requerir la doble firma de la clave saliente también puede facilitar futuros traspasos de clave, cambios de algoritmo y cambios en las longitudes de clave. No obstante, debido al tiempo para redefinir, publicar, desarrollar y distribuir códigos, así como también presionar el código en las operaciones, esta opción no resulta viable para este traspaso de clave KSK.

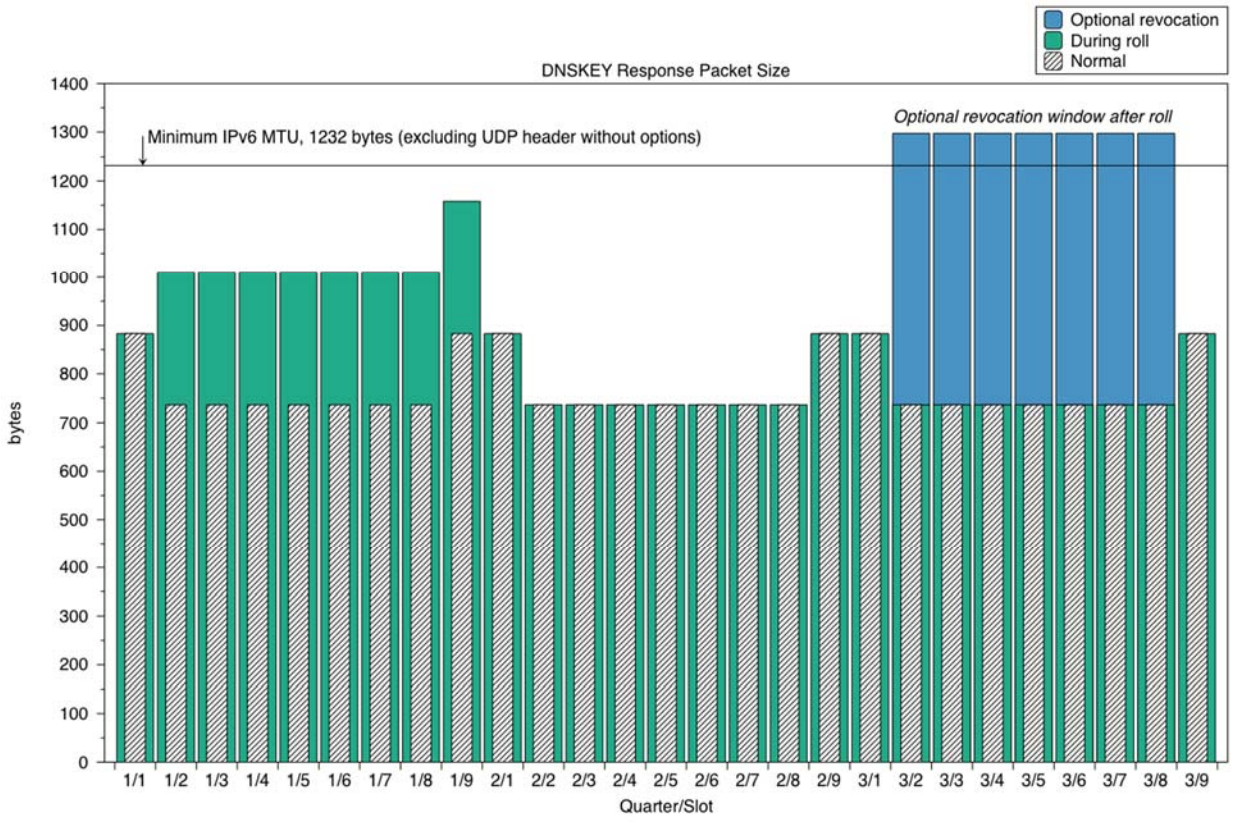

Gráfico 2. Tamaños de los paquetes de respuesta DNSKEY

9.5 Implementación de servidor raíz por servidor raíz

La introducción de DNSSEC de 2010 se realizó de servidor raíz por servidor raíz. En enero de 2010 apareció una versión preliminar de la zona firmada DNSSEC en un servidor, en otro servidor raíz en febrero, en dos servidores raíz más en marzo y así sucesivamente. El objetivo era permitir que los servidores recursivos (o cualquier cosa que enviara consultas a los servidores raíz) tuvieran la capacidad de probar DNSSEC primero y proporcionar respaldo si las respuestas no eran aceptables.

La estrategia fue propuesta para el cambio de KSK de la Zona Raíz, pero se descartó rápidamente por varios motivos. Con el objetivo de mitigar los problemas relacionados con la nueva KSK de la Zona Raíz y la capacidad de medir la adopción de un nuevo anclaje de confianza con el tiempo, se obstaculizaron las siguientes realidades.

Frente al error de validación de DNSSEC, la reacción del servidor recursivo de validación varía de herramienta a herramienta. Algunas herramientas son muy agresivas cuando vuelven a intentar, otras no tanto y a otras no les preocupa en absoluto.

Detectar si un servidor recursivo (o un origen de consulta) ha tomado una decisión explícita de preferir un servidor raíz por sobre otro es poco práctico. En circunstancias normales, el seguimiento que se realiza de los orígenes de consulta en los servidores raíz no es suficiente como para detectar servidores recursivos que prefieren un servidor raíz por sobre otro. La recopilación Un día en la vida de Internet (DITL)[26] que DNS-OARC realiza anualmente se ejecuta por un período breve. Es un esfuerzo enorme y aún nunca se ha gestionado para abarcar todos los servidores raíz en un período determinado.

Una consideración final es el período de tiempo disponible para introducir de forma incremental el nuevo anclaje de confianza. Hay solo 70 días en cualquier trimestre fuera de un ZSK de la zona raíz. La adición de la KSK entrante (al primer servidor) demora 40 días, lo que deja solo 30 días más para completar la tarea con un período de cambio de ZSK. La implementación incremental original se extiende por más de cuatro meses.

10 Reversión

Si se detectasen problemas serios tras la introducción de la KSK entrante, los RRset DNSKEy firmados solo por la KSK titular deben estar preparados y listos para implementación. Estos RRset están en formato *Respuesta de clave firmada* (SKR) y pueden producirse con las mismas ceremonias de clave KSK de la Zona Raíz que los RRset sin reversión. Los socios de RZM deben seguir desarrollando los criterios para tales necesidades de reversión.

Recomendación 14: Para reducir el tiempo de recuperación debido a dificultades que involucren a la KSK entrante, se generará un SKR generado solo por la KSK titular en paralelo con el SKR generado por la KSK entrante.

Recomendación 15: Los socios de RZM deben elaborar y documentar el proceso de utilización de la KSK titular generada por SKR.

Los SKR de reversión que contienen RRset DNSKEY estarán preparados para todos los trimestres del proceso. Durante T1 y T2, el SKR de reversión consta de RRset DNSKEY con la KSK titular y la ZSK actual, firmada por la KSK titular. La KSK entrante se omite. Durante T3, el SKR de reversión consta de RRset DNSKEY con la KSK entrante y la ZSK actual, firmada por la KSK entrante. La KSK titular revocada se omite.

Umbrales

[26] https://www.dns-oarc.net/ditl/2011

Las pruebas que se han realizado hasta la fecha de la implementación de DNSSEC indican que existe un margen de error de 5 %, aproximadamente. Esto significa que cualquier declaración relacionada con la cantidad de daño que ocurra tendrá que reconocer que el 5 % de la población (personas o servidores recursivos, según la manera en que se realicen las mediciones) puede sufrir cierta degradación de rendimiento sin que se lo detecte. A partir de esto, la definición de una métrica específica no se considera como una forma de definir un disparador de reversión.

Más aún, no es clara la forma que puede tomar el daño. Puede ser una implementación errante, un indicador de código errante, un procedimiento errante o un acto aleatorio de Internet. Por este motivo, el primer paso es mantener el contacto con los socios de canal y abrir medios para informar problemas, para luego aplicar el mejor criterio y reaccionar ante los informes.

Además de la gravedad y expansión del daño, en función de los muchos casos de uso, tampoco es claro si la reversión puede causar más daño que si se avanza y se mitigan los problemas a medida que se los detecta.

11 ¿Cuándo?

En el entorno operativo existente, hay cuatro días en el año calendario en los que una nueva KSK de la Zona Raíz puede asumir por la titular. Estos cuatro días son los primeros días de los trimestres, o los primeros de enero, abril, julio y octubre. La elección de una fecha específica para el cambio tiene dos componentes: lo razonable en términos operativos y lo compatible con los debates actuales sobre la transición de la IANA.[27]

Los razonable en términos operativos refiere a que las fechas implicadas deben evitar fines de semana, vacaciones que afecten los cronogramas de trabajo y períodos en los que el personal de operaciones cuente con un margen acotado. Y siendo necesaria la alineación de las tres fechas con una audiencia global, es posible que no todo lo anterior pueda ajustarse. Para agregar elementos al desafío, en 2016 y 2017, cada trimestre comienza un viernes, sábado o domingo; ningún trimestre comienza en otro día de la semana hasta 2018. (El cuatro trimestre de 2015, 1 de octubre, comienza un jueves, pero no habrá un plan en práctica ni se habrán completado las pruebas necesarias para contar con un cambio de clave para esa fecha.)

[27] http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

Un impacto no técnico es la transición de la custodia de la IANA planificada. Esto hace que sea poco práctica la recomendación de una fecha determinada en este momento.

12 Análisis de riesgo

12.1 Riesgo asociado con la preparación insuficiente

Descripción	Impacto	Probabilidad	Mitigación
El cambio de KSK con el mismo algoritmo, hash y tamaño no será suficiente para las partes interesadas	Bajo	Improbable	Planificación de otro cambio una vez que se complete el primero. Si se necesitan parámetros diferentes, se cambiarán.
Los operadores de red no estarán conscientes del cambio (es decir, la red de centros obtiene registro de incidentes, debe saber cómo reaccionar)	Moderado	Probable	En el plan de comunicación; enfocado al operador
Los operadores de red y desarrolladores de software (o “todos los Socios de canal”) no tendrán (acceso a) entornos de prueba adecuados	Moderado	Probable	Configuración de un banco de pruebas RFC 5011 de la ICANN con cambios acelerados y oportunos; otras pruebas

Descripción	Impacto	Probabilidad	Mitigación
La capacidad para centralizar las pruebas durante el progreso no es viable	Bajo	Probable	Desarrollo de enfoques de prueba distribuidos; desarrollo de lista de contactos
La falta de criterios de determinación para tomar decisiones a favor o en contra	Bajo	Probable	Necesidad de preparar comunicaciones y pruebas; viabilidad de estudios de mecanismos utilizados en el campo; intentos a largo plazo para desarrollar mediciones de aceptación de anclaje de confianza actualizado

12.2 El mecanismo de anclaje de confianza automatizado no funciona o no es adecuado

Descripción	Impacto	Probabilidad	Mitigación
RFC 5011 no está activado en todas partes	Moderado	Probable	Enfoques de gestión de anclaje de confianza alternativos
RFC 5011 no se implementó completamente	Moderado	Improbable	Comunicación con desarrolladores de software; verificación de la comprensión de RFC 5011
El proceso de arranque del validador no se implementó completamente	Moderado	Improbable	Comunicación con los integradores de sistema y los administradores del anclaje de confianza

Las definiciones del anclaje de confianza no están disponibles en el sitio web de la IANA de la ICANN	Bajo	Improbable	Supervisión de disponibilidad
Equipo con definiciones de anclaje de confianza sin sincronización por falta de mantenimiento	Bajo	Probable	Plan de Comunicaciones

12.3 La eliminación de la KSK titular provoca errores de validación

Descripción	Impacto	Probabilidad	Mitigación
El protocolo de anclaje de confianza automatizado no se siguió completamente (por cualquier participante del proceso)	Bajo	Probable	Prueba, comunicación; provisión de recursos para que los operadores aceleren la remediación
Tráfico elevado debido a “retry-in-face-of-failure” (reintentar frente a un error)	Bajo	Improbable	Evaluación de los efectos prolongados “roll-over-and-die[28]” (abandonar); recomendaciones de caché negativas

[28] http://iepg.org/2010-03-ietf77/dnssec-goes-wrong.pdf, http://www.potaroo.net/ispcol/2010-02/rollover.html

12.4 La adición de la KSK entrante causa que el tamaño de mensaje de DNS exceda el límite

Descripción	Impacto	Probabilidad	Mitigación
La transición de los conjuntos de clave provoca datagramas sobredimensionados	Moderado	Improbable	Planificación minuciosa de la transición al examinar el tamaño de los mensajes
Confusión sobre el manejo de la fragmentación de IPv6 en software de DNS	Bajo	Improbable	Análisis y prueba del software de DNS

12.5 Se produjeron errores operativos

Descripción	Impacto	Probabilidad	Mitigación
El cambio de KSK mal hecho cortará el impulso de adopción de DNSSEC	Alto	Improbable	Diseño y revisión cautelosos
El aplazamiento indefinido de un traspaso de clave aumenta el impacto si este se volviese urgente	Alto	Improbable	Compromiso con un cambio de KSK de la Zona Raíz
Una vez que comienza, ya no se puede volver al estado aceptable actual	Alto	Improbable	Definición de un plan de respaldo

La destrucción de la KSK titular (componente privado) no es suficiente	Bajo	Improbable	Compromiso para completar el plan

13 Lista del personal del Equipo de Diseño

13.1 Voluntarios de la comunidad

- Joe Abley, Dyn, Inc., Canadá
- Jaap Akkerhuis, NLNetLabs, Países Bajos
- John Dickinson, Sinodun Internet Technologies, Reino Unido
- Geoff Huston, APNIC, Australia
- Ondrej Sury, CZ.NIC, República Checa
- Paul Wouters, No Hats/Red Hat, Países Bajos
- Yoshiro Yoneya, JPRS, Japón

13.2 Socios de Gestión de la Zona Raíz

- David Conrad, ICANN
- Edward Lewis, ICANN
- Richard Lamb, ICANN
- Alain Durand, ICANN
- Hayley Laframboise, ICANN
- Elise Gerich, ICANN
- Kim Davies, ICANN
- Roy Arends, ICANN
- Jakob Schlyter, ICANN
- Fredrik Ljunggren, ICANN
- Brad Verd, Verisign
- Duane Wessels, Verisign
- David Blacka, Verisign
- Al Bolivar, Verisign
- Tim Polk, NIST del Departamento de Comercio de los Estados Unidos
- Scott Rose, NIST del Departamento de Comercio de los Estados Unidos
- Doug Montgomery, NIST del Departamento de Comercio de los Estados Unidos
- Ashley Heineman, NTIA del Departamento de Comercio de los Estados Unidos
- Vernita Harris, NTIA del Departamento de Comercio de los Estados Unidos

14 Referencias

- RFC 5011: Automated Updates of DNS Security (DNSSEC) Trust Anchors (RFC 5011: Actualizaciones automáticas de los anclajes de confianza de seguridad del Sistema de Nombres de Dominio (DNSSEC)) https://tools.ietf.org/html/rfc5011
- SAC063: SSAC Advisory on DNSSEC Key Rollover in the Root Zone (SAC063: Asesoramiento del SSAC sobre traspaso de claves DNSSEC en la zona raíz) https://www.icann.org/en/system/files/files/sac-063-en.pdf
- DNSSEC Practice Statement for the Root Zone KSK Operator (Declaración de Prácticas de DNSSEC para el Operador de KSK de la Zona Raíz) https://www.iana.org/dnssec/icann-dps.txt
- DNSSEC Practice Statement for the Root Zone ZSK Operator (Declaración de Prácticas de DNSSEC para el Operador de ZSK de la Zona Raíz)
- https://www.verisigninc.com/assets/dps-zsk-operator-1527.pdf
- DNSSEC Trust Anchor Publication for the Root Zone (Publicación de anclaje de confianza de DNSSEC para la Zona Raíz) https://tools.ietf.org/html/draft-jabley-dnssec-trust-anchor
- Establishing an Appropriate Root Zone DNSSEC Trust Anchor at Startup (Establecimiento de un anclaje de confianza de DNSSEC de la Zona Raíz adecuado desde el comienzo) https://tools.ietf.org/html/draft-jabley-dnsop-validator-bootstrap

15 Apéndice: Socios de canal

El término “socios de canal” refiere a las organizaciones externas que facilitan o confieren valor a la gestión de KSK de la Zona Raíz de forma independiente. Estas organizaciones no tienen relaciones formales con los socios de RZM, aun así, es esencial que exista cierto tipo de coordinación. Para cada organización, se mantendrán contactos adecuados para intercambiar estados u otra información relacionada con el cambio de KSK de la Zona Raíz.

A continuación se encuentra una lista de los socios de canal, sin un orden en particular.

15.1 Productores de software

La comunicación sustantiva entre estos socios corresponde a la implementación, o no, de la gestión del anclaje de confianza RFC 5011 en el software. El conjunto de socios es aquel con servidores de caché recursivos de validación La información de contacto de estas organizaciones no se incluye en el presente documento.

- Dominio de Nombres de Internet de Berkeley de ISC (http://www.isc.org)
- NLNetLab's Unbound (https://nlnetlabs.nl)
- Microsoft Windows Server (https://www.microsoft.com/)
- Nominum's Vantio (http://nominum.com/caching-dns/)
- DNSMASQ (http://www.thekelleys.org.uk/dnsmasq/doc.html)
- IRONSIDES (http://ironsides.martincarlisle.com)
- Infoblox (http://www.infoblox.com/
- Secure64 DNS Cache (http://www.secure64.com/)

15.1.1 Pendiente

El siguiente conjunto de socios ha debatido pero no lanzó servidores de caché recursivos con validación de DNSSEC. Se encuentran en una lista que se incluirá si se distribuye el código. (Otros servidores de caché recursivos de DNS sin respaldo para DNSSEC no dependen de la KSK de la Zona Raíz)

- Servidor recursivo por determinar de CZ.NIC (aparte de Knot)
- PowerDNS por determinar

15.2 Integradores de sistema

Estos socios de canal transmiten la KSK de la Zona Raíz como parte de los datos de configuración que incluyen, en algunos casos, el software de DNS antes

mencionado. La expectativa es que estas organizaciones revisen la KSK de la Zona Raíz entrante y la incluyan en sus actualizaciones de software.

15.2.1 Linux

- Mecanismos de Protección de Derechos de Red Hat Enterprise Linux (RHEL)
- SUSE de Micro Focus International (Mecanismo de Protección de Derechos)
- Fedora
- CentOS
- Debian and Canonical (Ubuntu) APT
- Montavista Linux

15.2.2 BSD

- Puertos FreeBSD
- NetBSD pkgsrc
- Puertos OpenBSD

15.2.3 Otros

- Apple iOS, OS X
- Google Android, ChromeOS
- Microsoft
- Cisco
- Juniper
- Belkin
- Cisco / Linksys
- Wind River (RTOS)
- QNX (RTOS)
- OpenVMS
- OpenWRT

15.3 Operadores de resolutores públicos

De acuerdo con los informes, estos operadores ejecutan servidores de DNS recursivos, en algunos casos con validación de DNSSEC. Se espera que incluyan la KSK de la Zona Raíz como datos de configuración y es posible que las revisiones internas deban conocer la KSK de la Zona Raíz entrante.

- Google Public DNS
- OpenDNS
- Neustar DNSAdvantage
- Symantec ConnectSafe
- Nivel 3

- Censurfridns
- Comodo
- Dyn Internet Guide
- Liquid Telecom

Además de la lista anterior de operadores con resolutores públicos, que se seleccionaron mediante la aceptación de tráfico desde cualquier lugar en Internet (en tanto sea visible), hay otros socios que operan resolutores públicos con restricciones en su base de usuarios de confianza. A medida que se identifiquen estos socios, también se les brindarán notificaciones de los eventos de KSK de la Zona Raíz.