Guía Rápida:

Preparación de los sistemas para el traspaso de la firma de la llave (KSK) de la zona raíz

¿Qué es el traspaso de la firma de la llave (KSK) de la zona raíz?

La Corporación para la Asignación de Nombres y Números en Internet (ICANN) está planificando traspasar, o cambiar, el par "superior" de claves criptográficas que se utiliza en el Protocolo de Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC), comúnmente conocido como la clave para la firma de la llave de la zona raíz (KSK). Esta será la primera vez que se cambie la KSK desde que se generó inicialmente en el año 2010. Se considera un paso importante relativo a la seguridad, de la misma manera que el cambio periódico de contraseñas es considerado una práctica prudente por todo usuario de Internet.

El cambio de la clave implica la generación de un par nuevo de claves criptográficas y la distribución de un componente público nuevo a los resolutores de validación de DNSSEC. Dado que todas las consultas de Internet que usan DNSSEC dependen de la KSK de la zona raíz para validar el destino, esto será un cambio significativo. Ahora que se han generado las claves nuevas, los operadores, como ISP, deberán actualizar sus sistemas con la clave nueva para que cuando un usuario intente visitar un sitio web, se pueda cotejar con la KSK nueva y validarlo.

¿Por qué debe prepararse?

Actualmente, una cuarta parte de los usuarios de Internet del mundo acceden a Internet a través de resolutores de validación de DNSSEC que pueden verse afectados por el traspaso de la KSK. Si estos resolutores de validación no tienen la clave nueva cuando se realice el traspaso de la KSK, los usuarios finales que dependen de dichos resolutores encontrarán errores y no podrán tener acceso a Internet.

Si no usa DNSSEC, su sistema no se verá afectado por el traspaso. No obstante, debe saber que las Extensiones de Seguridad del Sistema de Nombres de Dominio son una parte importante para evitar el secuestro de nombres de dominio.

La ICANN ofrece un banco de prueba para los operadores o cualquier parte interesada que desee confirmar que sus sistemas pueden gestionar el proceso de actualización automatizado correctamente. Visite la siguiente página para asegurarse de que sus sistemas están listos: **https://go.icann.org/KSKtest**.

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

Diseñado por el Equipo de Comunicaciones de la ICANN | Marzo de 2018

¿Qué debe saber?

Los sistemas pueden actualizarse en cualquier momento antes del traspaso con la nueva KSK de la zona raíz que se publicó el 11 de julio de 2017 y es posible que algunos sistemas ya tengan instaladas actualizaciones automatizadas. La acción que debe adoptar depende de lo siguiente.

Si el software es compatible con las actualizaciones automáticas del anclaje de confianza de DNSSEC (RFC 5011):

La KSK debería haberse actualizado automáticamente en el momento adecuado. No necesita adoptar ninguna acción adicional.

Cabe mencionar que los dispositivos que están fuera de línea durante el traspaso tendrán que actualizarse de forma manual si vuelven a estar en línea tras la finalización del traspaso.

La ICANN comenzó a ofrecer un banco de prueba en marzo de 2017 para los operadores o cualquier parte interesada que deseen confirmar que sus sistemas pueden gestionar el proceso de actualización automatizado correctamente. Puede obtener más información en **https://icann.org/kskroll.**

Si el software no es compatible con las actualizaciones automáticas de los anclajes de confianza de DNSSEC (RFC 5011) o no está configurado para usarlos:

El archivo del anclaje de confianza del software debe actualizarse en forma manual. La nueva KSK de la zona raíz está disponible ahora en: **https://go.icann.org/2DOB7zn**.

¿Cuándo tendrá lugar el traspaso de la KSK?

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

11 de octubre de 2018

Fecha propuesta en la que la nueva KSK se utilizará para firmar por primera

11 de enero de 2019

Fecha propuesta para la revocación de la antigua KSK.

Para obtener más información sobre el traspaso, incluso sobre los recursos que lo ayudarán a prepararse para el cambio venidero, visite **https://icann.org/kskroll.**

También puede enviar un correo electrónico a **globalsupport@icann.org** con el asunto "KSK Rollover" (Traspaso de la KSK) o bien, unirse a la conversación en Twitter mediante el hashtag #KeyRoll (TraspasoClave).

Diseñado por el Equipo de Comunicaciones de la ICANN | Marzo de 2018