COPENHAGUE – Taller sobre las DNSSEC -- Parte 1
Miércoles, 15 de marzo de 2017 – 09:00 a 10:30 CET
ICANN58 | Copenhague, Dinamarca

ORADOR DESCONOCIDO: (…) importante para compartir con ustedes, especialmente si quieren almorzar. En sus lugares deberían tener un cupón. Si no, avísenme a mí o a Kathy. Ese cupón tiene un mapa detrás, que quizás quieran seguir o no. quizás les vaya mejor que a mí. O si no, simplemente busquen a alguien que sepa dónde queda. Queda enfrente de donde estamos ahora, del otro lado.

Verán que hay una pausa opcional, de 10:30 a 11:00. Vamos a continuar durante la pausa porque tenemos mucho contenido para cubrir, pero el que quiera puede levantarse en cualquier momento, irse a buscar un café o lo que sea. Si quieren tomarse una pausa a esa hora, no hay problema.

Ahora le voy a dar la palabra a Dan York, quien va a comenzar. Gracias.

DAN YORK: Buenos días. ¿Cómo están todos? Buen día. Ahora, sí. Muy bien. Es la mañana. Tenemos que empezar con esto. Vamos a ver si la

cámara me encuentra. Está tratando de encontrarme. A ver dónde estoy. No, para este lado. Voy a tratar de quedarme de este lado. Miren la cámara. Me está buscando. Se está acercando a mí. No puede hacer 360 grados. Sube, baja. Ahí está. Hola participantes remotos. Sé que hay participantes remotos.

Buenos días a todos. Tenemos un día muy intenso hoy. Como dijo Julie, vamos a trabajar durante la pausa también. Nos vamos a saltear la pausa. Matt es la victima de eso, así que si en ese momento quieren pararse. ¿Cuántos escucharon hablar acerca del traspaso de la clave? Ayer dijimos que él iba a tratar de aportar algo nuevo, algo que quizás no vieron antes, pero tenemos muchos. ¿Cuántos nunca participaron en un taller de DNSSEC? Algunos. Bienvenidos. Es bueno verlos acá. Alan, usted no cuenta.

Bueno, vamos a comenzar. Vamos a ver qué vamos a hacer. Esta sesión está acá a través del comité del programa. ¿Cuántos miembros del comité del programa están acá? Pueden culparlos a ellos, si quieren. Vamos a hacer otro taller resumido en el foro de políticas en Johannesburgo. La idea es que eso se fusione con el Tech Day, como hicimos la última vez. Así que si les interesa mostrar sus investigaciones a la comunidad y que los demás se enteren de lo que ustedes hacen, vamos a hacer un llamado para la presentación de propuestas pronto. También

tendremos un día completo en la reunión de Abu Dabi en noviembre. ¿Noviembre, octubre? Cuando sea. A final de año.

Esas son las personas con las que hemos estado trabajando en las llamadas semanales. También queremos agradecerles muchos a estas tres empresas. Veo a Jim, de Afilias; Jacques, de [incomprensible]; y Christian, al lado de SIDN. Queremos agradecerles a estas personas. Un aplauso para ellos. Ellos son la razón por la cual vamos a poder almorzar hoy acá y continuar interactuando y hablando sobre estos temas, así que muchas gracias a ellos.

Voy a decir que también estoy buscando a un cuarto sponsor para poder continuar. Si les interesa, contáctense conmigo. Hace falta una pequeña suma que nos ayudaría. Esta es una foto de anoche. Queremos agradecerle a Erwin. ¿Dónde está? Erwin, de punto DK. Un aplauso para ellos. Lamentablemente se nos ocurrió tomar la foto al final, cuando la mayoría se había ido. De pronto dijimos: “Un momento. Necesitamos una foto para las diapositivas”. Imagínense. A esa altura había poca gente. Antes éramos 30 o 40. Tuvimos conversaciones muy buenas. Pasamos cosas muy buenas. Gracias, Erwin.

También debo decir que cuando vayamos a Johannesburgo vamos a buscar a alguien para que actúe como sponsor para esa noche y también para Abu Dabi, así que es muy buen momento

para interactuar, para hacer networking, para conectarse. Esta es una actividad apoyada por el comité asesor de seguridad y estabilidad. El programa Internet Society Deploy 360.

¿A dónde estoy yendo? Ahí estamos. Entonces acá tenemos el programa. Ustedes tienen una copia. Deberían tenerlo ahí. Pueden ver que tenemos un panel fantástico acerca de lo que ocurre con DNSSEC en Europa. Yo voy a hacer una actualización acerca del IETF y la próxima reunión. Luego, Matt va a hablar acerca del traspaso de la clave. Y luego, vamos a hablar acerca de qué estamos haciendo con la validación con los ISP en relación con el traspaso de la clave para la firma de la llave. Vamos a ver qué están haciendo los ISP para prepararse. Luego, tendremos una demo a cargo de Paul [incomprensible]. Paul, y más tarde [Vittorio], van a hablar acerca del intercambio abierto entre ellos.

Roland va a hablar acerca de la implementación de ECDSA. Allá Roland va a hablar sobre eso. ¿Ven la camisa que tiene puesta? Trabajamos para algorithm 13 (algoritmo 13). Después Wes… ¿Wes está acá? sé que tenía otras reuniones. Pero Wes va a ser MC para el gran ejercicio de preguntas y respuestas del DNSSEC. ¿Deberíamos completar el formulario con respuestas ahora? Porque todos están invitados a participar y a divertirse. Después, vamos a terminar con otra demo, de la que no sé nada,

salvo que es sobre email seguro y encriptado una vez más. Así que vamos a tener cosas muy interesantes.

Ahí llegó Paul. Bueno, continuemos. Esto no funciona. ¿Tienen que ir tocando? Sí, funciona. No sé. Está pasando algo acá. Error, dice el operador.

Bueno, primero vamos a hablar acerca del estado de la implementación. ¿Cuántos de ustedes vieron el informe sobre el estado de la implementación DNSSEC? Es un muy buen informe, que creamos muchos de los que estamos acá con datos estadísticos, en relación con dónde estamos en términos de la implementación del DNSSEC. Les voy a mostrar algunos mapas, pero si quieren una descripción más detallada les diría que traten de leer este informe porque tratamos de ver cuál es la línea. Este es el punto en el que estamos con la implementación del DNSSEC ahora. Mi organización está comprometida con la relación de una actualización de 2017. Vamos a tratar de terminar antes de la reunión de Abu Dabi para que ustedes sepan cuál es el punto en el que llegamos en 2017, cuál es el crecimiento observado, hasta dónde llegamos, así que por favor léanlo.

Quizás tengo que acercarme un poco más. Muy bien. Vamos a ver dónde estamos ahora. Vamos a ver los datos estadísticos. Acá tenemos el mapa de Jeff Houston con respecto de la

validación del DNSSEC. Él lo mantiene en línea. Estamos en un 14-15%. Ese es el promedio global. Varía en algunas partes. Vemos lo que pasa en Europa y lo que pasa a nivel global. Pueden ver dónde ocurre la validación global.

Para poder entender esto, el mapa de Jeff, tienen que hacer lo siguiente. En la primera columna tenemos el porcentaje de validación que él observa en esas regiones. Y aquí a la derecha donde dice "use Google's PDNS" tienen otro porcentaje. En algunos países donde vemos un alto porcentaje eso significa que los ISP locales no están haciendo validación, sino que la actualizan en Google. Pero fíjense acá en Europa occidental el uso DNSSEC está en un 7%. Eso muestra que muchos de los ISP están haciendo la validación local por su cuenta, que es lo que queremos porque queremos que los ISP locales hagan eso.

Esto es entonces el panorama global. Si se fijan en el panorama europeo… Ahí estamos. Uno para atrás. Muy bien. Acá estamos. Las islas [incomprensible], que están cerca de Islandia. ¿Más al norte? Perdimos un partido de futbol contra ellos. Esa es la parte importante que tenemos que saber. Ellos encabezan los datos estadísticos de Jeff Houston, con un 86% de todas las consultas de DNS que provienen de las islas. No sé cuántos hay, pero ese es el porcentaje. Pueden ver Dinamarca, que también está ahí. De nuevo estamos viendo los datos estadísticos, que en general van bajando en el DNSSEC de Google, lo que indica que

los ISP en esa región están haciendo gran parte de la validación, que es lo que buscamos.

Eso con respecto a la validación. Vamos a hablar acerca de la firma. Esto es de Rick Lamb. ¿Rick está acá? No lo vi. Cuando lo vean, pueden agradecerle por haber preparado este muy buen informe.

Uy, me están traduciendo y estoy hablando muy rápidamente, así que seguramente les estoy dando mucho trabajo. Bueno, vamos a hablar más despacio. No tan despacio.

Este informe muestra que la cantidad de dominios firmados. El gran salto es con los nuevos gTLD que fueron firmados. Entonces vamos a pasar a la próxima. Acá vemos la cantidad de dominios firmados y después, en los datos estadísticos de Rick, vamos a ver más esta información. ISDN… Christian, ¿qué es esto? Yo señalo a alguien y de pronto ese alguien desaparece. Christian estaba al lado de Jack. Bueno, sí. Todos los holandeses están acá. Todos los holandeses se corrieron de lugar.

Punto NL sigue teniendo la mayor cantidad de dominios con 2,4 millones. Después viene Brasil, y ya pueden ver los otros. Punto CZ. Andre, ¿está ahí? Él no se corrió. Estos números están en el sitio de Rick. Si quieren tener esta diapositiva tan linda que tengo yo acá, tienen que ir al sitio correcto de Rick, donde dice sign barra total. Si hacen clic en la columna “firmado total”, van

a tener esos datos. Si se fijan en ese gráfico y ven que su país no está representado ahí, entonces pueden enviarle un email a Rick, y quizás él trabaje con ustedes para incorporar al país. Rick está tratando de incorporar más datos estadísticos para poder mostrar los resultados más completos.

Pasemos a la siguiente. Estos son los nuevos gTLD. Nos gusta mostrar estos datos estadísticos para ver dónde están los nuevos gTLD en relación con el DNSSEC. En la parte superior los dominios firmados siguen siendo punto OVH, que es un proveedor de hosting, que ha tenido muy en cuenta la seguridad en términos generales.

Continuemos. Quiero hablar acerca de los mapas que tenemos acá. Los mapas que hacemos, para aquellos que no los conocen, se dividen en estas categorías. Los datos estadísticos que nosotros conocemos son si algo es experimental, si ya fue anunciado, si ya comenzaron a trabajar, si ya fue implementado de alguna manera u otra.

Continuemos. Ese es el mundo en general hoy en términos de ccTLD. En términos generales podemos ver que estamos bastante bien. A excepción de África, la mayoría de las regiones del mundo están firmando muy bien en muchas áreas. África, Sudamérica, algunas partes de Asia todavía necesitan mejorar un poco. Esta es la situación de África en este momento. La

buena noticia es que desde la última reunión incorporamos a Sudáfrica. ¿Hay alguien de Sudáfrica acá? Ellos hace rato están trabajando para poder llegar a la firma y lo lograron en diciembre, así que ya está firmado. También hay talleres que se están organizando. Rick fue a muchos países este año y trabajó con los ccTLD locales para lograr las firmas.

Pasemos a la siguiente. Asia Pacifico. Tenemos algunos que acaban de firmar. Hong Kong, Vietnam firmaron en diciembre. Samoa, en enero.

Continuemos. Europa. Está parecido a la última vez. América Latina continúa avanzando. Continuemos. Norteamérica, lo mismo.

Adelante. Estos mapas están disponibles. Se pueden suscribir. Se publican todos los lunes a la mañana. Ustedes pueden participar y mirar lo que ocurre. Continuemos. Esto ya lo mencioné. Continuemos.

Tenemos este proyecto sobre la historia. Buscamos voluntarios que quieran contribuir a este proyecto. La siguiente.

Eso es todo. Es todo lo que había preparado para esta mañana. ¿Alguien tiene alguna pregunta o comentario al respecto?

MARK: Observé que usted tiene punto EG en el mapa. ¿Observé correctamente? Punto EG de Egipto.

DAN YORK: Sí.

MARK: ¿Qué significa eso? porque nosotros somos un registrador de punto EG, pero no permiten acceso a la API para nosotros. Me preguntaba cómo funciona DNSSEC en esas circunstancias. Por lo que sé, no tienen acceso directo al sistema. Pasa por front-end o por nuestro contexto en el registro EG.

DAN YORK: Usted hace una pregunta excelente. El mapa hace un seguimiento de si el DNSSEC está firmado, pero no indica necesariamente si personas como usted pueden trabajar con el registro y descargar registros DS. Es una buena pregunta.

Volvamos al mapa de África. ¿Egipto está en etapa operativa? ¿Estaba en verde oscuro o verde claro? Es verde claro, lo cual significa que el DS fue firmado. Ya está en la raíz. No lo ponemos en verde oscuro en la etapa operativa hasta que verifiquemos que personas como usted pueden descargar los registros DS.

MARK: Es decir, que solo está en verde oscuro cuando está operativo y cuando se puede acceder.

DAN YORK: Sí. Si ven un país en verde claro y ustedes saben que pueden descargar los registros DS, contáctense conmigo porque el cambio de la raíz de DS a la parte operativa muchas veces, para enterarnos de eso, tenemos que enterarnos otra vez de otras personas que nos dicen que funciona de esa forma. Todavía no cambiamos a Egipto porque no lo sabemos. Desde el punto de vista operativo, sabemos cuándo hay un DS en la raíz, pero eso es todo.

Bueno, ahora le voy a dar la palabra al siguiente panel regional. ¿Están todos acá? Para los que acaban de llegar, esta es una sesión informal. Nos gusta que nos hagan preguntas, así que si tienen alguna pregunta, siéntanse libres, acérquense al micrófono y hagan las preguntas. No mordemos, ni hacemos nada por el estilo en general.

Yo también soy el moderador de este panel. Ah, bueno. Me voy a sentar acá porque seguramente no me van a querer ver parado al frente. Cuando hacemos estos talleres de DNSSEC, nos gusta que haya un panel que reúna a personas del área en la que estamos y nos cuenten acerca de lo que ocurre con DNSSEC. Tenemos acá a los miembros del panel sentados al frente. Por lo

tanto, voy a comenzar dándole la palabra a Andre, quien va a hablar acerca de lo que está ocurriendo en la Republica Checa.

ANDRE: Muchas gracias. Soy Andre [incomprensible], del registro punto CZ. Voy a dar una actualización acerca de lo que está ocurriendo en la Republica Checa.

Creo que ya se dijo que ya la mitad de los registros firmaron, la mitad de los dominios checos. Es necesario encontrar una forma de obligar a los registradores a firmar los dominios. La parte más compleja es convencer a la segunda mitad de los dominios. Estamos trabajando en esto. Estamos trabajando mucho. No es fácil. Principalmente estamos tratando de trabajar con algunos sitios de alto perfil, como bancos y periódicos, y tratamos de explicarles por qué es tan importante y por qué deberían hacerlo. Estamos creciendo, pero el crecimiento no va a ser tan rápido como lo fue antes.

También estamos haciendo lobbying en el país para comunicar información acerca de DNSSEC. Estamos teniendo bastante éxito en cuanto a incorporar DNSSEC en la estrategia gubernamental, en digital [incomprensible] 2.0, y también estamos tratando con la estrategia de seguridad cibernética. El gobierno debería firmar el dominio y el porcentaje de dominios firmados en sitios gubernamentales es más alto que en los otros

sitios. Eso es muy bueno. Además, la validación del DNSSEC se incorporó a los estándares para las conexiones con instituciones públicas. En este momento podemos decir que DNSSEC es casi obligatorio en el país, al menos se recomienda enfáticamente.

Otra buena actividad, otra actividad interesante, es el punto de intercambio nic punto CZ. Este punto de intercambio tienen un grupo de ISP que tienen estándares de seguridad más altos. Esos ISP ocupan un espacio especial dentro del intercambio de información. Para unirse a este club es necesario cumplir determinados requerimientos. La validación del DNSSEC y la firma para los nuevos dominios es un requerimiento. En este grupo, que está creciendo en todo el país, DNSSEC es casi obligatorio.

La próxima diapositiva, por favor. Las mediciones de validación también estamos en el 50% de los resolutores. Los números han cambiado últimamente. Tratamos de hablar con los ISP locales. Somos muy activos en las actividades organizadas por el punto de intercambio local. Solemos tener reuniones relacionadas con estos puntos de intercambio. O sea, intentamos educar a los ISP y convencerlos de comenzar con la validación por DNSSEC. Lo bueno es que por ejemplo todos los operadores móviles validan. Los grandes entonces tienen validación.

También tenemos mucho software de código abierto. Uno de ellos se llama not DNS, que es un servidor alternativo bastante estable para algunos operadores de servidores raíz. Este año intentamos brindar apoyo para los algoritmos EDDSA, que dependen de las múltiples bibliotecas. Para los nuevos TLD añadimos esta característica not DNS. Y también queremos dar apoyo para el traspaso de la llave, incluyendo CDS y CDN key. En este momento tenemos un mecanismo para la firma automática. Entonces el plan es brindar apoyo para el traspaso de la clave.

La segunda parte, el segundo software, es el not resolvable. Para este año tenemos una funcionalidad interesante relacionada con el DNSSEC. Uno es la implementación del RFC 7706, que requiere implementar una copia de la zona raíz en el [incomprensible], y así se aceleraría la velocidad y disminuiría la carga sobre la zona. Otra cosa es el RFC 8020 más un borrador del uso agresivo de la calle validada por DNSSEC. Cualquier cosa por debajo del nodo, si no existe es RFC 8020, y el uso agresivo de la calle validada por DNSSEC es la forma de manejarlo a través de una síntesis del punto de acceso a los clientes.

Por último, ya implementamos DNS sobre TLS. Es para clientes. Si tengo un cliente que hace recursivo, uso TLS para comunicarme y también para lo que es DNS sobre TLS saliente. O sea, desde el resolutor. Eso lo tendremos este año.

Ahí hay un error de tipeo. Pido disculpas. Nos estamos preparando para lo que es ECSA. Alrededor de 30.000 dominios están firmados por ECSA. Queremos hacer un segundo algoritmo. El traspaso por segundo algoritmo. Entonces estamos preparando la comunidad, comunicándolo a los ISP, como decía, en las reuniones con los IXP, con los puntos de intercambio. También hacemos conferencias. Pero el problema es que la IANA implementó una funcionalidad en la API, así que estamos esperando y con mucha cortesía estamos diciendo: "Señores, sería bueno si lo implementan rápido".

Otra cosa. La cadena de validación. Creamos un [incomprensible] para la cadena de validación para apoyar la conexión con IPv6. Y tenemos otra funcionalidad que indica que esta validado con ambos algoritmos principales y también con ECDSA. Si no soporta ECDSA el sistema se muestra que el botón no está verde. No rojo, sino algo diferente que dice que el resolutor soporta DNSSEC, pero no ECDSA. Así es como nosotros intentamos proveer la información.

Siguiente. Bueno, eso es todo. Muchas gracias.

DAN YORK: Gracias, Andre. Dos preguntas. ¿Puedes contarnos este tema de la IANA es que no apoyan el algoritmo 13?

ANDRE: Sí. No brindan apoyo para el algoritmo 13.

DAN YORK: Bueno, tenemos que ver cómo resolverlo. Otra pregunta. Ustedes hablaron de digital check 2.0 (República Checa digital 2.0). ¿Ya está pasando?

ANDRE: Sí. Es una estrategia nacional para el mundo digital.

DAN YORK: Entonces es parte del plan. ¿Alguna pregunta para Andre?

KIM DAVIES: Estamos trabajando para el apoyo bajo EDSA. Hay implementaciones maduras. Como saben, trabajamos con VeriSign. Me gustaría saber más detalles al respecto. Es un trabajo en curso.

ANDRE: Es importante no solo tener buena calidad, sino también trabajar con rapidez.

KIM DAVIES: No pido una fecha. No tengo una fecha que darle en este momento.

DAN YORK: Si por favor se presenta.

KIM DAVIES: Kim Davies, de IANA.

DAN YORK: Qué bueno tener gente en la sala cuando surgen temas como este. Gracias, Kim, por el comentario.

Ahora tenemos a Peter Koch, que va a hablar de punto DE y de DENIC.

PETER KOCH: Quiero agradecer al comité por la invitación para hacer otra actualización de lo que está pasando con DNSSEC en Alemania, con el dominio punto DE en particular.

Un poquito de antecedentes históricos. Comenzamos el despliegue pleno en mayo de 2012. Ya estamos en el sexto aniversario. Operamos sobre la base de la registración de los registros de clave por DNS key. Los registradores y registratarios no presentan los registros, sino que nosotros los recibimos

como hacen los checos. Configuramos hasta cinco claves. La mayoría de las veces la gente presenta una o dos. En el traspaso tuvimos un caso de alguien que presentó cinco claves. Y le dijimos: "Oiga, ¿qué está haciendo? Qué interesante". Y entonces nos dijeron que se habían equivocado en el sistema de presentación. Por otra parte significa mayor seguridad de limitación.

Aplicamos verificaciones de validación en el momento de la registración, como lo que explicaba Kim para la raíz, lo cual está alineado con nuestras verificaciones previas a la delegación, no DNSSEC. Lo que hacemos es verificar la cadena con dos registros que se validan, por lo menos con una clave presentada. Entonces esto sucede con todos los traspasos de llave.

Nosotros no encontramos la necesidad de dar apoyo para el registro [incomprensible]. Esto no se mencionó todavía, que es el RFC 8063, que está basado en EPP, que es un documento de un colega del ISDN y otro colega con el cual yo trabajé hace un par de años, que explica cómo hacer un cambio de operador sin pasar a tener inseguridad. Nuestro sistema de registración lo apoya en general por los aspectos intrínsecos que tiene nuestro sistema. Si les interesan los detalles, contáctenme aparte.

Pasó que tuvimos varios de estos cambios de operador, que eran seguros, y otros con problemas. Después daré más detalles.

En lo que hace al lado de los registradores, no hay proceso de acreditación. No requerimos firma para apoyo con DNSSEC. Simplemente lo hacen. Esto tiene que ver probablemente con las características de nuestro sistema de registración porque en general operamos un objeto de dominio completo. Es decir, alguien presenta un objeto con información del DNSSEC. Si el registrador cambia y el registrador no soporta DNSSEC, simplemente no presenta la información del DNSSEC y el dominio no está firmado. Pero con el cambio, por lo menos los clientes van a tener conocimiento.

Estos son los números. Como hablamos tanto de dominios firmados, esto es lo que tenemos. Esto es hasta el 2011, cuando empezamos. Acá de hecho vemos dos colores. El azul claro de abajo son el número de zonas con claves registradas o, como decimos coloquialmente, las delegaciones firmadas. 34.000, o 36.000 eran hace 10 minutos. Es un crecimiento constante. Hacia la derecha del grafico vemos que surgió cierto optimismo. El crecimiento se ha venido acelerando en los últimos 5 o 6 meses. No podemos explicarlo de ninguna manera específica. Simplemente vemos que está aumentando en amplitud. Cada vez más registradores trabajan en los registradores más grandes y celebramos esta participación.

Hay otro cambio que fue a mediados del 2015, cuando fue el día de DNSSEC, en cooperación con la autoridad de portales y un

par de registradores en esa oportunidad sintieron el incentivo de firmar todos los dominios. Eso explicó ese salto. Ahora lo interesante para nosotros, además del crecimiento, otro aspecto interesante que quería señalar son las barras rojas, que son los números de dominio que están firmados cuando encontramos material de clave en la zona que todavía no ha sido registrado con nosotros. Esto en parte es algo natural porque cuando se firma la cartera de dominios, primero se firma, luego se hace una prueba y se registra después. Pero estamos trasladando partes de estos hace meses, hablando con los registradores. A veces son los revendedores más grandes que hacen DNSSEC por un motivo u otro y luego esperan a hablar con los registradores, etc.

Entonces estamos ahora alentando a esta gente a que presenten el material de la clave. En este momento, hasta ahora no hemos tenido obstáculos, ni técnicos ni de procedimiento. No sé. A lo mejor la gente es tímida. Así es. La siguiente.

DAN YORK: No sé. Parece ser 20.000 dominios punto DE que no tienen registro DNSSEC.

PETER KOCH: Sí. Son unos 20.000 más, que es un tercio en comparación.

Las últimas actividades, las observaciones el año pasado, 2016. Cambiamos nuestro HSM, tanto para el KSK y la clave de firma de la zona. Quizás algunos aquí en la mesa o en el público recuerdan que usábamos ese [incomprensible] 6.000, pero no teníamos soporte. Entonces pasamos a una safe net la luna, que adquirió [incomprensible] systems y pasamos a esta tecnología. Esto implicó un traspaso de la KSK y de la ZSK, que tuvo lugar en agosto de 2016.

El resto lo conservamos. Seguimos con los SRA, en especial porque pensábamos que convenía esperar que las curvas elípticas y todo lo demás adquiriera ritmo. En cuanto al número de registraciones, un aspecto especial, también tenemos una funcionalidad que permite tener datos actualizados en la zona DE inmediatamente, hasta cinco registros por dominio. Muchos lo usan. También uno de nuestros registros. Tenemos más de 230.000 dominios en la zona DE, que de algún modo, por así decirse, firmaron accidentalmente. Ahora son casi 300.000 y las delegaciones firmadas son más de 64.000, que es un porcentaje menor del número de dominios.

En gran parte esto es impulsado por los registradores o debiera decir por el operador del DNS dentro del registrador. Vemos lotes de asientos o de unos pocos miles de dominios que han venido entrando a ser firmados en las últimas semanas desde la infraestructura operada por el registrador. A veces el cliente

sabe qué ocurre. A veces simplemente tiene que tildar un casillero. Mientras tanto tenemos un gran registrador con decenas de miles, que ha comenzado a migrar a DNSSEC. Entonces esperamos ver un crecimiento abrupto a finales de año. No obstante, sigue siendo impulsado por el operador. No obstante, hay una división entre lo que es KSK y ZSK, aun cuando en unificación sería más sencillo.

Hablando de algoritmos, la mayoría utiliza RSA. Ambos, el [incomprensible] tres, que es el número 7, que está arriba, y el 256. El algoritmo 13 no está para todos. Hay por lo menos un registrador que cae en esta categoría que firmó todos los dominios y utiliza el algoritmo 13 de curva elíptica. A la derecha, abajo, vemos un 0%, un puñadito de dominios con el algoritmo 14. El 5 RSA y el 10 RSA 512, con un 1%. Soportamos [incomprensible] y el 3DSA. Hay un registro con dominio [incomprensible]. Es un dominio de prueba propio. Y uno o dos DSA, pero por el nombre del dominio hay indicaciones de que es alguien que lo está testeando no para un propósito en particular.

Como decía Kim también, como hacemos validación, tenemos que dar soporte explícito a validación en el software. Aun cuando los algoritmos 15 y 16 ya están estandarizados todavía no hay implementación de nuestra parte. Podemos soportarlo,

pero en especial el ED 25519 caerá en nuestro ámbito de trabajo a finales de año.

Números de vuelta, empezando de abajo para arriba. En el 2013 teníamos aproximadamente 300 registradores, 42 de ellos tenían por lo menos un dominio firmado y registrado. Estamos todavía en el rango de unos 300 registradores. Vemos una fracción que soporta DNSSEC, una fracción que está creciendo. En este momento tenemos 109. Cuando digo por lo menos un dominio bajo administración, aparece en este gráfico. El eje Y llega hasta unos 16.000 y pico de registradores, que va hasta abajo. Y a la derecha, los 20 pilares que no se ven son los que tienen un único domino bajo administración. A la izquierda del gráfico, podemos reconocer que hay un puñado de registradores que contribuyen la mayoría de los números. Esto es por distribución por número de dominios. Espero que esto no se contradiga con lo que decía antes, que es impulsado por los registradores, que cada vez más registradores (un tercio ya) soportan DNSSEC.

La próxima. Bueno, creo que esto era todo. ¿Preguntas?

DAN YORK: ¿Alguna pregunta para Peter? Vamos, no pueden dejar que se vaya así tan fácil. Pregunten en alemán.

ORADOR DESCONOCIDO: Una pregunta. Usted habló acerca de un SDSA que apoya a un registrador. ¿Fue único en la región?

PETER KOCH: La verdad, no lo sé. No lo recuerdo de memoria.

Hablando de Holanda, debería decir que la mayoría de los registradores que apoyan DNSSEC son holandeses. Tenemos que darles el crédito que se merecen y debemos entender que la mayor parte de este crecimiento probablemente sea un efecto colateral de la iniciativa de los SDIN de convencer a sus propios registradores. Así que, sí, gracias por la pregunta.

ORADOR DESCONOCIDO: Una última pregunta. ¿Tendrían más registraciones si tuvieran EPP?

PETER KOCH: ¿Se refiere a más de 16 millones de dominios? No lo creemos, pero probablemente esa no era la pregunta.

No es que nadie haya expresado interés en dominios del lado del cliente o del lado de los registradores. No hay nada que los detendría, excepto que no hay interés, no hay tiempo, no hay

nada. Pero no hay nada sobre lo que nosotros pudiéramos influir, al menos por lo que sabemos.

DAN YORK: Muy bien, Peter. Muchas gracias.

Ahora viene el anfitrión de nuestra reunión de anoche. El país local, Dinamarca. Erwin Lansing va a hablar sobre punto DK. Le agradeceríamos que hablara en inglés.

ERWIN LANSING: Bienvenidos a Copenhague todos. Comenzamos a hacer DNSSEC en 2010, dos meses después de que se firmó la raíz. Después de seis años era hora de cambiar algunas cosas. Por lo tanto, nuestro tema el año pasado incluyó varios temas. Tenemos una lista extensa. Tengo que agradecerle a Jack por la idea. Nosotros dejamos que nuestros registratarios se contacten directamente con nosotros a través de nuestro portal de autoservicio. En lugar de que hagan copy and paste con long hashes, agregamos una nueva funcionalidad que se llama import DNS key (importar). Podemos buscar las claves en nuestra base de datos, calcular lo necesario y mostrarle al usuario esto: “Encontramos esta clave. ¿Cuál quiere? ¿Más fácil? ¿Menos posibilidades de que haya errores de tipeo o de que haya problemas con las claves?”

Próxima diapositiva. Cuando lanzamos nuestro portal de autoservicio hicimos algunos cambios también para DNSSEC. En nuestro sistema de registros pedimos que todos los nombres tienen que ser registrados en nuestra compañía. Es decir, sabemos el nombre del operador, que es NSA, y también el operador puede manejar las claves DNSSEC. Ellos pueden desactivar esto posteriormente, pero de manera predeterminada el operador puede manejar las claves DNSSEC en nombre de los registratarios, sin tener que pasar por el registrador.

Nos conectamos con los medios tecnológicos. Esto fue muy divertido porque el periodista pensaba que podía cambiar un poco lo que yo dije y acá dice: “Los proveedores daneses descuidan la seguridad DNSSEC. Menos de un 1% tienen la firma DNSSEC”. No estaban contentos, pero sí obtuvimos mucha atención. Es decir, que aparecer en los medios es algo que funciona. Luego, agregamos algoritmos más nuevos. Luego de recibir el aliento de algunas personas que están acá. Así que ahora tenemos 13, 14. Tenemos planificado también después tener soporte para 15, 16 más adelante este año.

Para nosotros la implementación de EPP fue un poco baja, con pocas funcionalidades. Nuestros registradores registraron nuevos nombres de dominios, extendimos el lanzamiento de

EPP este año en el otoño. Una de las funcionalidades es que pueden agregar claves DNS y eliminarlas también.

La próxima, por favor. No fue planificado, pero organizamos un taller año por medio. Es un taller de un día completo. Un taller técnico con parte práctica también. La teoría sobre DNSSEC y también la parte practica con [open] DNSSEC. Datos estadísticos. A todos nos encantan los datos estadísticos. Esto es diferente de lo de ustedes, Peter, porque la mayoría de los algoritmos son 13. Él sigue encontrando bugs en nuestro sistema.

La razón está en la próxima diapositiva. Debido a todas las implementaciones técnicas que hicimos empezamos a hablar con los registradores acerca de firmar todas las zonas. Pueden ver que la mayoría de los dominios fueron firmados recientemente en los últimos dos meses y esos registradores utilizan algoritmo 13. Ahora estamos llegamos al 5% de los dominios firmados y creo que somos el CC más grande sin incentivos, lo cual es algo muy singular. La mayoría de los registradores están malcriados. Cuando hablamos con ellos nos dicen: “Dennos dinero”. Y nosotros decimos: “Bueno, ustedes ya tienen la implementación. ¿Por qué no la hacen simplemente porque va a ser bueno para sus usuarios?”. Así que encontramos algunos registradores más chicos que lo están haciendo. Ahora llegamos al 5% y seguimos hablando con todos los demás y

decidimos no brindar incentivos monetarios y esperamos que lo hagan por su cuenta.

Igual que ustedes, Peter, vamos a recomendar a la gente que miren sus dominios, sus usuarios. Encontré un registrador con un par de miles de dominios firmados, pero no tenemos las claves para ellos, así que vamos a hablar con ellos.

Y creo que esta fue mi última diapositiva. ¿Alguna pregunta?

DAN YORK: ¿Alguna pregunta para Erwin? A todos les encantan Copenhague, así que no quieren irritar a los locales. Vamos, tiene que haber alguna pregunta para Erwin.

ORADOR DESCONOCIDO: Es muy bueno, Erwin, que nos ofrezca descargar las claves, aun cuando no somos registradores en punto DK. Muchas gracias y esperamos que otros sigan su buen ejemplo.

CHRISTIAN: ¿Cómo les está yendo a los ISP de Dinamarca, en términos de validación del DNSSEC?

ERWIN LANSING: Tenemos tres ISP importantes en Dinamarca. Dos están validando. El tercero, todavía no. estamos hablando con ellos. Así que digamos que tenemos un 50%.

CHRISTIAN: Interesante. La situación es al revés en Holanda. Tenemos una gran cantidad de nombres de dominio firmados, pero no hay muchos ISP que estén validando todavía. Es interesante.

¿Quiere corregirme?

DAN YORK: Para aquellos que están participando en forma remota, este fue un intercambio entre dos holandeses que están sentados en los dos extremos de la mesa. En inglés. Sí.

Christian, entonces ¿no hay ISP en Holanda que estén haciendo la validación nativa?

CHRISTIAN: Todavía no. hay algunos rumores de que un ISP importante va a empezar a hacerlo este año en algún momento. Si lo hacen, eso sería una muy buen noticia. Esperamos que esto lleve a otros ISP a seguir el ejemplo.

DAN YORK: Muy bien. Adelante, Erwin.

ERWIN LANSING: Tengo un comentario final. Lamentablemente me quedé sin remera, pero si quieren traer remeras tenemos muchas remeras con el algoritmo 13 en nuestro stand, así que pueden pasar a retirarla.

DAN YORK: Si quieren una remera de mujer, que diga algoritmo 13, pueden ir al stand de punto DK y les van a dar una remera de talle de mujer. Para quienes están participando de forma remota, Erwin no está mostrando una remera que dice “Queremos a punto DK”.

ERWIN LANSING: Tenemos diferentes temas.

DAN YORK: Ah, ¿hay diferentes temas? Tenemos que poner en la promoción que si pasan por el stand les vamos a dar una bufanda de DNS muy adecuada para el frio. Jacques me va a corregir.

JACQUES: Casi nos quedamos sin.

DAN YORK: Uy, se están quedando sin. Bueno, nos estamos quedando con poco material. Bueno, habiendo dicho esto, vamos a pasar a otro país, que va a hablar sobre esto. Alex va a hablar sobre DNSSEC en Austria.

ALEXANDER MAYRHOFER: Gracias, Dan. Buenos días a todos. Si se fijan en el formato de las diapositivas, van a ver que no cambiaron mucho desde la última vez que di esta presentación en 2014, lo cual demuestra, debo admitir… Lo voy a decir de forma positiva: Somos uno de los registros que está logrando un crecimiento orgánico en DNSSEC. No hay muchas actividades, pero les voy a dar un poco de información detallada sobre el tema.

La próxima diapositiva, por favor. ¿En qué áreas brindamos servicios de DNSSEC? Obviamente en relación con ccTLD punto AT y tenemos DNSSEC en producción desde febrero de 2012. También usamos open DNSSEC. Ofrecemos a nuestros registradores que descarguen los registros DS, con la extensión EPP. También operamos un producto que se llama registry in a box. Es un servicio de back-end de registros para nueve nuevos gTLD que operamos. Como seguramente sabrán, DNSSEC es obligatorio para los nuevos gTLD. Por lo tanto, tenemos open

DNSSEC para esos TLD también y permitimos que se descarguen registros de DS.

Algo que también operamos es nuestra red en [icast], que les ofrecemos a los clientes. Si no vieron todavía nuestra wiki, América First, lo recomendamos. También tenemos bump in the wire signing para los clientes. Utilizamos [incomprensible]. No me pregunten por qué. Eso es lo que decidió nuestro departamento de ingeniería. Es gratuito. Está incluido en el servicio. Algunos de estos registradores nos contrataron a nosotros porque eran demasiado haraganes como para implementar la firma ellos mismos. Por eso, contrataron este servicio.

La próxima diapositiva, por favor. Esta es una recapitulación de la línea de tiempo. Como pueden ver, tenemos banco de prueba. Algunos implementaron en forma deliberada la zona. Después lo implementamos en la raíz y empezamos con EPP un par de semanas después.

Datos estadísticos de registradores. A partir de marzo de 2017 tenemos 405 registradores. Perdimos un par de registradores desde 2014, principalmente debido a que introdujimos un arancel mínimo para los registradores, lo cual dejó afuera a algunos que eran muy pequeños. ¿Qué tenemos nosotros de especial? Pedimos a nuestros registradores que indiquen si

brindan soporte para DNSSEC o no y lo que ocurre en realidad… Podríamos hablar sobre este tema. Pero cuando vemos una transferencia a un registrador que no tiene DNSSEC activado, sacamos el registro DS de la zona. Esta es una decisión de política que tomamos en 2012. Probablemente haya que hacer una revisión de esto.

La buena noticia es que de los 405 registradores hay unos 20 más que decidieron decir: "Sí. Damos soporte para DNSSEC". De hecho, 43 de ellos. Sí, esto es marketing. Casi el doble que en 2013. Tenemos un dominio habilitado con DNSSEC. Entonces, como dije, nunca en realidad les dimos a los registradores ningún incentivo monetario para activar DNSSEC. Muy pocos firmaron nombres de dominio, pero mirando las cifras de 2014 vemos cuál es nuestro inventario. Y tenemos una buena noticia. Acá vemos la línea de tiempo. Fíjense el salto en los dominios que tiene el DNSSEC en 2015. Al parecer, eso coincide con la actividad en DNSSEC. Eso tiene sentido porque muchos de los registradores más grandes están basados en Alemania. Entonces al parecer [Nick] hizo muy buen trabajo para nosotros en cuanto a aumentar la cantidad de dominios firmados con DNSSEC. 50% en un mes, así que muchas gracias. Los vamos a buscar como sponsor la próxima vez.

También vemos algo interesante. Hay un número muy pequeño en el extremo del gráfico. Vemos un crecimiento acelerado en

cantidad de registraciones. Registradores. Esta no es una escala logarítmica. No es lineal. Vemos lo que coincide con las presentaciones de los demás. Vemos que está dominado por los más grandes. Hay unos cuantos que simplemente tienen dominio de prueba, que tienen una persona técnica a la que le gusta agregar DNSSEC a su dominio, pero la mayoría de las registraciones provienen de los 5 o 6 principales.

Entonces ¿qué hicimos recientemente? Sacamos los registros DS [incomprensible] de la zona raíz, hicimos un par de traspasos de KSK obviamente y pudimos brindar soporte para algoritmos 13 y 14 en EPP hace poco tiempo. Creo que hace un par de semanas. Lo que tenemos que tener en cuenta es la posibilidad de hacer un trabajo con la gente local de DNSSEC para ver cuál es la forma de hacer el traspaso de la clave para la firma de la llave. Es algo que se me ocurrió últimamente. Es una idea.

La siguiente es la última. Muchas gracias por su atención. Eso es todo.

DAN YORK: Muchas gracias con respecto a la información acerca de lo que ocurre en Austria. ¿Alguien tiene alguna pregunta para Alexander?

ORADOR DESCONOCIDO: ¿Cuándo fue que empezaron a trabajar con el algoritmo 13 barra 14?

ALEXANDER MAYRHOFER: Tengo que buscarlo. Fue hace un par de semanas, creo.

ORADOR DESCONOCIDO: Muy bien. Gracias.

DAN YORK: ¿Alguna otra pregunta? Vamos, gente. ¿Alguna pregunta para cualquier miembro del panel? Yo tengo una, si a nadie más se le ocurre. Así que que alguien haga una pregunta. Phil, ¿usted no tiene una pregunta? ¿Algún otro? Bueno, entonces mi pregunta básicamente es la siguiente. Si pensamos en todas las presentaciones que escuchamos, tengo una pregunta general. ¿Qué les parece que se puede hacer para que más registradores se ocupen de la firma? ¿Qué es lo que ustedes observaron en su espacio?

ERWIN LANSING: Lo que nosotros observamos en Dinamarca es que sirve hablar con los registradores, hablar acerca de los obstáculos, que pueden ser obstáculos técnicos, que tienen que ver con EPP. Tenemos un servicio diferente que se llama DS upload. Es una

API muy simple, en donde se publica la cadena de caracteres. Se publica y se dice “esta es mi clave”. Eso es todo. Ahora tenemos registradores que dicen “queremos EPP”. Puede ser una API simple, pero es diferente. Entonces agregamos EPP y puede haber otras cosas. Puede ser políticas. Hablamos con los registradores. Hay que ver cuáles son los obstáculos desde el punto de vista de las políticas. Y hablamos con ellos acerca de la necesidad de empezar a hacerlo, simplificarles las cosas para que lo puedan hacer.

ORADOR DESCONOCIDO: Lo interesante es que cuando hablo con los registradores muchas veces no se trata de una decisión técnica. Lo que ocurre a veces es que la gente de marketing les informa que hay un competidor, que está publicando que tiene una verificación más, un punto más, algo más que ofrece que se llama DNSSEC. Entonces el departamento de marketing habla con los ingenieros y les dice: “Nosotros no tenemos eso en nuestra descripción de productos. ¿Qué es?”. Los ingenieros dicen: “¡Uf! Bueno, está bien”. Ahí es cuando se acercan a nosotros y nos piden por ejemplo que les demos el bump in the wire.

Es difícil convencerlos de que hay una ventaja técnica en eso porque ellos lo ven como una carga administrativa. Es algo que todavía tiene que pasar, especialmente dado que hace años que

venimos hablando de esto y todavía no es un producto que vende. Entonces en la mayoría de los casos es algo impulsado por marketing, lo cual realmente es curioso.

DAN YORK: Hay que hablar entonces con la gente de comunicaciones de marketing.

PETER KOCH: Al igual que Alex, me gusta el término crecimiento orgánico. Creo que eso es lo que nosotros estamos viendo en punto DE también. También resistimos la tentación de buscar incentivos financieros. Un registrador por lo menos lo pidió. Y honestamente esto sería algo que no podríamos hacer en función de nuestro modelo financiero. No lo podríamos hacer, pero además no tiene sentido porque hay otros que ya lo hicieron y los estaríamos castigando. Los estaríamos poniendo en desventaja.

También vemos que probablemente no sea tanto una cuestión técnica, especialmente considerando que ya tenemos unos 20.000 dominios firmados. Lo que me olvidé de decir es que a veces hay cientos de dominios que están en el registrador, que ya está administrando varios miles de dominios. Entonces con frecuencia es un tema de comunicación para ser neutral entre

registradores y revendedores o los clientes empresariales. Pero las cosas están mejorando. Hablar sirve. Podríamos motivar a la gente para que hable con sus clientes específicos, pero lleva tiempo. La paciencia también ayuda mucho y lamento tener que decirlo.

DAN YORK: Gracias, Peter. ¿Alguien más?

ALEXANDER: Tengo una pregunta. En Alemania se escribieron estos documentos sobre el uso del DANE en el contexto del correo electrónico, considerando su obligatoriedad para los organismos del gobierno federal alemán. Por lo menos eso es lo que yo entendí de los documentos. ¿Ustedes vieron algún tipo de estandarización de los nombres? Porque en Holanda el gobierno lo puso en la lista y no pasó lo mismo con DANE. ¿Es una fuerza impulsora? Lo hemos visto que está en la lista de cumplimiento.

PETER KOCH: Me parece que no existe algo parecido a esta lista. Para los sectores regulados del mercado hay distintos requerimientos, pero solo afecta a un número bajo de partes. Lo que nosotros aquí vemos es la importancia del dominio. Si es el dominio de un

periódico importante o de un proveedor de acceso importante o alguien así, esto se cuenta como un dominio privado, como el suyo, como el mío.

Por supuesto, siempre podemos ajustar las medidas para impulsar el éxito, para que parezca exitoso. Pero es importante entender que en nuestro caso estos 16 millones de dominios no son necesariamente los que dan seguridad en la internet. Muchos dominios resultan en una o dos solicitudes de resolución por día. Otra palabra clave que no mencioné porque ya está en el informe que Dan mencionó. El BSI emitió una recomendación para los proveedores de servicio de correo electrónico que soporten DANE y validación en ese contexto.

Con esto se cubriría el servicio de correo electrónico. En ocasiones anteriores, pensamos que era un lugar interesante para desplegar DANE porque no había que afectar explícitamente a los clientes. Se puede hacer en el departamento de email. Nos sugiere que no se afectan los números. También el gobierno federal mismo firmó sus dominios. Tenemos un proveedor de cable grande que hace validación y que expone a los clientes a los resultados de la validación. Y por supuesto está Google. Pero las cifras están en línea con lo que dio Jeff. Hay algo de crecimiento, pero no sé refleja de inmediato en el número de dominios firmados.

DAN YORK: El crecimiento de recomendaciones para email de BSI, de [incomprensible] y de otros, como ven en la agenda, tenemos algo sobre los servicios de email. Tenemos otra pregunta.

ORADOR DESCONOCIDO: Soy [incomprensible]. Trabajo en una compañía de seguridad alemana. Estoy en la junta asesora desde hace un año. Tengo una pregunta para Peter y Alex.

En los números, ¿cuánto piensan que este incremento de nivel en Holanda tiene que ver con el cambio en los registradores alemanes? ¿Es solo la influencia holandesa o es el hecho de que los registradores alemanes hacen DNSSEC? A cualquiera.

PETER KOCH: Le pido disculpas que no puedo mirarle a la cara y hablar al micrófono a la vez.

Hay 109 registradores en la diapositiva a la derecha. Los de la izquierda son los más grandes. No estoy totalmente seguro, pero creo que dos de los cinco eran registradores alemanes que entraron en escena después de la iniciativa DS IDN. Pero ya estaba el terreno abierto y por muchos otros. La situación es complicada. Firmar el dominio involucra a los registradores y

revendedores. Siempre vemos al registrador, pero podemos investigar según el servidor y quien es el operador. Probablemente sea un registrador barra servidor de nombres holandés que va a un registrador basado en Alemania, lo que significa que el registrador soporta de alguna forma DNSSEC. También hay muchos registradores que hacen servicios mayoristas de nombres de dominios, que no necesariamente tienen soporte de infraestructura, lo cual complica más el panorama.

Para nosotros es difícil decirle por ejemplo al usuario final que este registrador o este otro soportan DNSSEC porque no sabemos exactamente como para que el usuario final sepa qué producto final usar. No sé si he respondido su pregunta.

ERWIN LANSING: Desde el punto de vista del cliente final, lo único que quiere usar el usuario es productos que cumplen con DNSSEC. Si es 100% en cumplimiento usa DNSSEC. En Alemania no tenemos reglamentación por seguridad de DNS por eso. DNSSEC tiene un nivel reducido. La situación es similar para nosotros. Por lo que recuerdo, creo que seis de los registradores más grandes tienen registración por DNSSEC y por lo menos tres eran grandes revendedores alemanes de alguna manera.

Yo no sé si la registración de nombres específicamente están basados en Holanda o en Alemania. No conozco demasiadas registraciones de Países Bajos, pero debería buscarlo. Por lo menos diría que la mayoría de las registraciones en nuestro registro provienen de los registradores con motores automatizados de los revendedores.

DAN YORK: Nos quedan 5 minutos.

JACQUES: Hace un par de meses, creo que fue, fue un día triste para el registrador, para DNSSEC. Muchos registradores intentaron hacer un cambio de operador de emergencia. La calle de DNS quedó mal durante 24 horas y fue difícil transferir el dominio. Intentamos despejar el registro DS. Bueno, es tema para otra sesión. Pero tenemos que considerar este ensayo. Es un ejemplo de un fallo a gran escala. Necesitamos una solución para esto.

DAN YORK: Acabas de secuestrar el tema de la próxima sesión, pero está bien. Es un buen tema. Cómo hacer la automatización de la clave de seguridad. Son varias las propuestas o implementaciones que usa la gente. Erwin.

ERWIN LANSING: Hace dos años se disminuyó el TTL de los registros a una o dos horas, que sigue siendo mucho en este caso, pero es menos que un día, que es lo que tiene el resto de la zona.

DAN YORK: Es un tema excelente si es que alguien quiere tratar esto en el taller en ICANN 59 o ICANN 60. No sé si alguien quiere ofrecerse. Parece ser un buen tema de conversación, si es que a alguien le interesa.

Ahora quiero pedir un aplauso para los oradores aquí de la región.

Muy bien. Me voy a poner de pie porque voy a hablar de IETF. Si alguien quiere hablar y ponerse de pie, como yo, es invitado o puede hablar desde la mesa.

JULIE HEDLUND: Perdón. Tengo que oponerme. Tenemos un conjunto de presentaciones en PowerPoint en general. Los pedimos en PDF en el caso tuyo, Dan.

DAN YORK: Porque yo soy especial. Quiero agradecer al caballero que hizo la pregunta de Egipto esta mañana porque me corrigieron

diciendo que EG no había firmado. Cuando buscamos en la base de datos tuve que ir al mapa que genera estos códigos y me preocupó porque no hay ningún registro para punto EG, así que hay algo que no está bien. Si tiene posibilidad de hacer el ciclo de actualización del código, por favor contácteme. Tengo que ver por qué EG no tiene registro. No obstante, tenía el color en el mapa.

Cuando hablamos sobre las actividades sobre DNSSEC en el IETF, ¿cuantos de ustedes participan del IETF? Varios. Bueno, quería hablar rápidamente. El IETF, para aquellos que no lo conocen, es el grupo de trabajo de ingeniería de internet, que crea los RFC o las solicitudes de comentarios, que son las normas que estandarizan la internet. Estamos organizados en grupos de trabajo, working groups, WG. Hay más de cien en distintos momentos. Tienen una carta orgánica que dura un cierto periodo, que les encomienda desarrollar ciertas normas. Una, por ejemplo, de las personas aquí presente es el presidente del grupo sobre DANE, sobre la norma DANE.

También tenemos las sesiones llamadas birds of a feather o BOF, donde se incorporan nuevas áreas de trabajo. Lo interesante de esto es que cualquiera puede participar en los grupos de trabajo a través de la lista de trabajo y cualquiera puede presentar un internet draft (un borrador de internet), que es el documento.

El proceso en el IETF es el siguiente. Alguien genera un internet draft sobre algo que piensa que debe ser estandarizado y se inicia un proceso el cual el grupo de trabajo discute el borrador, lo habla, lo debate, lo adopta y lo aprueba, hasta que eventualmente el borrador es publicado como un RFC o es descartado o se convierte en otra cosa. Pero este es el proceso general que sigue el IETF para la elaboración de normas.

Ahora con respecto al DNS, el IETF hace la mayor parte de su trabajo a través de las listas de correo, aprobaciones, análisis. Pero hace un tiempo la gente se reunió en distintos lugares del mundo, que va trasladándose según sea más o menos conveniente para la gente, tres veces al año. ¿Cuántos de ustedes estuvieron en el IETF 98 en Chicago? Fuera de la frontera estadunidense. Bueno, los que están aquí muchos estuvieron en Chicago.

Bueno, los ingenieros involucrados en los distintos temas ahí la gente tiene reuniones presenciales. Son de los temas más conflictivos. Se discuten aquellas cosas que no pueden resolverse de manera sencilla por correo electrónico. Se debaten. Surgen estas discusiones acerca de qué hacemos con cosas tales como el uso de los nombres de dominio para propósitos especiales, por ejemplo. Hay muchos debates apasionados. Es el trabajo constante. Entonces aquí están las

tres del año: Chicago, Praga y Singapur. Las reuniones de este año, y veremos después.

Algunas de las actividades del IETF que están relacionadas con la seguridad del DNS. El grupo más importante en este momento, donde se da gran parte de esto, es el grupo de operaciones DNS o DNS OP. Y Susan Wolf, que quizás la han visto aquí y está en la junta de la ICANN en RSSAC, es una de las copresidentas del grupo DNS OP.

La seguridad del DNS en este momento está en un estado tal que las normas están definidas. Es el momento de implementarlas. Producto de esta implementación surge feedback de mejora. Una de los RFC más recientes indica manejar los registros de DNS y la clave de CDS y de CDNS key, que es una nueva manera de tener un registro. Hay un borrador sobre lo que es caching N-SEC agresivo, que es lo que se llama en este momento la última llamada antes de la publicación. Son varios los documentos del proceso. Pero bueno, si les interesa saber dónde están estas normas, el DNS OP es el grupo a seguir.

Hay otras actividades operacionales que no tienen que ver con DNS, que están también en estas páginas. Otro grupo muy activo es el grupo de trabajo sobre DANE, que tiene encomendada crear la norma para DANE y otras normas relacionadas. Este grupo ha avanzado bastante. Está a punto de

terminar su trabajo. Está considerando el cierre de sus actividades.

Sí. Tome la palabra.

ORADOR DESCONOCIDO: El documento final está a punto de ser publicado o rechazado antes de cerrar el grupo.

DAN YORK: El copresidente lo mira con curiosidad, dudando. Eso es parte del proceso. El IETF le encomienda a un grupo que elabore una norma y cierra el grupo porque el trabajo terminó. La norma existe y tiene que ser implementada.

El otro grupo que también tuvo mucha actividad reciente es el grupo sobre privacidad del DNS o DEPRIVE, que es el grupo que se ocupa de la confidencialidad. Aquí hablamos de integridad y asegurarnos que los datos que salen del DNS son los mismos que se ingresaron al DNS. De eso es precisamente el DNSSEC. En este caso, este grupo se ocupa de la confidencialidad. Cuando uno presenta una consulta al resolutor local, cómo está protegida la consulta, como para que alguien no ingrese a saber qué sitios o no estuvo visitando y qué partes tiene.

Entonces una de las tareas que tiene este grupo es trabajar sobre el DNS sobre TLS, La conexión con el resolutor en el sistema local y el servidor recursivo. Ese es el trabajo que hacen. Publicaron dos RFC recientemente. La 7858 para DNS sobre TLS y la 8094, que es DNS sobre DTLS. Esto es de hace un par de meses nada más. Creo que fue enero.

Hay en este trabajo trabajo pendiente todavía. Empiezan a discutir si el grupo tiene que hablar del resolutor recursivo y pasar a hablar del servidor autorizado, o sea proteger la privacidad entre estos dos elementos. Les cuento que esto ha sido interesante. Cuando hablo con clientes empresariales en eventos empresariales, cuando la gente empieza a implementar DNS en las empresas, la gente ve esto y dice: “Un momento. ¿Todas las consultas de DNS desde mi laptop hasta el resolutor local van a estar encriptadas? Si eso sucede, no puedo hacer mi monitoreo, mi bloqueo y todas esas cosas que hago dentro de la empresa para impedir que la gente visite, no sé, sitios pornográficos o de deportes”. Esto fue una novedad para muchas empresas, que el IETF estaba estandarizando esto. Mi respuesta es: “Bueno, usted puede controlar la computadora y desactivarlo dentro de la empresa si le parece importante, pero tiene que saber que esto se está desarrollando por la vigilancia diseminada y todas esas cosas que están ocurriendo”.

Otra cosa que les interesará saber es que hay otro grupo que se llama [incomprensible]. Hay una cosa en IETF que tienen que saber, que es que les ponen nombres graciosos, que es la criptografía por curva elíptica. Cómo se manejan los protocolos. Hace poco hubo una norma a través de un nuevo RFC sobre ED DSA, la curva Edward del algoritmo criptográfico. Y ahora está la RFC 8080, que es el algoritmo número 15 y 16. Andre [incomprensible], quien no está aquí, fue uno de los autores, junto con… ¿Quién más? ¿O fue solo Andre? Andre y alguien más. No me acuerdo. Bueno, no importa. Ya está. Tenemos una nueva norma. Un nuevo algoritmo de encriptado. Hay gente que la va a implementar.

Bueno, estas son las actividades más importantes en el IETF 98, que será en dos semanas en Chicago. Lo que tratarán en lo que hace a DNS es que habrá un hack-a-thon con actividades sobre DNS. Lo hicimos ya en los últimos dos IETF. Un hack-a-thon dos días antes. ¿Van a estar ahí? ¿Quieres contarnos un poquito qué es lo que se va a hacer?

BEN: El sábado y domingo yo y algunos miembros de mi equipo, y también personas de CZ y desarrolladores, organizamos dos mesas. Tenemos una serie de proyectos en los que queremos trabajar. Hay una buena combinación, personas distintas,

proyectos que colaboran en la interoperabilidad de los RFC. A veces, por ejemplo, para el proyecto DNS también nos centramos es nuestro proyecto para poder avanzar e implementar nuevas funcionalidades. Para darle a la comunidad algo del interés del IETF es que se implemente la RFC. Hacemos implementación de prototipos o referencias.

DAN YORK: Si están en Chicago o conocen a alguien que va a estar en Chicago, que quiera ir a ayudar, o si vienen a la reunión del IETF antes, pueden ir y estar en una habitación sin ventas y trabajar con ellos. Es muy divertido.

BEN: Hay de unas 10 a 15 personas. Es muy bueno para intercambiar ideas.

DAN YORK: El grupo de operaciones DNS se reúne el lunes. Esta vez a principios de la semana. Todavía no se publicó la agenda. Hay una serie de versiones preliminares, que se están debatiendo. No hay muchos temas relacionados con DNSSEC. Por lo que vi en general tiene que ver con otras cosas de DNS. RPZ va a ser un tema controvertido. Va a haber toda una serie de temas

diferentes. No vi tanto. Warren, ¿ustedes vieron algo sobre DNS OP? No tanto relacionado con DNSSEC, ¿no es cierto?

WARREN: No. no tanto.

DAN YORK: Pero seguramente habrá conversaciones interesantes ahí. Paul, ¿dijo que podría haber alguien en el grupo de IPSEC? Algo de email. ¿Correcto?

WARREN: Es split DNS. Cuando hay un VPN, uno puede tener anclas de confianza de la red actuando en el propio dispositivo, cuando uno está conectado con el VPN.

DAN YORK: Fantástico. Es algo de lo que ya se habla en el grupo de IPSEC. Luego, en el área de seguridad, en este grupo hay una versión preliminar de NSEC 5 y la propuesta correspondiente. Eso también se va a hablar allí. Warren.

WARREN: Eso también es DNS OP. Aparece en varios lugares. Roy [incomprensible] también va a hablar sobre [incomprensible]. Se va a hablar sobre esa implementación.

DAN YORK: Perfecto. Eso es lo que está pasando en el IETF. Habiendo dicho esto, quiero ver si hay alguna pregunta. Sí. Adelante.

ORADOR DESCONOCIDO: Hablo de [CZ NIC]. Recientemente un grupo publicó la extensión de EPP para transferir claves y también está la versión de [incomprensible] acerca de la transferencia de material clave para los registros. Creo que este es otro grupo de trabajo importante en relación con DNSSEC.

DAN YORK: Gracias. Jacques, ¿esto se va a presentar en Chicago?

JACQUES: Estamos armando la agenda del equipo experimental.

DAN YORK: Muy bien. Es bueno saberlo. El grupo de extensiones de los registros es el grupo que ha estado trabajando en esto. Aquellos

que están acá, en la ICANN, los registradores, los registros, este es otro grupo con el que es bueno trabajar y es bueno seguir.

Bueno, esto es todo. Si entran en el sitio web del IETF, pueden participar de forma remota si quieren, si quieren ver lo que está pasando, lo que se está haciendo y no pueden participar. Eso es todo de mi parte. Creo que ahora Matt va a hablar acerca del KSK de la raíz.

Matt, ¿quiere usar este micrófono? ¿Él puede hacer esto mientras ustedes pasan las diapositivas? ¿No hace falta que use un puntero?

MATT: Hola. Si estuvieron en todas las sesiones de DNSSEC, seguramente esta será la tercera vez que me escuchen hablar en Copenhague acerca del traspaso de la clave para la firma de la llave. Así que seguramente es muy entretenido lo mismo tres veces. Quiero darles una breve actualización porque, como ya les dije, seguramente ya escucharon esto antes y ya lo saben. La próxima diapositiva, por favor.

Esta es la línea de tiempo para el traspaso de la clave para la firma de la llave. Generamos la nueva clave en el cuarto trimestre de 2016 en las instalaciones de la costa este. El próximo trimestre pasamos a la costa oeste. Entonces ya se

generó la nueva clave, ya fue a los lugares adecuados y está lo que consideramos en este momento estado operativo. Ahora estamos en la fase del proyecto en la que le hablamos a la gente acerca de la nueva clave.

Yo lo mostré no en esta presentación, sino en otras porque todavía no se publicó en DNS. Ocurrirá el 11 de julio. Estamos en la fase de proyecto entre ahora y el traspaso real, en la que estamos comunicando principalmente a los operadores que este es nuestro objetivo porque si los operadores no actualizan las anclas de confianza van a pasar cosas malas. Entonces este es el foco principal de las comunicaciones en este momento, pero con todo gusto hablamos con cualquiera y les agradezco la oportunidad de hablar con este público para contarles lo que está pasando.

La fecha importante es 11 de octubre. Esa es la fecha del traspaso de la clave para la firma de la llave y la fecha que todos tienen que tener en cuenta, especialmente aquellos que operan la infraestructura de validación del DNSSEC. Después de esto, vamos a revocar la vieja KSK. Y con el tiempo la vamos a quitar de manera segura de todas las instalaciones. Esto nos lleva al momento que está entre la generación de la clave y el traspaso propiamente dicho. Una de las cosas importantes que van a tener lugar es que cualquiera que tenga soporte para el protocolo de actualización automatizado del ancla de

confianza, si se actualiza correctamente, automáticamente va a actualizar el ancla de confianza. Si no están familiarizados con ese protocolo es muy simple. La idea es que si ya confían en una clave y luego vemos una nueva clave firmada, entonces con el tiempo, después de 30 días, van a pasar a confiar en la nueva clave. Se transfiere la confianza de una clave a otra.

Entonces es importante que si dependen de RFC 5011, que funcione. Y si ya hicieron pruebas con FRC 5011 anteriormente va a funcionar bien porque RFC 5011 tiene este periodo de 11 días. Es difícil probarlo en tiempo real porque hay que esperar 20 días. Desde el punto de vista de los desarrolladores de software, lo que pueden hacer craquear el contador del tiempo y hacerlo en tiempo acelerado para hacer el traspaso rápidamente. Pero en la ICANN lo que queremos hacer es ofrecer un banco de prueba para aquellos que quieren probar en tiempo real la implementación del RFC 5011.

Pasemos a la próxima. Entonces anunciamos este banco de prueba esta semana en la ceremonia de apertura. Creamos este banco de prueba diseñado para que un operador con infraestructura en producción pueda utilizar. En lugar de traspasar la zona raíz, traspasa esto y lo pasa a un árbol al que nadie va a ir. Por lo tanto es seguro hacerlo con un resolutor de producción. La idea es que el resolutor desempeñe ese papel de ancla de confianza con estas zonas y si logra hacerlo

exitosamente entonces vamos a estar en condiciones de avanzar.

No estamos tratando de probar las implementaciones de cada uno de ustedes. No me preocupa eso. No me preocupa el código, sino más bien el empaquetado de ese código. Ver si pueden escribir la clave en el sistema. Si alguien implementa accidentalmente esto tenemos que asegurarnos de que no funcione. Son cosas que son poco probables. La gran mayoría de las personas que piensen que tienen soporte para RFC 5011 sí lo tienen. Sin embargo, esto fue algo bastante simple de configurar. No es ninguna ciencia espacial. Es algo que le podemos ofrecer fácilmente a la comunidad. Básicamente es una lista de mailing.

Hay una nueva zona por semana que pasa por el traspaso todos los domingos. Lanzamos una nueva zona que pasa por este proceso. Acá pueden ver 2017-03-05. Esta fue la zona de la semana pasada. La de esta semana es 03/11 porque el domingo fue 11. Entonces si van a la página del banco de prueba, que está ahí abajo (pasemos a la próxima diapositiva), van a ver esto. Como pueden ver, no hay demasiado diseño gráfico en este sitio web. Deberían haberlo visto antes. Teníamos el mejor HTML de 1995.

Entonces hay que suscribirse a la lista de mailing para acceder a la zona de esta semana y ahí van a recibir algunos mensajes, uno por semana. Creo que ocho en total. Les van a indicar qué es lo que está pasando en el banco de pruebas esa semana, qué es lo que habría que esperar. Es algo muy simple, muy directo. Es un recurso para los operadores o cualquiera que esté interesado en esto.

Bueno, esto es lo más importante que tenía para contarles. Quiero que sepan que se está haciendo un traspaso de la KSK. El proceso está avanzando bien. Quiero recordarles a todos la fecha del 11 de octubre del 2017. Es la gran fecha del año. Voy a responder cualquier pregunta que puedan tener.

DAN YORK: ¿Alguien tiene alguna pregunta para Matt? Si nadie tiene una pregunta, aparentemente voy a tener que preguntar a qué hora va a estar la clave en la zona raíz.

MATT: Esa es una buena pregunta. Usted es la persona señalada para hacer preguntas en el público. Vamos a anunciarle a la comunidad a qué hora va a funcionar la nueva zona raíz con la nueva clave por primera vez. Le vamos a avisar a la gente con anticipación para que sepan exactamente a qué hora tienen que

entrar en el bunker para prepararse para el fin de internet o buscar champán.

ORADOR DESCONOCIDO: De [CZ NIC]. Vi que hay una guía que explica cómo configurar [incomprensible]. ¿Será posible también incluir el traspaso?

MATT: Sí. Gracias por mencionarlo. Les pido disculpas porque no llegué a esto. Me quedé sin tiempo. Les agradecería muchísimo que envíen texto. Si envían texto, lo vamos a actualizar inmediatamente. Muchas gracias.

DAN YORK: ¿Algo más? ¿Algún otro tiene alguna pregunta? ¿Todos están preparados? ¿Ya actualizaron las anclas? Adelante, [incomprensible].

ORADOR DESCONOCIDO: Tengo una pregunta acerca del banco de prueba. Sé que yo pude hacer la firma y lo vi en el sitio de la IANA. ¿Puedo hacer bancos de prueba en otros sitios?

MATT: Perdón. ¿Podría repetirlo? Porque no escuché.

ORADOR DESCONOCIDO: El sitio de la IANA tiene una primera ancla y tiene también la nueva ancla. ¿Esto también va a formar parte de estas pruebas?

MATT: No. tomamos la decisión consciente de no ejercer esa parte de la maquinaria porque eso es específico de la zona raíz. Lo dejamos fuera del alcance. Declaramos que estaba fuera de nuestro alcance. Dejamos que la gente probara la implementación de 5011, pero no ejercemos la capacidad de descargar el archivo del ancla de confianza porque eso está dedicado a la raíz. Es maquinaria que trabaja específicamente en relación con la clave de la zona raíz, en contraposición a un ancla de confianza arbitraria.

DAN YORK: ¿Ninguna otra pregunta? Bueno, Matt, lo dejamos irse entonces.

MATT: Muchas gracias.

DAN YORK: Gracias, Matt. Nos quedan un par de minutos antes de comenzar con el próximo panel, así que quiero decir que afuera hay algo para comer. Hay muffins, queso, etc. También hay café (…)

[FIN DE LA TRANSCRIPCIÓN]