MARRAKECH – Atelier du DNSSEC
Mercredi 9 mars 2016 – 09h00 à 15h15 WET
ICANN55 | Marrakech, Maroc

INTERVENANT NON-IDENTIFIE: .CA, Canada.

INTERVENANT NON-IDENTIFIE: .AMAZON.

INTERVENANT NON-IDENTIFIE: ... des Etats-Unis.

INTERVENANT NON-IDENTIFIE: Monsieur Ardan, du ccTLD.

VICKY RISK: Vicky Risk, ISC. On travaille avec le DNSSEC depuis 2006. Je ne sais pas si vous le faisiez déjà ces dix dernières années.

RAO NAVEED BIN RAIS: Naveed Bin Rais, du Pakistan, de l'université de la capitale.

NEIL GINS : On travaille depuis 1960 sur cette question.

Remarque : Le présent document est le résultat de la transcription d'un fichier audio à un fichier de texte. Dans son ensemble, la transcription est fidèle au fichier audio. Toutefois, dans certains cas il est possible qu'elle soit incomplète ou qu'il y ait des inexactitudes dues à la qualité du fichier audio, parfois inaudible ; il faut noter également que des corrections grammaticales y ont été incorporées pour améliorer la qualité du texte ainsi que pour faciliter sa compréhension. Cette transcription doit être considérée comme un supplément du fichier mais pas comme registre faisant autorité.

JOHN CHAND : Boursier ICANN des iles Fidji.

WILLIAM STUCKE: William Stucke, études ICANN de l'Afrique.

DAN: Bien, on a encore des personnes ici.

BEN : [pas de commentaire en français]

INTERVENANT NON-IDENTIFIE: [inaudible] Je travaille avec le DNSSEC depuis avant même la standardisation.

INTERVENANT NON-IDENTIFIE: Zambie.

SIMON BALTHAZAR: Tanzanie.

SONAM KEBA: Bonjour à tous. Sonam du Bhutan, je suis venu ici pour en apprendre plus sur le DNSSEC parce que cela n'a jamais été mis en œuvre dans mon pays, donc je suis ici pour apprendre quelque chose.

RAJEEWA ABEYGUNARATHNA: Rajeewa du Sri Lanka. Boursier ICANN.

[BOUZAH ZECHARIAH] [Bouzah Zechariah], du Maroc.

[ESLOUHI MUHAMMAD]: [Eslouhi Muhammad] du Maroc.

INTERVENANT NON-IDENTIFIE: Bien, il ne nous reste plus personne. Monsieur, vous voulez dire votre nom ?

INTERVENANT NON-IDENTIFIE: [Bario Ramso], .RU.

JOSE URZUA: Jose Urzua , .CL. Oui, .CL.

INTERVENANT NON-IDENTIFIE: ... de l'Inde.

INTERVENANT NON-IDENTIFIE: Est-ce qu'il nous manque des gens. Oui, Dani.

DANI GRANT: Je suis Dani, de CloudFlare.

INTERVENANT NON-IDENTIFIE: Quelqu'un d'autre ? Bonjour.

SARA MONTEIRO: Sara, .PT, du Portugal.

BRAM FUDZULANI: Bram Fudzulani du Malawi.

INTERVENANT NON-IDENTIFIE: On devrait faire ça plus souvent, en fait. C'est bien, c'est intéressant.

Bonjour, Robert.

ROBERT MARTIN-LEGENE: Robert Martin-Legene, du Centre d'Echanges sur les Marques Commerciales.

DAN YORK: Donc, bienvenue à tous à cet atelier de travail sur le DNSSEC. Excellent exercice pour commencer cet atelier de travail.

Alors, vous devriez regarder ce petit document pour ceux qui n'ont jamais participé à un atelier de travail sur le DNSSEC. Je ne vous conseille pas de rester jusqu'à 14 :15 cet après-midi, dans cette salle sans jeter au coup d'œil à ce document.

Notre ordre du jour pour voir ce qu'on va voir, l'ordre des présentations, etc. Julie, vous vouliez dire quelque chose ?

JULIE HEDLUND: Oui. Je voulais vous dire que pour le déjeuner, vous allez recevoir un ticket avec une carte au dos. Le déjeuner ne sera pas ici, ce sera à l'extérieur, mais ce n'est pas tout près. On vous donnera deux minutes pour aller chercher ce papier parce qu'il faut que vous ayez votre ticket. Donc gardez-le sur vous, même si vous voulez quitter la salle avant, assurez-vous de l'avoir sur vous.

DAN YORK: Je vais aussi dire aux personnes qui vont intervenir que Russ Mundy a un chronomètre avec lui donc sachez qu'il va s'assurer

que nous respectons tous notre ordre d'interventions et le temps qui nous est imparti.

Une diapo très rapidement ici. Je m'appelle Dan York, je fais partie du comité du programme – la présentation ne marche pas. Ça ne marche plus ! On a un petit problème technique avec la présentation. Ah, tout va bien, ça marche. Allons-y.

Alors, diapo suivante. En théorie, il devrait y avoir des vidéos sur YouTube dont vous voyez les liens à l'écran. Ça marche ? Non, en fait les liens vidéo ne marchent pas sur AdobeConnect. Bon, ça ne marche pas ? Non ? Ecoutez, ce n'est pas grave.

Bon, ça on l'a fait à Dublin à la réunion 54, il y a un comité du programme. Combien de membres de ce comité se trouvent dans la salle ? Levez la main. Plusieurs ont participé à ce comité et à l'organisation de cette réunion.

Nous sommes les responsables, entre guillemets, de cette réunion des présentations. Voilà le comité du programme pour la prochaine réunion 56 qui devait avoir lieu au Panama. Voilà les sponsors qui nous ont permis d'organiser cette réunion. Afilias, est-ce qu'on a quelqu'un qui représente Afilias dans la salle ? Non. Jim va venir dans un instant. Sara, Jacques et Amanda aussi. Pour Dyn ? SIDN alors ? Je sais que Christian était dans les parages ?

Merci à ces gens parce qu'Ils nous aident. Ils nous ont aidés pour le déjeuner. Ecoutez, si vous le permettez, je vais les remercier maintenant. Afilias aussi, qui a également aidé à la réunion des spécialistes en mise en œuvre DNSSEC.

Ensuite, diapo suivante.

INTERVENANT NON-IDENTIFIE : Oui, je crois que pour la conférence B, le DNSSEC et l'autre équipe travailleront en plus étroite collaboration, donc j'espère que ça donnera des résultats.

DAN YORK: Oui, j'aimerais également dire que la personne qui a coordonné cet évènement a fait un excellent travail, parce que la personne là-bas, .TR, nous a fait une excellente présentation sur les menaces et attaques qu'il y a eu en Turquie, donc allez-y monsieur.

INTERVENANT NON-IDENTIFIE : Non, en fait, ce n'est pas moi la présentation, excusez-moi. Moi je suis [Dami].

DAN YORK: Excusez-moi, j'ai confondu. Bon, écoutez, ce n'est pas grave. Allez voir cette présentation, elle est excellente.

Egalement ce monsieur de la Tanzanie qui a fait une excellente présentation sur ce qu'il fait par rapport au DNSSEC et la raison pour laquelle il est présent aujourd'hui. Excellente présentation aussi.

Diapo suivante. Atelier de travail offert par le SSAC de l'ICANN, avec l'assistance de l'Internet Society et le programme Deploy 360.

Voilà notre ordre du jour. Vous devriez en avoir un sous les yeux qui va vous permettre d'avoir une idée de ce qu'on va faire aujourd'hui.

Vicky va nous en dire un peu plus sur le DLV. Aussi ce qui se passe du côté du DNSSEC en Afrique. Puis une présentation d'Alain sur le *switchover* du DNSSEC. Egalement Claire. Et pour ceux qui n'ont qui n'ont pas participé, nous avons l'excellent questionnaire sur le DNSSEC. Qui a remporté cette petite compétition pour l'ICANN 54 ? En tout cas, cette personne est connue maintenant puisqu'elle a remporté ce petit questionnaire.

Ensuite, comment améliorer la cryptographie sur le DNSSEC. Là encore on a d'excellentes présentations avec une discussion sur le KSK *rollover* et ce qui se produit là-bas.

Julie est en train de dire quelque chose, mais c'est sans micro donc je ne l'entends pas.

Bien, écoutez, il semblerait que ce ne soient pas les bonnes informations que je suis en train de vous montrer à l'écran. Ce n'est pas grave, on va faire sans présentation pour l'instant.

Est-ce que quelqu'un veut dire quelque chose ? Je ne sais pas. Robert ?

Oui, je sais, normalement il fait froid ici, mais là il fait chaud. Ecoutez, je suis désolé, Julie, pour ces problèmes. C'est peut-être moi qui suis à l'origine de tous ces problèmes parce que normalement Julie est très efficace avec tout cela. Donc elle est en train d'essayer d'actualiser les liens, mais en fait c'est moi qui suis derrière tout ça. Désolé pour ceux qui suivent à distance.

[INTERVENANT NON-IDENTIFIE SANS MICRO]

DAN YORK : Oui, alors, la dernière fois, quand on était à Dublin, il n'y avait pas de caméras, donc on ne pouvait pas projeter de vidéos. Ce qu'on a fait, c'est que je suis venu avec une caméra au dernier moment et on a filmé avec ça, de manière improvisée.

Aujourd'hui, on a une caméra là, sur le portable au milieu de la salle et on peut projeter en direct avec ça.

Nous y voilà. Là, c'est la bonne présentation, n'est-ce pas ? Oui ? Attendez, revenez en arrière. Voilà. Parce que Christian a un nouveau logo ici, le nouveau logo du DNSSEC.

Donc on cherche un cinquième sponsor, une entreprise qui serait disposée à nous aider à financer ces évènements. Vous aurez la possibilité, si vous le voulez, de nous aider à financer ces évènements, en figurant sur la liste des sponsors et sur les tickets déjeuner aussi.

Donc nous remercions tous nos sponsors et ceux qui veulent le devenir, nous les remercions d'avance, parce que c'est toute une organisation pour réserver la salle, la salle de déjeuner, etc.

Voilà certaines des personnes qui ont participé à cet évènement, ici sur la photo, on a passé un très bon moment, on a parlé avec les développeurs, etc., donc les uns et les autres ont eu l'occasion de se parler.

Ensuite, on veut parler de statistiques portant sur le DNSSEC, les cartes et j'aimerais vous rappeler que lorsqu'il s'agit de ça, il y a deux parties. La partie signature et la partie validation, donc il faut d'abord signer, puis valider la signature.

Alors, première présentation Geoff Huston, grâce à cet extraordinaire graph, d'ailleurs ces présentations sont disponibles sur le site de l'ICANN. Mais le diagramme de Geoff montre l'augmentation continue dans la validation du DNSSEC au niveau mondial. On voit donc une augmentation continue dans le nombre de validations. Cette chute importante ici, en septembre, ça c'est dû à un évènement particulier, mais ensuite c'est une augmentation constante.

Alors, ici, je suis sûr que vous n'arrivez pas à le voir d'où vous êtes parce que c'est écrit en petit, mais ce qu'il est intéressant de noter, c'est la vision générale de ce qui se passe au niveau des validations dans le monde. Si vous regardez tout en haut, certaines des régions du monde où il y a le plus grand nombre de validations DNSSEC se trouvent en Afrique, en fait. Mais vous pouvez voir les régions où il y a le niveau le plus élevé, je crois que c'est 34% en Afrique.

Diapo suivante. Ensuite, vous voyez ici la perspective mondiale sur la validation DNSSEC en Afrique, là aussi c'est très élevé. Si vous regardez un peu plus dans le détail, vous voyez qu'Il y a une utilisation plus élevée également des données y afférent et des IPv4 et IPv6. Ça, on ne peut pas le voir d'ici.

Si vous voyez les statistiques de Geoff, vous voyez ce qui se passe. Certains des pays représentés ont un gros pourcentage

de validations, mais c'est surtout parce qu'ils utilisent le DNS public de Google.

Vous voyez que Madagascar a 8% du DNS Google, ça veut dire que les autres 92%, c'est la validation DNS qui se passe au sein d'ISPs locaux qui [sont à Madagascar]. C'est une bonne nouvelle.

Au niveau des signatures, vous voyez les pourcentages maintenant des TLDs signés, nous en sommes à plus de 80%. La plupart d'entre eux sont de nouveaux gTLDs signés par défaut.

Prochaine diapo. Je ne peux pas lire d'ici mais je verrai la prochaine fois, je sais que je ferai les choses en plus grand pour pouvoir les lire de loin. Je ne peux aller plus près puisque j'ai un micro mobile. Merci, Robert, de me le signaler.

Donc vous voyez au dessus .NL arrive en premier avec 44% de leurs domaines signés, avec plus de 2 millions. Vous êtes là, vous faites du bon travail.

Le Brésil est là aussi, avec un grand nombre de signatures. Ce que je vois du côté de Rick, Rick vous dira - si vous cliquez sur le total, vous pouvez – je vois donc un gros chiffre, alors qu'il y a un pourcentage assez bas, mais on voit une augmentation, on voit que les pourcentages augmentent.

Prochaine diapo. Nous avons cinq étapes pour l'expérimentation. Nous savons que ces gens travaillent un peu

sur le DNSSEC. On ne sait pas encore si le DS est partiel, ensuite s'il est dans la racine.

Ensuite, certains d'entre vous m'ont demandé pourquoi notre carte montre encore le DS dans la racine et pas opérationnel. Je n'ai aucun moyen de le savoir à moins que vous me le disiez, que vous me disiez que vous acceptez. Donc si vous acceptez les informations DS, il faut me le faire savoir.

Voilà donc une vue d'ensemble, vous voyez qu'il y a de plus en plus de vert où c'est opérationnel. Oui, il reste des endroits où on doit travailler encore.

Pour l'Afrique, il y a quelque chose qu'on devrait rajouter ici parce que félicitations aux gens du Maroc, vous avez signé mais vous avez signé après que j'ai préparé cette présentation, donc vous serez sur la prochaine diapo. On a aussi le Botswana qui a également signé depuis.

Il y a donc beaucoup plus de croissance maintenant. Alain participe énormément au programme Afrique qui fait beaucoup pour étendre la signature en Afrique.

L'Asie-Pacifique, dans cette région générale du Moyen-Orient, il y a du changement depuis la dernière fois, à savoir que l'Azerbaïdjan a signé .AZ.

L'Europe n'a pas changé depuis la dernière fois, comme vous le voyez. L'Amérique latine non plus. L'Amérique du Nord non plus, ça ne changera pas.

Ensuite, ces cartes sont publiées tous les lundis matins, nous les mettons à jour et vous pouvez les retrouver sur le site. Nous avons aussi un calendrier avec tous les évènements des DNSSECs qui y sont notés. Vous pouvez aussi aller voir cela sur le site.

Vous savez que l'on a ce qu'on appelle un *hack-a-thon*. L'IETF fait ça avant l'IETF, le weekend. Ça a été fait il y a plusieurs années. Tous ces gens qui travaillent sur la vie privée du DNSSEC, sur DANE et ainsi de suite, il y a même des récompenses qui sont distribuées pour le *hack-a-thon.* Donc un autre groupe se retrouvera si vous allez à l'IETF. Vous savez, les développeurs seront là et veulent travailler sur la sécurité du DNSSEC et nous aimerions que vous y participiez si vous le voulez.

Ensuite, il y a un projet d'histoire du DNSSEC et nous essayons de retrouver des informations de retours.

Nous allons donc continuer tout de suite en passant la parole à Julie.

JULIE HEDLUND : Nous avons deux questions dans l'espace de tchat. La première vient de Marcus, du Village Global. Il a une question sur les statistiques que vous avez rajoutées. Pourquoi est-ce que Mayotte a un taux de validation de 95% et que son utilisation Google est à 96% ?

GEOFF HUSTON : Ce n'est pas seulement Google, il y a d'autres validateurs.

Je pense que c'est plus bas en fait comme pourcentages.

Déjà, qu'on mette plus de résolveurs dans leur configuration locale. Et c'est souvent le cas que les ISPs pourraient lister Google en tant que résolveur. Quand on parle de DNSSEC, on peut voir que lorsqu'on va sur un domaine qui n'est pas bien signé, et Mayotte en a un, cela ne dit pas que ça a été mal signé. Le retour d'informations du DNS, c'est que ce serveur est en échec. Si leur résolveur ne valide la réponse, vous allez être mis sur le mauvais chemin et vous irez sur un domaine qui n'a pas été bien signé. Il y a beaucoup de gens qui utilisent des résolveurs locaux en plus de Google et Google va leur dire de ne pas y aller parce que ce n'est pas bien signé. Donc, en fait, les bonnes réponses ne sont pas sélectionnées. Certains font cela est c'est un peu stupide.

Julie.

JULIE HEDLUND : La personne a trouvé la réponse donc tout va bien. La prochaine question a été répondue donc ça va.

DAN YORK : Oui, tout le monde peut poser des questions quand vous le voulez, nous sommes là pour ça, nous ne mordons pas et nous sommes heureux de pouvoir vous parler de tout.

Vicky, vous pouvez passer à votre présentation, vous pouvez utiliser le micro ici ou continuez de votre place.

Nous n'avons pas de cliqueur. Nous allons essayer de voir ce qu'on peut faire avec le cliqueur.

VICKY RISK : Je suis Vicky Risk, de l'ISC, ISC.ORG. Nous publions les systèmes BIND open source. aujourd'hui, nous allons parler du DLV.

LE DLV, cela veut dire le validateur Lookaside DNSSEC. C'est quelque chose que l'ISC a développé en 2016. L'idée derrière cela était que les gens qui voulaient utiliser le DNSSEC avant la racine et que les TLDs étaient signés pouvaient utiliser ce DLV comme un parent adoptif, si vous voulez. A ce moment-là, comme vous l'avez déjà entendu de la part de Dan, un gros pourcentage de TLDs est donc signé et la racine est signée,

ensuite le DLV a accompli ce qu'il pouvait faire pour assister dans cette adoption précoce. Il faut continuer à voir ce chemin, disons, alternatif, pour pouvoir valider votre DNSSEC. Ainsi on peut décourager les développeurs qui restent.

Il y a un an, en 2015, l'ISC a annoncé que nous allions éteindre le DLV, l'arrêter à la fin 2017. Je suis désolée que ma diapo soit écrite en très petit, mais à Singapour, en février dernier, nous avons mis à jour la page principale du site, nous avons mis cela sur notre propre site, donc nous sommes passés du site DLV au site ISC.ORG. Nous avons fait une mise à jour des listes de diffusion, du BIND OS, et nous avons envoyé un courriel à tous les utilisateurs du DLV. Nous voulons nous assurer que nous allons commissionner cela, bien sûr, avant de l'arrêter.

Notre plan était donc de commencer un processus étendu afin de décourager les gens à faire des requêtes de DLV. Nous voulions arrêter tout cela et commencer, graduellement, à retirer la zone dans le DLV, avec le temps.

Notre plan est donc de continuer à répondre aux requêtes au sein du DLV de façon indéfinie parce que c'est mieux pour le résolveur de recevoir une réponse négative rapide plutôt que de ne pas recevoir de réponse et continuer à faire la demande.

Voilà donc un exemple des courriels que nous avons envoyés. Nous avons envoyé ça en juin l'année dernière. Nous sommes

allés dans notre système et avons vérifié quelle était la zone de chaque utilisateur, si ces zones travaillaient, si elles pouvaient valider sans le DLV puis nous avons envoyé l'information sur chaque zone et on a demandé aux gens de les retirer si possible.

Je vais maintenant vous montrer deux, trois exemples de réponses que nous avons reçues qui sont très représentatives.

Celle-ci, je sais d'ailleurs de qui elle venait et cette personne est très engagée vis-à-vis du DNSSEC mais n'avait pas d'autres manières d'avoir leur zone inversée signée. Pour beaucoup de gens, ça dépend d'où ils sont, ils n'ont pas forcément le choix d'ISP, donc cet utilisateur n'avait pas d'autres façons de signer sa zone inversée.

Il s'agit de quelqu'un d'autre qui a donc une voie pour signer mais qui ne peut pas obtenir que sa zone parente accepte ces informations.

Ce sont deux réponses très communes en fait. Si je vous montre cette présentation, c'est parce que je sais que beaucoup d'entre vous dans cette salle avez de l'influence pour améliorer les informations pour ces utilisateurs qui veulent s'engager vis-à-vis du DNSSEC, qui signent leur zone depuis 2006, et qui vont rencontrer des problèmes lors qu'on arrêtera le DLV.

Depuis que nous avons posé la question aux gens et que nous leur avons demandé de retirer leur délégation s'ils le pouvaient, nous avons retiré 800 et quelques zones, des zones fonctionnelles. Il y avait beaucoup plus de zones qui ne fonctionnaient pas. Je pense que beaucoup de gens utilisent le DLV en tant qu'outil de formation et d'apprentissage. Les 2000 et quelques restant n'ont peut-être pas d'autre option afin de conserver leur sécurité DNSSEC.

Nous avons déjà étendu le calendrier avant de pouvoir purger les zones qui pourraient valider sans le DLV. En ce moment, on en est à la ligne bleue que vous voyez. On s'apprête à arrêter les enregistrements dans les nouvelles zones qui pourraient valider sans le DLV et comme vous le voyez, à la fin ici, en juillet 2017, c'est là que l'on pense retirer tous le DLV. Il y aura donc deux ans pour que les gens retirent leurs informations.

Jusqu'à présent, ce que je vois, c'est que nous allons être obligés de forcer les gens à ne pas être sécurisés, des gens qui n'ont pas forcément d'autre solution. Même deux ans ne sont pas suffisants, apparemment.

Nous avons parlé des informations dans le DLV, maintenant nous allons parler des requêtes de résolveurs du DLV, les résolveurs qui essaient de valider le DNSSEC.

Mettre des requêtes sur le DV met une charge supplémentaire sur les résolveurs, surtout s'ils ne sont pas sur des zones importantes. Il est donc désirable de minimiser ces requêtes en allant de l'avant.

Après 2017, il n'y aura plus de zones dans le DLV et ce sera complètement inutile pour les résolveurs de faire des requêtes, nous voulons donc décourager cela.

Paul n'est pas là. Un de ceux qui nous a aidés avec cela, qui nous a aidés à retirer les requêtes dans le DLV et remettre sur la configuration par défaut, comme l'ont fait d'autres packageurs. L'équipe d'élaboration *onbound* nous a aussi aidés avec la configuration par défaut, ils nous ont mis aussi dans leurs recommandations qu'on ne fasse plus de requêtes au DLV. Nous avons donc beaucoup moins de requêtes maintenant qu'Il y a un an.

Puis comme je l'ai dit, le processus d'arrêt ou de fermeture sera complété d'ici 2017, mais on s'attend à ce qu'il y ait encore des requêtes au DLV après cela, donc nous laisserons le service en route disons.

En résumé, l'ISC a créé le DLV pour encourager plus d'utilisation du DNSSEC et nous avons fait du bon travail. Ce n'est pas une solution pour le problème systémique de non-support dans la

chaîne du DNSSEC en général, mais nous continuons tout de même à planifier sa fermeture.

Je voulais remercier Afilias. Pendant le projet, Afilias a fourni des services pour le DLV.

DAN YORK : C'est une question. D'ici 2017, est-ce que le DLV va continuer à fonctionner ?

VICKY RISK : Oui, il répondra aux requêtes mais il n'y aura plus de zones dans le DLV. Nous continuerons à répondre aux requêtes parce que nous voulons aider les résolveurs à aller plus vite.

DAN YORK : Oui, mais le service DLV sera donc fermé en juillet 2017.

D'autres questions ? Russ, puis Alain.

RUSS MUNDY : Merci, Vicky, pour la présentation. J'ai vraiment apprécié. Je voudrais aussi insister sur le fait que chaque personne dans cette salle, si vous êtes allés à la session des débutants, vous m'avez entendu en parler. Malgré tout ce que vous faites avec le DNSSEC, continuez à demander plus de support DNSSEC, que ce

soit de vos bureaux d'enregistrement ou de vos opérateurs de registres ou de vos vendeurs. Comme je l'ai dit l'autre jour, il y a beaucoup d'activités qui ne pourront pas être validées, donc la meilleure façon d'avoir une utilité plus importante du DNSSEC dans l'industrie, c'est de s'assurer que tous les supporteurs de toutes les fonctions incluant le DNS fassent ce qu'il faut afin que le DNSSEC soit disponible pour tous ceux qui veulent l'utiliser. Donc posez, posez, posez vos questions.

VICKY RISK : Oui, je voudrais être capable d'envoyer ces gens vers un opérateur, un ISP qui pourrait les aider pour qu'ils puissent maintenir leur chaîne de confiance DNSSEC après la fermeture du DLV. On nous a déjà demandé ces informations, mais je me rends compte maintenant qu'en fait, si nous avions fait payer de l'argent à ces gens-là, on pourrait l'utiliser maintenant pour faire autre chose et créer un marché pour cela. C'est un peu trop tard pour ça.

DAN YORK : Alain ? Non, j'ai vu Alain qui va poser sa question en premier.

ALAIN AINA : D'abord, je voudrais remercier l'ISC. Durant la discussion au départ, nous savons qu'il n'était pas facile de recevoir une

décision consensuelle de la part de la communauté à ce sujet. Les gens, dans cette salle, se rappellent des discussions qu'on a eues sur le DNSSEC et ses fonctions. Je pense qu'il était donc très utile d'en apprendre plus de la part de l'ISC. Dites bonjour à Paul Vixie pour moi.

VICKY RISK : Oui, je n'étais pas à l'ISC à l'époque, mais on m'a dit qu'il y a eu beaucoup de conflits.

ROBERT MARTIN-LEGENE : C'est bon que vous fermiez le DLV. Je pense que la technologie reste à travers d'autres logiciels, donc les gens pourraient faire leur propre DLV s'ils le voulaient, si j'ai bien compris. Savez-vous ce qui reste de tout cela ? Est-ce qu'il y a quelque chose, est-ce qu'il y a des pays qui ne soutiennent pas encore cela ?

VICKY RISK : Oui, il y a encore des zones inversées. J'ai parlé aux gens de DE. Il y avait des gens dans le domaine académique. Je pense que c'est vraiment un peu partout. Il y a des gens qui ne le font pas. Je ne sais pas ce qui je peux vous dire exactement ce qui reste. Certains l'utilisent en tant de mécanisme de transition quand ils passent d'un fournisseur à un autre sans coopération entre ces fournisseurs. Je pense que la délégation est temporaire. Je ne

sais pas si c'est une chose, tout simplement ce n'est pas si logique ça. Quelques personnes gèrent beaucoup de délégations à travers cela, mais en général ce ne sont que quelques uns.

DAN YORK : Quelqu'un d'autre ? Oui, Ondrej.

[ONDREJ SURY ?] : Oui. En fait, vous venez de répondre un peu à ma question. Vous voulez le fermer, n'est-ce pas ? Parce que le nombre de requêtes fait qu'il y a peu de zones. Que se passerait-il si demain vous l'arrêtiez ? Si vous le fermiez, je pense que vous pourriez fermer le DLV selon vos plans. Mais ma question, vraiment, c'est est-ce que vous avez peur de ce qui va se passer une fois que vous aurez fermé le DLV ? Je ne pense pas qu'il y aura des dommages par rapport à votre réputation. C'est la seule chose qui va se passer mais j'en doute, vous pouvez tout simplement tuer le DLV.

VICKY RISK : Oui, les gens qui sont au DLV ne sont pas précisément heureux de cela.

DAN YORK : Y-a-t-il d'autres questions ?

[ONDREJ SURY ?]: Oui, je pense que ceux qui sont heureux que vous le tuiez ou que vous l'éliminiez sont déjà partis.

DAN YORK : S'il y a des gens dans la salle qui souhaitent intervenir, n'hésitez pas à lever la main ou à vous manifester pour faire savoir que vous voulez prendre le micro.

J'aimerais reprendre ce qu'Alain a dit, merci à Vicky et à l'ISC pour cet outil particulièrement utile pendant la transition. Merci beaucoup.

Alors, présentation suivante. On a besoin des membres du panel régional qui vont faire cette présentation.

Je vais me tourner vers Mark qui sera le modérateur de cette séance.

MARK ELKINS : Je suis Mark Elkins, le modérateur de la prochaine séance.

Alors, le premier membre du panel vient nous rejoindre mais très lentement. Oui, mettez-vous en face pour qu'on vous voie sur la vidéo.

Alors premier présentateur – on en a quatre, moi compris – le premier, Alain Aina, très actif dans la communauté AFRINIC. Il a sa propre entreprise, il est très engagé dans l'AFRINIC, et l'organisation de formations en Afrique. Il a également été depuis novembre le directeur de projets pour AFRINIC et a passé beaucoup à l'île Maurice, pendant tout ce qui concernait le DNSSEC. Par exemple toute l'AFRINI a le DNSSEC pour l'inversé, y compris v6 et le *legacy*, ce dont je me réjouis. Il travaille également comme consultant sur le DNSSEC et les projets qui lui sont liés, je pense qu'il va d'ailleurs nous en parler dans un instant.

ALAIN AINA : Merci, Mark. Et si je parlais en français ? Non ? Peu de gens ont leurs écouteurs.

MARK ELKINS : Ecoutez, si vous préférez faire la présentation en français, on peut mettre les écouteurs.

ALAIN AINA : Merci, Mark. Comme vous le disiez, je viens faire cette présentation en tant que consultant ICANN pour le *roadshow* en Afrique du DNSSEC.

Sur la carte, vous pouvez voir que l'Afrique est en retard par rapport à l'adoption des ccTLDs du DNSSEC et je dois dire que ce vous avez vu en 2015, les chiffres que vous avez vus pour 2015 sont bien meilleurs que ceux de 2013 lorsque nous avons commencé, mais on a encore beaucoup à faire.

Ce *roadshow* du DNSSEC fait partie de la stratégie Afrique ICANN et on essaie d'aider les ccTLDs en Afrique à comprendre ce dont il s'agit, qu'est-ce que le DNSSEC, comment l'améliorer, nos services à la communauté, etc.

Mais ce n'est pas une chose facile du tout, parce qu'on sait tous que le DNSSEC entraîne certaines complexités dans le DNS et lorsque vous n'avez pas d'opérations de registres de DNS fiables, c'est difficile d'ajouter le DNSSEC.

Donc si vous allez DNSSEC/AFRICA.ORG, vous verrez les résultats enregistrés en Afrique et la progression historique. C'est la première fois qu'on voit une clef DNSSEC pour un CC, on l'a d'ailleurs inscrite et on inscrit également la date de la première signature CC. Mais on continue à suivre les changements, les algorithmes.

Nous avons 9 CCs sur le continent distribués par zones. Donc signature de zones, ça c'est une chose, mais être opérationnel, ça veut dire accepter le DS de la part de votre bureau d'enregistrement, ça en est une chose, c'est une toute autre

histoire. Je crois que dans un instant, on nous en dira un peu plus sur le nombre d'enregistrements DS signés depuis 2009, etc.

Donc nous avons trois CCs qui ont actuellement des clefs DNS avec des zones de signature clef qu'on appelle zones racines, au Sierra Leone. Donc on suit cela de près.

En ce qui concerne le *roadshow* du DNSSEC, ce qu'on fait, c'est qu'on se rend dans les pays et on organise un évènement sur trois jours.

Le premier jour, on se réunit, on demande à nos hôtes d'inviter toutes les parties prenantes parce que le DNSSEC ne concerne pas simplement la signature mais aussi la validation. Don on demande au pays hôte d'inviter les RSI, les fournisseurs de services Internet, toutes les parties prenantes qui ont à voir avec le DNSSEC. Ensuite on présente les avantages, en quoi consiste le DNSSEC et on présente les membres de l'équipe d'experts du DNSSEC. Et on montre aux gens comment déployer le DNSSEC, notamment la validation, etc. Le dernier jour, on s'assoit avec les CCs dans une salle, et on leur demande de nous montrer leur système de registres, puis on leur montre comment ils peuvent déployer le DNSSEC et on leur propose un plan. On essaie d'appliquer ce plan mais ce n'est pas toujours facile. Souvent, les registres ne sont pas fiables, il n'y aucun outil de

surveillance, il n'y a pas de ressources humaines qui puissent s'y consacrer, donc on dit « écoutez, on va d'abord régler le problème de votre registre et ensuite, on ajoutera le DNSSEC ».

Ici, voilà ce qu'on fait sur le terrain, dans les régions et nous espérons pouvoir améliorer l'adoption du DNSSEC en Afrique. L'année dernière, me semble-t-il, je crois que vous avez tous entendu parler des deux incidents du DNSSEC. Imaginez, vous essayez de promouvoir l'adoption du DNSSEC, mais malheureusement l'an dernier on a eu deux incidents liés au DNSSEC, au Botswana et au Kenya. Ces deux incidents nous ont montré qu'il fallait retourner dans ces deux pays, gérer les incidents et s'en remettre.

Donc à l'ICANN, on analyse bien ces aspects, on en parle dans les *roadshows*, on appelle les CCs pour parler de la gestion en cas d'incidents, parler de la poursuite de la mise en œuvre des plans.

Voilà, Mark, pour répondre à votre question.

MARK ELKINS : Oui, je pense qu'on va garder les questions pour la fin de la séance, si vous êtes d'accord. Donc écrivez vos questions et on y répondra à la fin de cette séance. Merci beaucoup, Alain. Ça fait maintenant de nombreuses années que je connais Alain. Si vous

allez à un évènement, sachez que ce n'est pas un évènement AFRIINIC s'il n'y est pas. Merci.

Alors, le prochain orateur, c'est moi-même. Si j'en crois l'ordre du jour, c'est à moi de parler. Je vais vous faire un rapport très bref sur ce qui se passe en Afrique du Sud.

Ça fait maintenant plus de dix ans qu'on fait des formations sur le DNS, depuis la première conférence ICANN en Afrique du Sud au Cap. Donc une formation avancée, c'est à dire qu'on a formé les gens sur le DNSSEC, et je pense qu'on en a vu les fruits.

Moi, ça fait sept ans que je travaille au DNSSEC, et je travaille sur un système, s'il vous plaît, ne le retirez pas. D'ailleurs, j'allais poser cette question lors de la présentation de Victoria mais je me suis retenu.

Alors on devrait savoir que le Zeda EPP a une extension du DNSSEC et moi, j'ai participé au roulement de la clef depuis ces dernières années. La raison pour laquelle .ZA n'est pas signé, c'est que les trois villes gTLDs, Durban et les autres, ont signé et fonctionnent bien. Lorsque j'ai regardé cette zone récemment, il n'y a qu'un domaine signé et je suis justement celui qui l'a introduit.

Comme je l'ai dit, cela a porté ses fruits, toutes ces formations ont porté leurs fruits. Ce que je peux vous dire que Telecom

Afrique du Sud semble faire les choses de leur côté et ne parle pas aux gens, mais ils viennent à ces cours de formation parce qu'ils sont gratuits. Ils gèrent des résolveurs DNS avec 15% des requêtes en Afrique du Sud. En tout cas, il y a un chiffre de 15% qui circule.

J'aime aussi parler de l'augmentation en Afrique de l'Est et d'ailleurs, lors du dernier forum AFRICA, j'ai vu les résolveurs de l'époque et je suis satisfait de voir que les chiffres sont bons.

Donc l'Afrique du Sud devrait signer très prochainement mais ça ne se passe pas pour l'instant pour le .ZA. Comme je l'ai dit, les installations pour introduire dans la zone sont là mais ça ne se produit pas. Les ZACR s'occupent des .ZA, .ZAORG, etc.

Ensuite, autre domaine en Afrique du Sud, tout n'est pas géré par des organisations centrales mais il y a une délégation pour faire les choses au deuxième niveau. Il y a peut-être ici source de confusion. Moi je m'occupe de .ZA, un autre ami s'occupe d'un autre domaine et ensuite, il y a les enregistrements DLV, puis de petits domaines qui sont signés.

Du point de vue AFRICA, en tout cas de mon point de vue, tous les inversés sont là et le sont depuis longtemps. Vous ne verrez jamais une personne en Afrique se plaindre du fait qu'elle ne peut pas faire un DNSSEC inversé en tant que tel.

L'ICANN a lancé un IRP pour une étude en Afrique, moi-même et un collègue, William Stucke, qui est ici dans la salle, et quinze autres personnes participent à cette étude. Cette étude à voir ce qui est signé dans le DNSSEC, donc ça c'est en cours. Mais si vous êtes ici en tant qu'administrateur, bureau d'enregistrement ou opérateur de registre africain, alors vous allez recevoir les résultats et ce rapport, cette étude vous intéressera, parce qu'on collecte les donnés dans les différentes présentations des gens et votre contribution pour nous aider.

Je crois que j'en ai fini avec ma présentation.

Troisième membre du panel ce matin : Sara. Oui, vous m'avez donné votre CV, Sara, n'est-ce pas ? Un diplôme en science de l'informatique de l'université de Lisbonne, vous êtes portugaise, membre de l'équipe d'infrastructures au DNSSEC .PT depuis 2006, responsable de la gestion des ccTLDs au Portugal. Plusieurs fonctions dans le domaine technique donc, vous faites plusieurs choses, des activités avec l'extension du DNSSEC, et vous allez nous parler en anglais, n'est-ce pas ? Parfait.

SARA MONTEIRO: Bonjour. Comme Mark l'a dit, je suis membre du ccTLD .PT, donc je fais partie de l'équipe technique, mais aujourd'hui je suis ici pour représenter certains ccTLDs africains où nous sommes le contact technique pour l'IANA

Avant de vous parler spécifiquement de certains ccTLDs, j'aimerais vous en dire un peu plus par rapport à l'UsNIC, c'est une association de ccTLDs lusophones qui a été créée l'année dernière dont la mission est de promouvoir et coopérer dans la défense de l'intérêt des ccTLDs de langue portugaise. Nous pensons qu'avec cette association, nous allons pouvoir aider certains ccTLDs, en particulier en Afrique et d'autres ccTLDs de manière générale pour qu'ils coopèrent entre eux.

Alors LusNIC, comme je l'ai dit, a pour principale fonction de partager les résultats des recherches dans le domaine des questions techniques, juridiques et qui ont trait à la sécurité, également concevoir ensemble des actions communes et assurer le développement continu de la langue portugaise dans le système des noms de domaine. On s'occupe aussi de .BR, [du .GW en Guinée Bissau], .PT et .AO. Voilà pour l'instant ceux qui ont signé et pour les membres de l'association. Mais nous espérons que d'autres membres vont se joindre à nous pour partager avec nous leurs expériences.

Pour entrer dans le détail du .AO de l'Angola, pour la gestion des domaines de premier niveau au Portugal .PT, nous avons également obtenu d'autres responsabilités, nous aidons .AO aussi de l'Angola. A la fin 2015, il y avait 364 noms de domaine enregistrés sous ce .AO.

En ce qui concerne le DNSSEC, nous avons organisé une formation d'une semaine sur le DNS au cours de laquelle nous avons essayé de partager nos connaissances dans le domaine du DNS, à Lisbonne, dans les bâtiments de notre association DNS .PT, afin d'améliorer le DNS, les connaissances sur le DNS et le DNSSEC. Nous avons donc organisé un atelier de travail avec six participants en tout provenant de deux entités différentes.

Prochaine diapo, s'il vous plaît. En ce qui concerne .CV, pour le Cap Vert, en 2010, le DNS .PT gérait .CV en tant que serveur primaire. Nous remplissons donc ce rôle vis-à-vis de l'ANAC, l'Agence Nationale des Communications, et ils ont commencé à assumer leur rôle eux-mêmes. Dans la même année, nous avons mis en place un atelier de travail au Cap Vert et des entités locales sont venues pour faire la promotion de leur domaine CC. En 2013, une fois de plus, nous avons fait une présentation et invité le personnel technique. Nous avons parlé d'infrastructures .CV et nous avons essayé de les aider à configurer les ajustements nécessaires pour adopter le DNSSEC. Je pense qu'ils sont donc bien préparés pour adopter cela. Je ne sais pas pourquoi ils ne l'ont pas encore fait. Ils sont plus à l'aise quand nous les aidons, donc ils essaient de s'organiser pour pouvoir venir au Portugal une fois de plus pour continuer leur déploiement, ou nous irons les aider, je ne sais pas, nous verrons.

Nous avons aussi offert d'installer un serveur de façon à les assister dans la gestion leur propre ccTLDs. Nous avons aussi aidé avec notre logiciel de façon à ce qu'ils puissent gérer le système indépendamment.

Prochaine diapo. Nous parlons maintenant du .GW, pour la Guinée Bissao. En juillet 2014, notre RN qui est responsable de la gestion le .GW est donc désormais gérée par la Guinée Bissau. Donc le DNS .PT s'occupe de la gestion technique, des opérations administratives et juridiques de .GW, mais nous allons essayer de transférer ce rôle à l'entité elle-même. Nous ne pourrons pas le faire avant d'avoir fait beaucoup de formations, avant qu'il y ait de nouvelles installations et des infrastructures techniques.

Prochaine diapo, s'il vous plaît. On veut partager avec vous ces informations dans cette communauté .GW. Voilà une diapositive sur la délégation. Au 4 mars 2016, nous en étions à 238 noms de domaine et nous pensons que cela est arrivé parce que .PT a aidé et conseillé ce nouveau ccTLD dans leurs affaires. Il y a eu aussi une alliance de 15 registres.

En ce qui concerne le DNSSEC, en février 2015, depuis que nous gérons la zone, nous l'avons signée avec le DNSSEC. Nous devons encore soumettre les informations de ressources DS dans la zone racine, mais c'est juste une question de temps. En

mai de la même année, une fois de plus, nous avons tenu un atelier de travail en Guinée Bissau, de façon à donner une large vue d'ensemble de l'Internet, surtout sur les sujets du DNS et sur la cybersécurité et les affaires DNSSEC. Nous leur avons fait des présentations et nous avons eu 32 participants.

C'est tout pour moi. J'espère que cela vous aidera. Merci.

MARK ELKINS : Merci beaucoup, Sara. Je n'avais pas réalisé qu'il y avait autant de pays parlant le portugais en Afrique.

Prochaine présentation, prochain orateur, c'est quelqu'un que je connais depuis longtemps, le Dr. Eberhard Lisse. Il est très connu dans cette communauté, pour sa participation à la journée Tech.

Je vais vous dire quelque chose que personne ne sait, son meilleur truc à l'ICANN, c'est de demander aux gens quel est son travail dans la journée, hors de l'ICANN. Ça n'a rien à voir avec le fait qu'il soit opérateur de registre. Il est gynécologue.

Enfin, il est fantastique quand il s'agit de s'occuper de la protection des femmes et des enfants, d'essayer de changer les lois pour que les femmes soient plus libres en Namibie. Il a vraiment un très grand cœur, ça ne se voit pas mais il a bon cœur, c'est sûr.

Oui, continuez s'il vous plaît, allez-y.

EBERHARD LISSE: C'est à mon tour. Comme je le disais, j'avais une profession. Je disais que j'étais gynécologue dans la journée et obstétricien dans la soirée, ce que je ne fais plus donc je dors beaucoup plus en fait, puisque je ne fais plus d'accouchements. Mais cette profession m'a appris beaucoup de choses.

Passez à la prochaine diapo. Un patient ne se préoccupe pas du nombre de visites du docteur du moment qu'on règle son problème, je suis donc très critique sur beaucoup de choses. Je suis heureux de voir que de nombreux pays adoptent le système. Et il y a peut-être une meilleure approche à utiliser à l'avenir. De toute façon, je ne me suis pas rendu compte, j'ai essayé de voir comment on a dépensé pour faire le *roadshow* du DNSSEC. Le gestionnaire des finances a l'habitude de recevoir mes emails maintenant. Les *roadshows* nous permettent de promouvoir l'adoption du DNSSEC.

Si vous pouviez passer à la prochaine diapo. Comme vous le voyez, en 2013, vous avez la photo, la carte de l'Afrique à l'écran et maintenant vous voyez en 2015, on a utilisé beaucoup de notre temps et pas à bon escient. Soit certains sont trop feignants pour faire le travail, mais si vous voyez que le travail n'est pas fait à la base, s'ils peuvent pas voir quel est le travail à

faire. Ce n'est pourtant pas si difficile que ça. Vous voyez les résultats, c'est vraiment dommage que seulement deux pays soient opérationnels, à savoir la Tanzanie et la Namibie. Vous voyez, les autres ne sont même pas visibles sur la carte, ce sont des îles et elles ont des plateformes différentes. Si le ccTLD de la Guinée Bissau est sur la plateforme .PT, elle ne compte pas.

Ce n'est pas compliqué pourtant. On a du personnel, on envoie les gens à l'université pour qu'ils obtiennent des Masters en informatique mais ils ne sont même pas capables de faire ce travail. Je vais demander aux gens de .CZ de ne pas trop s'énerver encore, on va y arriver. C'était une blague. Il y a deux voies pour faire les choses avec le DNSSEC.

Le DNSSEC, c'est simple mais ce n'est pas facile. Ce qu'on voulait faire, c'est d'un côté demander à Tarlis de donner les programmes de façon économe, il nous en faut trois. Je sais qu'on peut faire des mises à jour avec Tarlis, on n'a pas besoin de les remplacer mais on doit les obtenir à des prix intéressants. On doit voir si on peut faire quelque chose pour 20 dollars disons. Soft HSM est une réponse, et BIND rendrait également les choses plus simples mais avec BIND on ne peut pas le faire pour 20 dollars. Le problème, c'est lorsque BIND est mis à jour parce que ce ne peut pas être fait facilement. Si on pouvait simplement faire une mise à jour avec l'administrateur de

packages, ce serait plus pratique. On pourrait faire les choses plus rapidement.

[Le DNSSEC ouvert], c'est compliqué. Cela supporte Soft HSM mais cela a besoin d'une série de données et le DNSSEC ouvert a l'habitude de s'arrêter, de ne plus fonctionner ou d'arrêter de signer sans vous le dire, donc il n'y a pas de façon simple de faire les choses.

On passe à la prochaine diapo. Le DNSSEC ouvert était inclus dans les crises de plusieurs ccTLDs, ce n'est pas facile de retirer les bugs. Ce que je fais, c'est que je signe avec Soft HSM. Je dois éliminer le [inaudible] plusieurs fois par jour afin que cela recommence et resigne. Donc ce n'est pas une bonne façon de faire les choses.

Quand j'écrivais cette présentation, je pensais que nous devrions, au lieu de gaspiller plus d'argent pour voyager avec les *roadshows* du DNSSEC, utiliser cet argent pour voir ce qui fonctionne comme la signature du DNSSEC courante et soutenir un programme qu'on pourrait recommander. Il serait bon de voir ce qui fonctionne et ensuite de le montrer dans les *roadshows.* Voilà ce que le financement devrait nous apporter.

Prochaine diapo. En attendant, Ondrej [inaudible] qui a parlé lundi, pendant la journée Tech, nous a dit que le DNS qui s'emparera du monde entier pourrait parler au Soft HSM. Je vais

donc discuter avec lui pour voir si on peut trouver ces informations pour pouvoir faire les mises à jour avec l'administrateur de packages. Si ça marche, ce pourrait être une solution pour augmenter la sécurité et ainsi, on n'aurait pas besoin de dépenser autant d'argent. C'est une petite carte, cette petite carte coute 20 dollars, si vous l'achetez en Allemagne, vous pouvez en avoir six pour le prix de cinq. Il y a une petite puce qui fait la signature. Ça peut faire environ cinq signatures par seconde.

Est-ce que je peux finir ma présentation, s'il vous plaît ? Anthony [inaudible], quelqu'un que je n'aime pas forcément beaucoup, il le sait, il est désormais disponible, il n'a plus de travail et rien à faire, il a mis sur sont site qu'il avait été viré et il a dit que pour le marché [inaudible], il y avait cinq sortes de registres. En ordre descendant, c'est l'approche du supermarché. Certains gTLDs essaient de vendre beaucoup de domaines pour des profits énormes. Je ne sais pas si cela va marcher, ça m'étonnerait. Donc l'ICANN aimerait que les opérateurs de registres soient seulement intéressés par l'infrastructure. Ce qui fonctionne bien pour nous en tant que petit commerce, ça permet de garder les coûts bas et nous demandons à avoir un nouveau taux. Je pense que nous devrions avoir le meilleur des deux listés sur la diapo. Ce sont les fonctions techniques pour les petites entreprises. Si on doit payer [20 000] dollars pour une machine, on ne peut pas

se la permettre. Soft HSM n'est pas encore prêt pour le *prime time,* il est donc très facile de faire un PCH pour mettre en place en toute sécurité, pour pousser la zone et ainsi signer en toute sécurité.

Nous faisons donc déjà cela pour les noms de deuxième niveau, accepter les informations DNSSEC, avec [inaudible] *tool,* qui est une version qui a démarré l'année dernière, les informations DS et Mark peut vous en parler. Moi je ne viens pas pour vous montrer combien on a de clients. On en a pratiquement aucun qui sait si on va à la banque et vous dites que vous avez besoin d'acheter https même s'ils n'ont pas renouvelé leur certificat, je vais vous dire qu'on va descendre cette année et que vous serez en échec parce que votre certificat aura expiré.

Le message à en retirer, c'est de construire et nous viendrons vers vous. Si vous pouvez construire relativement peu coûteux, éventuellement, quelqu'un pourra s'en préoccuper. Quand on a dit au gouvernement qu'il ne pouvait pas faire le DNSSEC tout de suite avant qu'on puisse commander de façon descendante - il est donc difficile de régler ce problème pour qu'ils signent. Si je dis à mes bureaux d'enregistrement qui sont des fournisseurs de connectivité, si je leur dis « à moins de faire une validation, je vais vous donner un premium sur mon enregistrement ou si vous le faites un rabais », et tout de suite quand ça devient une histoire d'argent, ils le font immédiatement.

Voilà la fin de ma présentation, je vous remercie.

MARK ELKINS : Merci beaucoup. On a encore dix minutes. Vous avez des questions à poser ?

Alors une définition rapide. Si je regarde ce que sont les HSM - module de haute sécurité – pour moi un soft HSM, c'est un logiciel conçu par Richard Belkin en Suède, c'est ça ?

INTERVENANT NON-IDENTIFIE : Oui, ça fait partie du projet DNSSEC ouvert c'est [Rikard Balkrom ?] qui s'occupe de la maintenance, de l'entretien de ce système.

MARK ELKINS : Oui, le HSM dont parlait l'orateur précédent, c'est comme une carte de crédit avec une petite puce et ce qui est intéressant, c'est qu'elles sont réellement peu onéreuses ces cartes. Elles permettent une pré-configuration de beaucoup d'éléments et à l'autre bout de la chaîne, vous avez les autres HSM comme les *tallies*, les *cyper machines,* etc. Voilà donc de mon point de vue trois types – vous voulez préciser quelque chose, Dan ?

J'allais également poser une question rapide à Alain. Alors, 54 pays en Afrique, combien de pays vous reste-t-il et combien de temps ça va prendre ?

ALAIN AINA : Ce que l'on fait, c'est qu'on va chercher les gens et on se rend uniquement dans les pays où il y a des gens qui sont désireux de nous recevoir. On fait de la sensibilisation, on essaie de voir où sont les gens et si les gens sont disposés à organiser des évènements. On ne se rend pas dans chacun des ccTLDs. Donc c'est difficile de vous dire combien de gens ou de pays il nous reste. Ça dépend de la disponibilité des gens, s'ils sont prêts et désireux d'organiser un évènement.

MARK ELKINS : Oui, c'était justement ma question. S'il y a des pays représentés dans la salle qui aimeraient organiser le *roadshow* – j'ai d'ailleurs eu de très bons retours de l'organisation de ces *roadshows* – comment doivent-ils s'y prendre ?

ALAIN AINA : Il y a deux façons de s'y prendre. S'adresser à moi ou s'adresser à Pierre ou aux gens du bureau de l'ICANN en Afrique, ou parler aux gens du DNS pour l'Afrique, Richard Lang, etc. Vous avez donc plusieurs moyens pour arriver à vos fins.

DAN YORK: Je crois que c'est excellent la partie où vous avez parlé de la récupération et la reprise suite à un incident. J'aimerais encourager tout le monde à participer à l'étude dont Marl parlait, parce qu'on a besoin de mesures, on a besoin de davantage de données sur l'utilisation et tout ce genre de choses.

JULIE HEDLUND : Veuillez vous présenter, dire votre nom et d'où vous venez pour les gens qui sont à distance. Moi, je vous connais pour la plupart, mais je ne vous connais pas tous. Si vous avez un micro, Kathy qui est ici debout, a un micro volant donc assurez-vous de poser votre question dans le micro pour ceux qui nous suivent à distance.

J'ai une question sur le tchat, dès que vous serez prêts, je pourrai la poser.

MARK ELKINS : Je ne vois pas d'autres questions. Voulez-vous la lire maintenant ? Attendez, Victoria.

VICKY RISK : J'ai un commentaire. Eberhard, je sais que vous avez cherché du soutien pour ces cartes HSM, à condition que nous ayons les documents nécessaires, on pourrait les mettre à disposition pour d'autres utilisateurs, c'est ainsi que ça fonctionne. Si vous voulez faire une présentation à d'autres collègues concernés par l'utilisation du HSM, je serai heureuse d'organiser un webinaire ou quelque chose de ce genre.

EBERHARD LISSE : Oui, là il y a un changement, parce que j'ai eu un échange avec la personne chargée de la mise en œuvre, et il m'a dit qu'il n'était pas intéressé.

VICKY RISK : Oui, en fait, il y a des opinions divergentes par rapport à ces HSM et il y a une grande différence entre la recommandations de solutions comme étant une solution cryptographique d'excellence. Pour ceux qui travaillent au DNSSEC, je suis sûre qu'on peut parvenir à un consensus, surtout si vous avez une solution qui nous aide.

EBERHARD LISSE : Excellente nouvelle. Je vais rester en contact avec vous pour voir ce qu'on peut faire.

MARK ELKINS : Je vois qu'on souhaite que Victoria et l'ISC soutiennent les normes HSM fondées sur ces cartes.

Alors, question à distance.

JULIE HEDLUND : Question de Marcus du Village Global : est-ce que les opérateurs de registre africains utilisent l'extension EPP DNSSEC ou vont utiliser le .PT ?

SARA MONTEIRO : Je pense que la question s'adresse à moi.

Effectivement, il n'y a pas encore d'extension EPP mise en œuvre pour l'instant. Ils n'utilisent pas les mêmes techniques que pour le .PT parce qu'on n'essaie pas de reproduire ce que l'on fait et que les autres l'appliquent. On essaie simplement que les autres puissent trouver leur propre système et qu'avec leurs propres connaissances et outils techniques, ils améliorent ce qu'ils ont et qu'ils soient capables de l'utiliser.

Donc pour l'instant, vous pouvez soumettre les informations concernant le DNSSEC par écrit et à l'avenir, je ne sais pas. Ils décideront eux-mêmes de ce qu'ils feront pour le .PT.

EBERHARD LISSE : Alors tout registre qui utilise le [inaudible] *tools* depuis mai ou juin 2015 peut accepter les enregistrements standards EPP parce que ça, ça fonctionne pour tout bureau d'enregistrement accrédité de l'ICANN, et nous avions eu un problème, maintenant c'est réglé et ça fonctionne parfaitement bien.

MARK ELKINS : Y-a-t-il une autre question ? Robert ?

ROBERT MARTIN-LEGENE : Robert, du PCH. Je voulais revenir sur ce qu'a dit Eberhard dans sa présentation sur la signature de PCH.

Ce n'est pas nécessaire de s'adresser à d'autres services, mais vous pouvez le faire. Si vous voulez des informations sur le DNS, DNSSEC, etc., n'hésitez pas à vous adresser à nous.

RUSS MUNDY : Merci aux membres - Russ Mundy du SSAC – merci à tous les membres du panel pour toutes ces présentations. Je me réjouis de voir les progrès accomplis depuis les cinq dernières années, ce sont des progrès énormes.

L'une des choses qui m'a particulièrement intéressé dans toutes ces présentations, c'est lorsque Eberhard a dit que le gouvernement envisageait de rendre l'utilisation du DNSSEC

obligatoire ce qui, en soi, est un progrès extrêmement positif. Qu'un gouvernement envisage de faire cela est extrêmement positif.

J'ai deux questions. D'abord, est-ce qu'il y a d'autres gouvernements en Afrique qui sont en train d'envisager de prendre des mesures similaires ? C'est-à-dire faire en sorte qu'une certaine partie de la communauté utilise obligatoirement le DNSSEC.

Deuxièmement, et c'est une autre question : est-ce que les fonctions des bureaux d'enregistrement continuent de présenter des défis significatifs pour l'utilisation du DNSSEC, de manière générale en Afrique ?

EBERHARD LISSE : Les bureaux d'enregistrement peuvent soumettre [des registres DS] de deux manières, par IPP ou si vous utilisez les outils [inaudible] *tools,* mais il n'y a pas de demande. Si vous allez voir une banque et que vous leur demandez comment ça fonctionne, ils vont vous dire qu'ils n'ont pas de certificat, nous avons des certificats SLL. Ils ne comprennent pas ce dont il s'agit. Vous pouvez leur expliquer un milier de fois de la meilleure manière qui soit, en étant aussi poli que possible, vous pouvez être plus ou moins précis, mais ils ne comprennent pas. Les banques, ça ne les intéresse tout simplement pas et je pense vraiment qu'il

ne faut pas pousser la demande du côté des vendeurs. On offre ce service, et bien si ça les intéresse, très bien, sinon tant pis. Nous, on va dire à nos gouvernements qu'ils devraient faire en sorte que tout remplacement soit validé.

MARK ELKINS : J'ai vu que l'AFRINIC utilise le site Web SSR et je vois que Dan a une question.

DAN YORK : Oui, j'ai une question pour Sara. D'abord, merci Sara d'être venue nous parler de LusNIC parce que je ne savais pas non plus qu'il y avait autant de pays lusophones en Afrique jusqu'à votre dernière présentation.

Ensuite, lorsque vous parlez de .GW, il y a des retards ? Aue se passe-t-il exactement ? Pouvez-vous nous en dire un peu plus ?

SARA MONTEIRO : Oui, en fait, d'abord il y a eu des retards techniques et lorsque l'on soumet l'information, il faut qu'on obtienne l'approbation de tous et ce n'est pas très convivial finalement pour ceux qui n'ont jamais utilisé ce système auparavant. En fait, le problème, c'est que .PT a également été transféré d'une ancienne infrastructure vers une nouvelle infrastructure, en 2015, donc il y

aura des changements et ce qu'on essaie, c'est d'opérer tous ces changements en même temps et que les entités de direction et d'opérations s'adaptent. On espère pouvoir le faire en 2016.

MARK ELKINS : Dernière question, [.CZ ?].

INTERVENANT NON-IDENTIFIE : Oui, j'aimerais ajouter à ce qu'a dit Vicky qu'on est en train aussi de mettre en œuvre un support CS dans le DNS et dans ce cadre, on est en train de tester de nouveaux HSM. Donc si vous avez des HSM que nous aimeriez ajouter dans nos produits et si d'ailleurs vous pouvez nous offrir un meilleur accès aux HSM, on pourra vous apporter ce soutien, parce que ça ne veut pas dire qu'il y a un support pour tous les HSM, chaque HSM est différent.

MARK ELKINS : Merci beaucoup.

Alors les résumés. 30 secondes par personne. On commence par Alain.

ALAIN AINA : Merci. J'aimerais voyager en classe affaires mais ce n'est pas toujours possible pour se rendre aux *roadshows.* Une partie de ces *roadshows* consiste justement à fournir des ressources. Si

vous regardez ces sites Web, vous trouverez des ressources et vous verrez que ça ne consiste pas simplement à passer en revue l'aspect technique des choses. On a aussi besoin de faire participer la communauté pour que les gens ressentent le besoin de vous suivre.

MARK ELKINS : Ok, les 30 secondes sont passées.

Sara.

SARA MONTEIRO : Je crois que le principal objectif est d'aider au déploiement du DNSSEC dans tous les pays et dans tous les ccTLDs et gTLDs, c'est ce qu'on essaie de faire. On partage toutes les connaissances, on essaie d'unir nos efforts pour aider les uns et les autres à atteindre cet objectif.

MARK ELKINS : Merci beaucoup.

Monsieur Lisse.

EBERHARD LISSE : Je vais avoir du mal à résumer en 29 secondes, je n'ai rien de précis en tête d'ailleurs. En fait, c'est difficile parce qu'on est

paresseux. Oui, oui, je n'ai pas l'air paresseux mais je le suis. D'ailleurs, Mark l'est aussi. Le fait est que je ne pense pas que de faire cela de manière descendante va être utile, et créer une demande artificielle non plus. Donc on essaie de rendre les ressources disponibles mais il faut non seulement essayer de convaincre les autres de le faire, mais il faut aussi faire en sorte que ces ressources soient disponibles dans la pratique.

MARK ELKINS : Merci beaucoup, merci aux membres de ce panel pour ces excellentes présentations, et on vous applaudit.

JULIE HEDLUND : Merci aussi à Mark.

DAN YORK : Oui, on espère que cette carte de l'Afrique sera un peu plus remplie la prochaine fois. Merci.

JULIE HEDLUND : On est censés avoir une pause de 15 minutes mais qu'en pensez-vous Dan, si on en profitait pour récupérer le temps perdu ?

DAN YORK : Oui, excusez-moi, je n'ai pas mon ordre du jour. D'ailleurs, si vous ne participez pas au déjeuner, laissez votre ticket déjeuner pour les autres.

15 minutes de pause café, ensuite Alain Aina sur l'expérience Switchover de signature DNSSEC ouvert.

Attendez, attendez, vous êtes partis pour une pause. Pause rapide, pour être de retour aussi vite que possible. Donc pause de 15 minutes.

Oui, vous voulez entendre Alain à tout prix.

[Pause café]

DAN YORK : Comme Russ l'a dit, nous devons revenir pour travailler, merci. Si vous êtes assis sur des chaises autour de la salle et que vous voulez vous asseoir à la table quand il y a des sièges disponibles, n'hésitez pas.

Revenez vers nous. Il nous reste quelques minutes mais revenez.

Si vous voyez une place libre à la table, si quelqu'un veut même s'asseoir à côté de moi.

Est-ce qu'on est prêts ? Kathy est prête ? Oui, ça va ?

Si ça va, je voudrais que l'orateur, orateur qui nous a parlé tout à l'heure, Alain, et je serai le modérateur pour les questions s'il y en a, n'hésitez pas. Alain.

ALAIN AINA : Alain Aina, pour l'Afrique. Je voulais juste partager les informations du DNSSEC, depuis que nous sommes passés de l'AFRINIC. Maintenant je suis [inaudible], j'étais donc AFRINIC auparavant. Nous avons fait des changements. Ces changements, cette bascule ont été faits à l'AFRINIC. L'AFRINIC était le RIR pour les espaces v4 et v6. L'AFRINIC gérait neuf zones, six v4 et trois v6.

L'AFRINIC a fait le DNSSEC depuis 2012. On utilisait le DNSSEC ouvert et nous avons dû changer et passer à, comme vous allez

le voir, au nouveau DNSSEC comme vous le voyez sur l'écran. Vous pourrez ainsi voir ce dont je parle, regardez la diapositive.

Donc, dans le contexte AFRINIC, on utilise le DNSSEC ouvert pour signer les neuf zones avec les clefs en Soft HSM. L'algorithme, c'est RSASHA256. Le DNSSEC ouvert qu'on utilisait à l'époque s'appelait SQLite Database. En chemin, nous avons rencontré quelques problèmes de signature de zone, et nous avons donc des problèmes de phrases disons, ce qui a causé des délais. Ce que l'on a fait pour résoudre le problème, ce sont des travaux, si vous voulez, de changements, de rechargements, parce que toutes les heures il fallait resigner pour redémarrer la machine, si vous voulez. Nous avons donc travaillé afin de pouvoir régler le problème.

Il fallait donc aller vers un nouveau système de signature. Avec le DNSSEC ouvert, on a changé des bases de données. Cela nous a permis d'ajouter plus de zones, parce que l'AFRINIC gère aussi le DNS normal et les noms pour le continent. Ainsi, nous planifions aussi de signer d'autres membres. Nous avons décidé de passer au SQLite pour la nouvelle version de Soft HSM avec les mêmes algorithmes et les mêmes politiques de signature.

Notre stratégie, parce que nous gardons les clefs au sein du Soft HSM, il n'y avait donc plus de nouveaux démarrages si vous voulez, pas d'exportations de clefs, il fallait garder l'état de

validation dans toutes les zones signées en permanence. Quand on a décidé de faire cela, on a dit qu'on ne ferait pas de nouveaux démarrages parce que nous avions commencé avec ce plan et nous avions déjà un membre qui avait des zones signées et nous devions garder cet état de validation ouvert en permanence. Nous avons donc migré avec un roulement de clefs.

Voilà l'architecture à l'écran. D'un côté, vous voyez comment on signait avant et comment on signe aujourd'hui. Comme vous le voyez, il y a deux zones. Nous sommes passés au master public et nous avons désormais des serveurs secondaires.

Comme vous le voyez, c'est ce qu'on a fait. Bien sûr, nous pré-publions les clefs DNS et les doubles DS. Vous pouvez prendre la clef de KSK et [la clef DS ?] des nouvelles signatures et nous les pré-publions, nous mettions le DS de la nouvelle clef, à l'IP6.APA. Nous exportons les clefs publiques des autres signataires vers les nouveaux signataires afin de pré-publier les clefs DS et les nouvelles signatures. Nous commencions par l'ancien signataire et nous passions au nouveau. Voilà comment on faisait les choses avant le changement, avant la bascule.

Comme vous le voyez à l'écran, maintenant nous avons les clefs DS utilisées pour signer avant et après. Passons à la prochaine diapo. Après le changement, une fois de plus, c'est ce que nous

faisons maintenant. Vous voyez donc les deux clefs DS qui sont utilisées pour signer qui sont au dessus. Vous avez donc maintenant deux clefs avec ce système. Avant cela marchait avec les clefs DS. Ce sont les deux clefs que vous voyez au-dessus. Nous avons les anciens KSK et comme vous le voyez à l'écran, la dynamique a changé.

Comme vous le voyez, maintenant, nous avons retiré les anciennes clefs et donc l'étape finale consistait donc à retirer le DS des anciennes clefs et à passer au [inaudible .zone]. Comme vous le voyez, cela a demandé beaucoup de planification et il a fallu qu'on suive une certaine chronologie. Il a fallu prendre son temps, il a fallu vraiment gérer les clefs et leur état, etc. Il a vraiment fallu gérer ce changement parce qu'on voulait maintenir cet état de validation pour qu'il n'y ait pas de moment où il aurait été impossible de valider. Il fallait donc faire très attention, il n'y a pas eu de problème, pas eu de crash, pas d'alerte.

C'était donc une bonne expérience et je pense que cela pourrait s'appliquer aussi si vous passez de la signature BIND au DNSSEC ouvert, dans un sens ou dans l'autre, la même chose se produirait. Il suffit de gérer le clef pour que ça fonctionne bien. Si vous passez de BIND au DNSSEC ouvert ou l'inverse. Peut-être que nous n'aurons plus de clef privée, peut-être une des options serait d'en construire une nouvelle et de l'avoir dans le SSM.

La prochaine fois, même algorithme, sauf que nous pré-publierons le KSK. Nous l'avons fait dans le DS mais ce n'était vraiment pas nécessaire puisque nous n'avons pu le faire avec WDS. Nous avons cependant décidé de pré-publier le KSK pour éviter des problèmes et la prochaine fois, nous devrions le faire en pré-publiant le KSK et faire .DS.

Merci, c'était ma dernière diapo.

DAN YORK : Pouvez-vous nous dire pourquoi vous pouvez ne pas publier le KSK, ou clef de signature de clef ?

ALAIN AINA : En faisant le .DS, vous aurez une nouvelle clef déjà publiée dans le BIND, donc il n'est pas nécessaire de pré-publier la clef de signature de clef, parce que quand vous avez - si vous voulez, c'est comme si on faisait un roulement de clefs de signature de clefs. Si vous le faites, vous pouvez faire .signature ou .DS. Nous on a fait .DS et .signature en pré-publiant la clef de signature.

DAN YORK : Nous avons des questions. Il y en a une de Robert. Robert et [Ben] sont dans la queue pour poser une question. S'il y en a d'autres, faites-le moi savoir.

ROBERT MARTIN-LEGENE : Robert, de PCH.

Ben et moi, nous sommes d'accord que vous n'avez peut-être pas raison à propos de la pré-publication. Quand on pré-publie la clef de signature de clef, vous avez un ensemble de signatures sur la clef DNS, sur les informations de clef qui pourrait être en cache quelque part, et là vous risquez d'avoir des problèmes. Mais si personne ne s'en est rendu compte, c'est bien.

Ma question est en référence à cela. Quand vous avez fait le roulement de clefs, avez-vous trouvé des gens qui avaient des problèmes de meilleures pratiques DNSSEC, sur comment utiliser la chronologie, etc. ? Est-ce que vous avez montré comment faire le DNSSEC ? Est-ce que vous aviez des documents sur comment on peut réaliser le développement ? Est-ce que vous avez eu des réponses sur cette réalisation ?

ALAIN AINA : Gérer le temps qu'on avait pour déployer le DNSSEC, oui dans ce cas-là, nous avons observé les RFC et certains documents publiés sur le sujet par des gens qui l'avaient déjà fait. Nous devons maintenir cette chaîne de confiance, si vous voulez. Donc nous avons vraiment dû observer nos politiques de signature, la chronologie, et concevoir un système qui

correspondait à nos besoins. Nous avons donc utilisé les meilleures pratiques du RFC.

BEN [OFREINER ?] : Un des signataires importants du DNSSEC, merci Alain, d'avoir partagé cela avec nous. C'est toujours bon d'entendre ce qui va et ne va pas, c'est le genre de retours que nous pouvons utiliser et ainsi améliorer les choses.

Quand il s'agit de la chronologie, quelles sont vos restrictions, quelles sont vos politiques ? Le DNSSEC 2.0 va arriver et être publié, est-ce que vous avez des moyens plus efficaces de montrer vos politiques ?

ALAIN AINA : Oui, comme je vous l'ai dit sur la deuxième diapo que j'ai montrée, nous avons publié des informations sur le blog AFRINIC. Je vous avais donné deux liens et vous cliquez sur l'un de ces liens et ainsi obtenir les informations. Il y a un lien vers un blog aussi. Donc si vous voulez en savoir plus, allez sur ces liens.

GEOFF HUSTON: RFC 6781 est le document que vous cherchez. Si vous regardez ce document, vous verrez qu'il y a une analyse sur les façons de faire ce roulement de clefs. La double signature où il y a les deux

clefs introduites dans la zone, augmentant la réponse des DNS ou causer des problèmes, on peut faire une étape sans double signatures, mais cela amènerait des compromis, ce qui n'est pas facile à faire. RFC 6781 a été écrit pour ceux qui comprennent le DNSSEC, mais si vous commencez à faire des roulements de clefs, c'est que vous comprenez le DNSSEC et RFC 6781 est bien une lecture obligatoire pour comprendre le RFC.

ALAIN AINA : Merci, Geoff.

DAN YORK : Y-a-t-il d'autres questions à ce sujet ?

RUSS MUNDY : Merci, Dan. Merci, Alain. Très utile, cette présentation. Deux questions.

Dans le panel de la région Afrique, il y a eu beaucoup de discussions au sujet de la lenteur pour la validation et l'utilisation de la zone de signature. Je suis curieux : avez-vous établi une manière de mesure ou de collecter des données pour les utilisateurs finaux ? Est-ce que vous avez examiné s'il y avait des cassures, des ralentissements ou des problèmes avec la taille des BIND, dans des domaines prédominants où ces zones

sont utilisées ? Pouvez-vous nous expliquer ce que vous avez fait dans ce domaine ?

ALAIN AINA : Vous parlez de ce roulement de clefs précis ?

RUSS MUNDY : En général, est-ce qu'il y a des mesures qui ont été collectées ?

ALAIN AINA : Durant ce roulement de clefs, nous avons utilisé le DNS la plupart du temps, mais aussi des résolveurs comme moi, par exemple. J'ai fait ça à distance, j'étais au Togo, ensuite je suivais ça en utilisant mon résolveur au Togo. Puis une autre personne se trouvait en Afrique du Sud, nous avons quelqu'un aussi à l'Ile Maurice. C'est un peu comme ça que nous suivons ces roulements de clefs pour nous assurer que la chaîne ne se casse pas.

RUSS MUNDY : Merci, vous allez certainement entendre ça de Dan aussi. Mesurez, mesurez, collectez les données, nous n'en avons pas assez et nous en voulons plus.

ALAIN AINA : Oui, nous en avons, bien sûr.

DAN YORK : Je voudrais aussi souligner cela, encore une fois, je vais parler comme Julie. Si vous pouvez nous donner notre nom quand vous parlez au micro.

WAFA DAHMANI ZAAFOURI: Wafa Dahmani Zaafouri, de Tunisie. Je voulais faire un commentaire sur le travail d'Alain.

Alain, merci pour votre soutien, le soutien d'AFRINIC. Aujourd'hui, la Tunisie a signé. Nous avons beaucoup de travail à faire, nous allons passer aux prochaines étapes, nous allons signer toutes les zones et nous avons beaucoup de travail à accomplir avec les bureaux d'enregistrement. Vous êtes le meilleur formateur DNSSEC que j'ai jamais vu.

ALAIN AINA : Est-ce que je peux faire un commentaire sur le commentaire ?

Elle travaille pour ATI et ATI, si vous regardez les statistiques sur les zones AFRINIC, vous verrez qu'ATI et Marcus [inaudible] sont les deux personnes qui ont signé, qui ont poussé le DS et ils

m'ont vraiment aidé à démontrer aux PDG d'Afrique que j'étais capable de faire les choses.

DAN YORK : Est-ce que quelqu'un d'autre a quelque chose à ajouter ?

Je voudrais remercier Alain de nous avoir apporté ce genre d'exemples. On a souvent demandé des choses comme celles-ci pour la prochaine session de l'ICANN 56. On aime bien ce genre d'études, on aime voir comment les gens font les choses, ce qu'ils feraient pour améliorer leur système, comment cela fonctionne pour eux. Si vous faites ce genre de choses et voulez faire des commentaires, si vous voulez parler, comme vous voyez, on ne vous pose pas des questions très difficiles. Certains de nous auront peut-être des questions plus pointues, mais nous avons vraiment apprécié votre présentation, Alain, merci.

Ensuite, nous avons le plaisir de le recevoir. Beaucoup d'entre vous savent que CloudFlare a fait de nombreux remous ces dernières années en annonçant qu'ils allaient permettre la signature des millions de domaines existants. Oliver, qui est souvent là, en tout cas il est déjà venu nous parler de ce qu'ils allaient faire et des pas qu'ils allaient suivre. Et Jack, qui était à côté de moi – ah il n'est plus là. Donc les deux ont partis, ils ont travaillé là-dessus. Dani Grant est ici avec nous pour nous parler

de ce que fait CloudFlare et comment faire le DNSSEC à grande échelle pour des millions de domaines.

DANI GRANT : Bonjour à tous. Dani. Je suis l'une des managers du DNS, donc manager de produit pour DNS CloudFlare.

CloudFlare s'occupe de 4 millions de domaine. Chaque jour, nous répondons à plus de 40 milliards de demandes. Nous gérons le DNS pour tout domaine gratuitement. Ça, ça a été un défi. Il a fallu qu'on soit très créatifs dans la mise en œuvre et j'aimerais partager avec vous les mesures qu'on a prises pour que le DNSSEC soit une réalité.

Comment est-ce qu'on a choisi ces mesures ? Qu'avons-nous fait en cas de réponse négative et qu'avons-nous appris en termes de protocoles de réponses aux bureaux d'enregistrement ?

CloudFlare atténue les attaques pour [400] millions de paquets par seconde, pour des attaques sur la zone racine, 1/80 par taille. Une fois que ce site est attaqué, on répète les requêtes avec de petites requêtes mais de grandes réponses. Il y a des adresses qui sont capturées et ainsi des attaques perpétrées.

Revenez en arrière, s'il vous plaît. Les zones avec le DNSSEC, parce que les requêtes sont petites, en général les réponses sont

bonnes. Le mois dernier, nous avons publié un rapport sur la sécurité sur les problèmes que nous rencontrons sur le domaine et sur les réponses faites à ces attaques. Imaginez que tous les domaines puissent être utilisés pour ce type de simplification, alors on deviendrait une cible nous-mêmes.

C'est la raison pour laquelle nous avons pris les mesures de précaution nécessaire pour nous assurer que chaque réponse DNS que l'on envoie s'intègre dans un paquet inférieur à 512 bits. Ce que l'on fait, c'est utiliser l'algorithme de signature de courbe elliptique et il y a un mathématicien hollandais qui est connu, qui a parlé de l'énergie. Il a pris l'énergie nécessaire pour faire ce genre de choses et l'a comparée à l'énergie pour faire bouillir une cuillère à café d'eau. Ensuite, comment comparer cette énergie à l'eau nécessaire sur la Terre. Donc pour une clef ECDSA, combien d'eau nécessaire pour faire bouillir toute l'eau de la Terre ? Ça nous permet d'utiliser une clef plus petite avec une plus grande sécurité. Donc on a utilisé 228 bits de clefs RSA contre 228 bits de clefs ECDSA. Là vous pouvez voir ce qui se produit pour une taille paquet.

Autre avantage de l'ECDSA, c'est sa rapidité. On génère 50 millions de signatures par jour, donc ça nous intéresse beaucoup. Nous pensions que l'ECDSA était rapide, mais lorsque les ingénieurs ont mis en œuvre ce système, ils ont vu une

augmentation 21 fois plus élevée de la vitesse. Maintenant, ça prend 0,00001 seconde pour signer l'enregistrement DNS.

Alors, réponse négative. Il y a deux problèmes vis-à-vis de ces réponses négatives. D'abord, toute requête pour renvoyer le nom, c'est cher pour CloudFlare, et il y a des informations par rapport à la zone. Deuxième réponse, il y a deux enregistrements et deux réponses consécutives pour les noms qui manquent. Je vais donc parler des prochains noms.

Un peu d'historique par rapport à notre DNS. CloudFlare utilise un serveur DNS qu'on appelle RRDNS, qui représente RRDNS. C'est un système pour CloudFlare et pour les ingénieurs qui travaillent sur ce projet. Apparemment, je vais trop vite. Ce qui est unique par rapport à notre DNS, c'est qu'il n'y a pas de concept de fichier zone.

DAN YORK : Ecoutez, j'ai le même problème que vous, je parle trop vite. Je m'emballe dès que je parle donc les gens me disent « Dan, on se calme ». Ne vous inquiétez pas, vous n'êtes pas seule.

DANI GRANT : On me dit d'aller plus vite. Non, non.

Alors, notre DNS. Ce qui est unique avec notre serveur DNS, c'est que nous n'avons pas de concept de fichier zone. Ce que l'on a, c'est une base de données secrète qui éclate et lorsque nous recevons une requête DNS, pour l'enregistrement, on va dans la base de données et on prend la donnée dont on a besoin.

Autre aspect unique de notre DNS, c'est que beaucoup de notre logique commerciale est gérée par le DNS. CloudFlare génère de manière dynamique ses réponses, donc on ne sait pas toujours comment on doit répondre avant de faire cette réponse.

En général, il faut renvoyer le nom précédent et le prochain nom, donc là il faudrait demander à la base de données de faire une recherche aléatoire et avec nos réponses dynamiques, ce serait tellement difficile pour nous de savoir ce que serait les noms précédents et prochains sans ces contributions.

Deuxième problème par rapport à ces noms, c'est que ça expose les noms qui existent dans la zone. La solution à cela, c'est NSEC3. Il y a une proposition par rapport à ce nom, c'est le RFC 4470, par rapport aux « petits mensonges ». On essaie de trouver quelque chose qui existait juste avant que disparaissent les noms. Donc ça, ça nous aide parce que ça empêche le *zone walking* et les recherches extra-base de données.

A CloudFlare, on a décidé de prendre des mesures et nous, ce qu'on fait plutôt que de petits mensonges, ce sont de gros

mensonges. Une fois que ce nom existe, mais pas du type demandé, on dit « voilà, tous les types existent mais pas le type que vous demandez précisément. Donc si vous demandez un TXT, on dit « oui, c'est pas de chance, on a tous les types mais pas le type TXT », puis on demande à MX, « écoutez, vous êtes encore à côté de la plaque. Nous avons tous les types TXT mais pas MX ». Ça, c'est ce qui se produit du côté de la taille des paquets. Nos réponses négatives sont de 300 bits. Pour les réponses négatives, et ICANN.ORG, IETF.ORG, etc., c'est plus de 1000 bits. Donc la base de données regarde encore ce qui se passe et là il y a des réponses négatives aléatoires. C'est vraiment difficile pour nous.

Ensuite, au-delà des défis techniques du DNSSEC, une grande préoccupation pour le déploiement du DNSSEC à grande échelle, ce sont les coûts que cela représente. Pourquoi est-ce que les gens ne peuvent pas demander le déploiement du DNSSEC pour les opérateurs de registre et bureaux d'enregistrement ?

Je veux vous montrer l'une des choses que les bureaux d'enregistrement - voilà ce qui est intéressant ici. Souvent, lorsque les utilisateurs d'adressent aux bureaux d'enregistrement, ils s'en prennent aux équipes de soutien qui n'ont jamais entendu parler du DNSSEC ou leur donnent de mauvaises informations. Ce que j'aimerais vous montrer, c'est

ce type d'informations erronées qu'on donne aux utilisateurs. Ce premier exemple vient d'un grand bureau d'enregistrement et il y a confusion ici sur celui qui peut ajouter le DS. Le bureau d'enregistrement dit à notre utilisateur : « Afin de permettre à notre DNSSEC de fonctionner, le nom de domaine doit donner au bureau d'enregistrement la gestion du DNS. Les changements n'ont pas été finalisés et cette requête a été fermée ». Bien entendu, ceci est incorrect. Ils peuvent ajouter le DNS, même si la requête n'a pas été résolue.

Autre exemple : « J'ai parlé à l'équipe de soutien du bureau d'enregistrement et ils m'ont dit qu'il fallait m'adresser à vous pour l'enregistrement DS ». Là encore, c'est incorrect.

Voici mon exemple préféré. C'est un tchat avec le bureau d'enregistrement qui dit : « L'option DNSSEC n'est pas encore opérationnelle. Nous ne fournissons toujours pas de soutien pour cela. » La réponse : « Le DNSSEC est-il vraiment actif ? ». Réponse du soutien du bureau d'enregistrement : « Exactement ».

Un client a même reçu un script et il y a également de bons exemples. Parfois, il y a un soutien supplémentaire pour le DNSSEC depuis qu'on l'a lancé. Il y a même une promotion du DNSSEC avec des promotions sur la signature des noms de

domaine. Ça, c'est un problème d'efficacité. C'est quelque chose qui devrait être automatique.

Nous, à CloudFlare, on aimerait vraiment pouvoir envoyer ces enregistrements DNS automatiquement, mais les règles ICANN sont très strictes par rapport au type d'organisations qui peuvent s'adresser. On essaie de parler aux opérateurs de registre mais CloudFlare ne peut pas le faire.

Vous voyez ici, à droite, Sara. Nous avons pu élaborer un projet pour permettre aux opérateurs DNS de passer un accord avec les bureaux d'enregistrement, etc., pour envoyer un DNS automatiquement, pour plus de 300 noms de domaine.

Y-a-t-il des questions ?

DAN YORK : Je suis sûr qu'il y en aura.

Peut-être des questions de la part des interprètes ?

Je vois qu'il y a toute une série de questions sur le tchat.

Peut-être Dmitry, d'abord.

DMITRY : Oui, un commentaire. Par rapport à la mise en œuvre, il y a un [inaudible].

Deuxième commentaire. Il y a une chose supplémentaire, d'ailleurs je l'ai à l'écran, vous ne pouvez pas le voir puisque je l'ai sur mon écran, avec ce type de base de données, on a 3, 5, 6, 7, 8, 9, 10. Et je crois que c'était il y a deux ans, et la mise en œuvre était encore en suspens pour une raison en particulier.

DAN YORK : Attendez la réunion de cet après-midi, vous aurez une réponse à cela.

Une question à distance ?

JULIE HEDLUND : Je vais rappeler à tout le monde ici de dire votre nom et au nom de qui vous parlez.

Question de Marcus de Village Global. Il dit : « Je comprends que les algorithmes de courbes elliptiques sont sensibles aux attaques quantum. Est-ce que vous pensez que cela est un problème ? »

DANI GRANT : C'est un problème si les ordinateurs quantum sont appelés à être une réalité.

DAN YORK : Si on en avait une pour la mettre à l'essai. Il y a une séance cet après-midi qui parlera justement de ça, des courbes elliptiques. Oui, effectivement, on a une séance là-dessus cet après-midi.

Alors, je vois qu'il y a Mark, Robert, Lars qui souhaitent intervenir.

LARS-JOHAN LIMAN: Merci. Ce qui m'intéressait, ce sont les gros mensonges dont vous avez parlé. Alors si vous mentez en laissant de côté le type d'enregistrements ou de records qui est demandé, toutes ces informations en caché ?

DANI GRANT : Oui, c'est la raison pour laquelle on a autant de choses en caché. Ces informations pourraient avoir changées avec le temps.

LARS-JOHAN LIMAN : C'est cohérent.

MARK ELKINS : J'adore ce terme de gros mensonges.

Le cas de figure où vous avez mis cela dans une zone et que la réponse a été oui, c'est parce que ce n'était pas signé, c'est réellement ce qui se passe ?

DANI GRANT : Oui, c'est intéressant. Je crois que dans le meilleur des cas, vous avez un DS qui se propage au fichier parent et tout es signé. Ça, c'est dans le meilleur des cas.

DAN YORK : Robert.

ROBERT MARTIN-LEGENE : Robert, du PCH. Ce que j'ai aimé, c'est que vous avez utilisé la courbe elliptique, parce que personne d'autre ne le fait. Avez-vous une idée pour savoir si d'autres ont des problèmes de validation ?

DAN YORK : Je vous le répète, restez pour la réponse à cela.

DANI GRANT : Lorsqu'on a commencé à élaborer cet algorithme, il y en avait un qui n'avait pas ce support, mais grâce au DNS, on a un support de plus.

ROBERT MARTIN-LEGENE : Par rapport aux gros mensonges. Vous auriez peut-être dû parler de mensonges sinueux.

DANI GRANT : On a une personne dans mon bureaux que ça intéresserait beaucoup.

JULIE HEDLUND : Question à distance d'Antoine [Vershouren ?]. En fait il pense que c'est un commentaire mais c'est une question. Il dit : « Les opérateurs DNS qui ne peuvent pas parler aux opérateurs de registre sur des questions techniques, c'est une erreur au sein du modèle de l'ICANN. Que pouvons-nous faire pour convaincre la communauté ICANN pour changer le modèle afin d'augmenter la sécurité et la stabilité ? »

DANI GRANT : Oui, nous sommes d'accord. Pour répondre à cette question : qu'est-ce qui est fait ? C'est donner la preuve que ce concept marche. Voilà, c'est ça, c'est qu7il faut faire, démontrer que cela marche.

OLAFUR GUOMUNDSSON: Olafur, de CloudFlare. Par rapport à ce concept de ccTLD, on sera heureux de travailler avec tous les ccTLDs pour démontrer que cela fonctionne bien. Donc n'hésitez pas à nous parler à l'issue de cette réunion, ou envoyez-nous un mail.

INTERVENANT NON-IDENTIFIE : Bonjour, je suis de .DK. J'étais venu à Dublin à votre réunion. Vous pouvez nous parler, donc, c'est ça ? Je travaille actuellement sur un nouveau document donc surtout ne quittez pas la salle.

JULIE HEDLUND : Nous avons un micro volant.

DAN YORK : Geoff ? Non, pas de question ? D'autres personnes dans la salle ?

Merci, Dani, c'était vraiment fascinant. Nous sommes fans de CloudFlare à beaucoup de niveaux, surtout pour qu'il y ait plus de CDN et aussi pour la poussée sur la courbe elliptique. Je vous remercie pour votre présentation, merci beaucoup.

Maintenant, nous avons fait quelque chose d'intéressant peut-être, parce que c'est la vitesse avec laquelle Dani a parlé, nous sommes 10 minutes en avance. C'est très bien puisque ça va prendre beaucoup de temps pour aller à l'endroit où on mange.

JULIE HEDLUND : Ils s'attendent à ce qu'on vienne à midi, donc je dois vous dire que s'il y avait de la nourriture qui arrivait dans cette salle tout à l'heure, comme vous l'avez vu. En fait cette nourriture était pour

notre salle, ils se sont trompés donc nous irons définitivement à la salle Grand Bleu et c'est vraiment un endroit extraordinaire pour déjeuner.

DAN YORK : Alors, vous allez donc avoir cette expérience de cette nouvelle chose. Il y a des fiches qui sont distribuées. Tout le monde a cette feuille de papier ? Vous allez certainement avoir un papier. Vous savez, il y a une vieille création qui s'appelle un stylo. Combien ça vous a pris pour voir qu'il y avait un stylo dans le sac de l'ICANN avec aussi une petite lumière ? Vous vous êtes dit « ah c'est un crayon » mais non, il y a aussi une petite lumière dessus, c'est génial.

Donc, ce que vous allez faire. Nous allons nous amuser un peu. Pour ceux qui sont nouveaux, c'est le quizz DNSSEC. On appelle le quizz du DNSSEC mais ça a à voir aussi avec le DNS.

Vous avez donc une feuille de papier devant vous, et ce que vous allez faire et la raison pour laquelle il y a des noms sur les fiches, c'est que nous ne voulons pas que les gens trichent. Nous voulons que vous remplissiez le quizz et que vous passiez la fiche à la personne à côté de vous pour qu'elle puisse vous corriger. On veut finir ça pour pouvoir aller déjeuner. Allons-y.

Donc, ces questions ne sont pas mes questions, surtout ne pensez pas que ce sont les miennes. Roy Arends de Nominet. Oh, je devais pas le dire. Roy Arends de l'ICANN, pardon. C'était un employé de Nominet pendant très longtemps avant de venir ici, depuis quelques temps, il est passé à l'ICANN. Paul Wouters aussi en a écrit certaines. D'autres personnes ont participé à ces questions.

Donc il y aura une question sur l'écran, vous y répondez. Dans plusieurs cas, il y aura plusieurs réponses, plusieurs réponses correctes. Après, nous pourrons en discuter. S'il y a conflit, c'est moi qui aurais raison de toute façon. Voilà.

Vous devez mettre votre nom, tout ça. Ce qui est à l'écran, on l'a déjà fait. Il n'y aura pas de points pour les mauvaises réponses.

Quel TLD ne déploie pas le DNSSEC ? Est-ce que c'est A, EC ? B, MA ? C, TV ? D, MX ? Vous pouvez inscrire votre réponse sur le papier que vous avez devant vous. Vous répondez A, B, C, D. Oui pour ceux qui ne connaissent, c'est le niveau de questions que nous allons avoir.

EBERHARD LISSE : Pour citer Clinton : qu'est-ce que ça veut dire le déploiement du DNSSEC ?

DAN YORK : Ce que je veux dire, c'est quel est celui qui n'est pas signé.

Prochaine question. Qu'est-ce que TPC et TPC.NIT veulent dire ? Est-ce que c'est le centre de transition de politiques ? Le comité de programme technique ? Le câble trans-pacifique ? Ou la compagnie de télécom ? Ça ne dit pas DNSSEC. Si vous voulez, si vous n'aimez pas ces questions, aidez-nous pour la prochaine fois.

Si vous n'avez aucune idée, lequel de ces domaines n'existe pas : IPv4.INT, IPv6.INT, EUROFISH.INT ou CTO.INT ? Je ne sais pas où Roy trouve ces questions.

Voici une question plus facile. Qu'est-ce que le DO bit veut dire dans une requête DNS? Est-ce que ça veut dire DNSSEC on, DNSSEC off, DNSSEC out, DNSSEC ok ? Qu'est-ce que DO veut dire ? On ne va pas se disputer à propos de ces questions. Retournez vers votre RFC.

Qu'est-ce que 257 indique dans les infos d'une clef DNS ? A, clef de zone et point d'entrée sécurité? B, clef de signature de zone DNSSEC ? C, Algorithme 257? D, CCLVII ? Ce sont des chiffres romains, bien sûr, la dernière réponse.

Numéro 6, quels sont les algorithmes valides? NST3H ? SHA1 ? SHA256 ? SHA384 ? Ou GHOSTR34.11-94 ? Rappelez-vous qu'il peut y avoir des réponses multiples. Roy, si vous m'écoutez.

Qu'est ce que CD bit veut dire dans les requêtes DNS ? Ça veut dire A, compact disk (disque compact)? B, checking disabled (vérification désactivée)? C, cryptographyc device (outil cryptographique)? Ou D, change directory (changement de liste) ? Si je faisais ce quizz, je ne suis pas trop sûr de mes résultats, mais moi j'ai les réponses de toute façon. J'ai quelques réponses, j'ai les réponses de Roy. Qu'est-ce que KSK veut dire ? Est-ce que c'est Key signing key ? Kill signing key ? Vous avez tous les choix à l'écran. On dirait que dans la question, Roy n'a pas mentionné « qu'est-ce que ça veut dire dans le DNSSEC » alors que c'est le quizz DNSSEC.

Alors, prêt pour la prochaine. Combien d'adresses de serveurs racines y-a-t-il ? A, 12 ? B, 13 ? C, 24 ? D, 26 ? Je vois des gens qui regardent autour d'eux. Combien donc y-a-t-il d'adresses différentes de serveurs racines ? Pas combien y-a-t-il de nœuds, mais d'adresses de serveurs racines ?

On ne regarde pas sur son ordi, non, non, non. Les ordis devraient être éteints, on n'a pas le droit de tricher.

Quel ccTLD a été le premier déployé dans le DNSSEC ? Porto Rico ? Suède ? Danemark ? Ou Allemagne ? Connaissant Roy, il doit y avoir un truc dans la réponse. Quand on dit « déployé », moi je dirais quand c'est signé.

EBERHARD LISSE : Ces noms ne sont pas des ccTLDs.

DAN YORK : Si je lis ça très précisément, ça dit : quel pays, quel pays a été le premier ? En fait, si on est honnête, Porto Rico n'est même pas un pays.

Comment ça va ? Vous êtes prêts ?

Alors, assurez-vous bien que votre nom est sur la feuille de papier. Est-ce que vous avez déjà fait ça ? Vous aviez mis votre nom ?

C'est vous qui avez changé l'écran ? Je regardais, j'étais en train d'appuyer sur mon cliqueur et la présentation bougeait toute seule à l'écran.

Rappelez-vous bien que vous avez un point pour chaque réponse correcte. Voilà nos choix.

Quel TLD n'a pas déployé le DNSSEC ? Quelle est la réponse ? A, la réponse est A, l'Equateur n'a pas déployé le DNSSEC. B, Maroc. Qui est du Maroc ici ? Le 16 février, ils ont mis leur DS dans la racine, c'est notre nouveau signataire. Ils ont leur signature mais ils n'ont pas les infos DS, ils n'ont pas de clef DNS ? Si, ils en ont une, je le savais.

Très bien. Donc on veut aller déjeuner. Le déjeuner arrive, il faut qu'on se dépêche. Je suis l'arbitre. La réponse est A. Allez voir les infos ailleurs. Il a trouvé la réponse, oui.

Depuis combien de temps travailles-tu pour le DNS ? Tu n'as pas écrit de logiciel toi ? Il a fait beaucoup de choses là-dessus.

Alors, on doit continuer, sinon on n'ira jamais manger. Que veut dire TPC et TPC.INT ? Est-ce que quelqu'un était là quand le TPC.INT a commencé ? Ah, c'est vous qui le gériez ? Vous connaissez la réponse alors ? D. LA compagnie des télécoms : telephone company. Moi, j'aurais mis la mauvaise réponse, je n'étais pas au courant. Ça a eu lieu bien avant moi.

Quel domaine INT n'existe pas pour l'instant ? A ? Qu'en pensez-vous ? D ? La réponse est B. IPv6.INT n'existe pas actuellement. Apparemment, EUROFISH.INT est réel. Jetez le blâme sur Roy qui a fait les questions.

Quelle est la prochaine question ? Alors, qu'est que le do bit dans les demandes DNS ? La réponse est ? Combien on choisit A ? B ? D ? C ? Qui a dit C ? D ? La réponse est D. DNSSEC ok. Regardez ça dans le RFC si vous ne me croyez pas.

Prochaine réponse. Qu'est-ce que le chiffre 257 indique dans les infos des clefs DNS ? A ? Oui, c'est la zone clef. Quels sont les algorithmes valides au sein du NSEC3 Hash ? Roy dit seulement

la réponse A. Olafur dit qu'il a raison. Puisque Olafur a écrit le RFC sur le NSEC3, il a donc raison, la réponse est A. Est-ce que je peux revenir en arrière ? Oui. A seulement.

On continue. Question numéro 5. Que veut dire CD bit dans les requêtes DNS ? B, checking disabled. C'est la bonne réponse.

Qu'est-ce que KSK veut dire ? Dans le DNSSEC, qu'est-ce que cela veut dire ? Ce dont vous me parlez n'appartient pas à cette conversation. Bien sûr, c'est la réponse A qui veut dire « clef de signature de clef ».

Combien y-a-t-il de serveurs racines ? Combien pensent que c'est A ? B ? C ? Combien pensent que c'est D ? Nous avons eu beaucoup d'opérateurs, les gens de chez RSSEC disent pourquoi serait-ce C ? Correct. Il y en a 13 avec IPv4 et seulement 11 avec des adresses IPv6. Jim, que dis-tu ?

Alors quoi, vous me dites que la vraie réponse, c'est 25 ? 26 ?

LARS-JOHAN LIMAN : Ce devrait être 27 maintenant.

DAN YORK : Pour tous les nouveaux ici, nous sommes vraiment des geeks. Bon, je vais utiliser la réponse à 24, c'est correct. En fait, 26, c'est la bonne réponse. On va utiliser la réponse de Roy, mettez le

blâme sur lui. Je vais utiliser la réponse C. Si vous avez un problème, posez la question à Roy.

Maintenant, quel pays a été le premier à déployer le DNSSEC ? Puerto Rico, la Suède, le Danemark ou l'Allemagne. Quelle est la réponse ? B, la Suède.

INTERVENANT NON-IDENTIFIE : Ce ne serait pas le Danemark ?

DAN YORK : Ah, c'était supposé être une blague.

Combien alors ? Calculez donc vos réponses. Vous devriez avoir un total de 10 points. On n'avait pas de réponse multiple ? Roy n'a pas fait son boulot. On continue rapidement, parce qu'on va aller manger.

Combien de personnes ont une bonne réponse seulement ? Non, vraiment ? Je ne veux pas commencer avec les meilleures réponses.

Disons, qui a au moins cinq bonnes réponses ? Combien d'entre vous en ont six ? Et sept ? Huit bonnes réponses ? Neuf bonnes réponses ? Nous avons match nul entre Ondrej et Olafur. Merci à tous. Nous remercierons Roy pour avoir fait tout cela. Si vous voulez nous aider pour le prochain quizz, nous serions heureux

d'avoir ces informations. Allez au déjeuner. Julie va vous donner des informations.

JULIE HEDLUND : Amenez les tickets qu'on vous a donnés, les bons de déjeuneur. Il n'y a qu'une entrée là où nous allons déjeuner. Les trois autres côtés sont entourés d'eau, donc vous pourriez y aller en nageant mais bon, votre ticket serait un peu mouillé pour pouvoir rentrer.

DAN YORK : Si vous n'avez pas reçu de bon d'entrée pour le déjeuner et que vous voulez vous joindre à nous, vous pouvez aller voir Ondrej.

JULIE HEDLUND : Mais pour venir déjeuner avec nous, il aurait fallu que vous soyez là depuis ce matin, pour avoir gagné votre déjeuner. Suivez la carte qu'il y a au verso du bon et bonne chance pour trouver l'endroit. Nous vous revoyons bientôt. Merci.

DAN YORK : Cette salle ne sera pas verrouillée donc vous voulez emporter avec vous tous vos biens personnels.

[PAUSE DEJEUNER]

DAN YORK : On voit qu'ici, il faut chaud, dans cette salle, par rapport à la température extérieure.

Je vais demander aux membres du panel. Dan, c'est moi. Geoff Huston, Jim Galvin, Olafur, and Ondrej, venez s'il vous plaît ici, à mes côtés, ou là-bas. Il y a aussi Julie et Kathy à côté. Geoff, si vous le voulez, vous pouvez venir è mes côtés.

Je ne sais pas à qui appartient ce sac.

Bien. Soyez les bienvenus pour cette séance de l'après-midi de notre atelier de travail du DNSSEC. Si vous êtes assis sur une chaise, au fond de la salle, vous pouvez venir ici autour de la table et l'avantage, c'est que vous avez des prises opur brancher vos ordinateurs autour de la table.

Alors, on a dit que nous allions avoir un conflit entre mon lieutenant-général à ma gauche et étant donné qu'ils sont très grands tous les deux, à ma gauche, ça va être intéressant de voir le combat. Je vais commencer à prendre les paris. Comment faites-vous les combats, ici, au Maroc ? A l'épée ? Bon, pas grave.

Plus sérieusement. On peut applaudir Afilias, Sara, SIDN. Afilias, Sara, SIDN, Dyn. Nos sponsors. Et en particulier Kyle York de Dyn, qui est celui qui s'est chargé de tout cela pour nous. On n'est pas membres de la même famille, même si on habit tous les deux dans le New Hampshire. Ce sont les hasards de la vie.

Bien. Nous sommes branchés sur Adobe. J'aimerais commencer cette séance qui concerne le DNSSEC et l'algorithme de signature numérique à courbe elliptique, le CDSA. Voilà ce dont on va parler. Donc je vais vous donner un peu plus de détails là-dessus. Passons à la première diapo.

Pourquoi utilise-t-on les algorithmes DNSSEC ? Pour générer les clefs pour la signature. On les utilise pour les signatures DNSSEC, on les utilise pour les enregistrements DS pour la chaîne de confiance et pour la validation des enregistrements DNSSEC. Voilà ce pourquoi on utilise les algorithmes DNSSEC.

Voyons maintenant les registres actuels IANA. Il y a toute une série d'algorithmes qui existent. Geoff en parlera, il y a un très petit nombre de ces registres qu'on utilise, mais voilà les algorithmes disponibles actuellement.

Ensuite, il y a deux nouveaux algorithmes. Les plus récents remontent à cinq ou six ans. ECDSA et Ghost. L'ECDSA avait très peu de taux d'adoption jusqu'à il y a environ quatre mois, date à laquelle CloudFlare l'a lancé. On va parler des autres dans un instant.

La raison pour laquelle on s'y intéresse, c'est en raison de ce à quoi Dani a fait référence. D'abord, la rapidité dans la validité, ce qui est discutable. Les clefs sont plus petites, les signatures aussi et il y a une meilleure cryptographie. Ce dernier élément est

particulièrement important pour moi, puisque, vous le savez peut-être, mais à l'Internet Society, je travaille pour accélérer l'approbation du DNSSEC, son adoption. Or le problème particulier qu'on a actuellement, c'est qu'une partie de la communauté sur la sécurité qui essaie de s'éloigner du RSA 1024 bits. On essaie aussi de fermer les certificats TLS inférieurs à 1024 bits.

Donc la manière dont on fonctionne est différente. On a des ZSK de trois ou quatre mois, on peut discuter de la situation mais certains vont dire que 1024, ce n'est vraiment pas bon et qu'il faut s'en éloigner. Passer au-delà de ça pour faire en sorte que le DNS et le DNSSEC soient plus sûrs. On veut s'éloigner de ces clefs et la courbe elliptique, pour l'instant, est donc la solution.

Comme on l'a dit, il y a les aspects liés au déploiement de nouveaux algorithmes. Il faut penser là à la validation, à la signature, à l'hébergement du DNS et également aux opérateurs de registre qui doivent accepter les enregistrements DNS.

Du côté validation, on s'est penchés là-dessus et on s'est aperçu que les résolveurs doivent être mis à jour avec les nouveaux algorithmes afin de mener à bien la validation. Donc s'agissant du déploiement de nouveaux, il faut voir ce qui existe pour l'Instant. On a déjà entendu parler des bibliothèques non mises à jour. Comment faites-vous pour faire cela ? L'un des éléments

qu'on a identifiés dernièrement, c'est que le document RFC 4035 dit que si on n'a pas la possibilité de soutenir les algorithmes, il faut voir du côté de ce qui n'est pas signé.

Effectivement, parce qu'on utilise le DNSSEC avec des algorithmes plus sûrs, en fin de compte, il y a des zones qui sont traitées comme si elles n'étaient pas sécurisées par le DNSSEC du tout.

Du côté signature, le logiciel pour les serveurs DNS faisant autorité ont besoin de mises à jour, bien sûr. Il faut changer cela et ça, ça peut avoir des incidences quand on passe d'un serveur à l'autre.

Du côté des opérateurs de registre, certains acceptent uniquement les enregistrements DS avec certains algorithmes. Le problème, c'est que du point de vue des programmes, on ne sais pas quel opérateur de registre accepte tel ou tel algorithme. On nous a donc suggéré ce qui suit. Par exemple, actualiser le feed EPP pour indiquer quels sont les algorithmes qui sont acceptés. On a ici une expérience en la matière de par le passé et on peut poursuivre les discussions là-dessus.

Du côté des bureaux d'enregistrement, certains ont des interfaces Web et n'acceptent que certains algorithmes. Voici un exemple d'un bureau d'enregistrement qui conserve l'anonymat mais vous aurez peut-être une petite idée. Il s'agit d'un domaine

Google. On demande à quelqu'un l'ECDSA, vous voyez une liste d'algorithmes, ensuite ils reçoivent toute une série d'algorithmes. Vous verrez qu'il y a aussi un chiffre à côté de l'algorithme. Ça, c'est un peu curieux parce que dans certains cas, les opérateurs d'hébergement DS ont ce type d'enregistrement. Donc ils vous fournissent le numéro mais pas l'algorithme. D'autres vous donnent l'algorithme mais pas le numéro. Donc les bureaux d'enregistrement vous montrent les deux, le numéro et l'algorithme. Jacques et ses collègues ont trouvé des moyens pour faire en sorte que l'utilisateur n'ait pas à rentrer dans ce genre de détails. Pourquoi est-ce que les bureaux d'enregistrement ont besoin de vérifier le type d'algorithme et aussi tout ce qui concerne la sécurité. Avec les développeurs, le défi ici, c'est que si vous donnez à quelqu'un une liste de vérification, on a dit aux vérificateurs de vérifier les limites et finalement, il n'y a jamais de mise à jour lorsqu'il y a de nouveaux algorithmes. S'agissant de la liste IANA, beaucoup de logiciels qui vérifient les algorithmes existants ne vont pas faire de mises à jour.

Vous voyez ici les différentes étapes de la discussion, à mesure qu'on introduit de nouveaux algorithmes. Il faut que l'on voie comment faire pour promouvoir la valeur, la valeur ajoutée de ces algorithmes et comment faire en sorte que ces changements aient lieu. On peut donc en parler ici, en dehors de ce panel. Il

faut essayer de voir ce qu'Il faut faire pour que notre DNSSEC soit encore plus sûr.

Voilà, j'en ai fini. J'allais suggérer que Geoff nous en dise un peu plus par rapport à ce qu'Il a vu dans le domaine du DNSSEC.

D'ailleurs, si vous avez des questions spécifiques qui s'adressent aux membres du panel, vous pouvez le faire maintenant. Peut-être que si ce sont des précisions ou des questions un peu plus longues, on attendra la fin des interventions.

GEOFF HUSTON : Geoff Huston, je travaille à l'APNIC. On a énormément travaillé sur les mesures et l'un des aspects de ces mesures, c'est justement la mesure du DNSSEC. Je vais parler du niveau de soutien du ECDSA du côté des résolveurs. Je ne vais donc pas parler du type d'algorithmes utilisés, pas du tout. Moi, ce qui m'intéresse, ce sont les résolveurs. Si vous signez vos zones avec l'ECDSA P-256, il s'agit de l'algorithme numéro 13, vous serez capable d'utiliser cet algorithme et de voir s'il est suffisamment sûr ou non.

Ce qui est intéressant ici, c'est qu'on nous dit, et moi j'Ai toutes les raisons de le croire, que la force de l'ECC, c'est qu'Il y a plus de bits. Donc, d'après ce qu'on me dit, 256 bits de CC, ça équivaut à 3072 bits de RSA. Or les spécifications originales du

DNS disaient qu'une fois qu'une réponse DNS obtient plus de [512] bits de payload, alors on ne peut pas avancer davantage, une fois que vous allez de 1000 octets, on ne peut plus avoir certaines réponses. Ensuite, si vous allez au-delà de 1500 octets, là encore, problème et problème grave. Si vous utilisez v6, alors rien ne vous aidera.

Donc il y a des problèmes graves vis-à-vis de la fragmentation. Il vaut mieux utiliser de plus petits algorithmes. Voilà le type d'exemples d'ECDSA, avec les mêmes questions d'ECDSA. 527 octets, presqu'en dessous de la limite, et la même chose, RSA 937.

Alors, oui, faisons-le, pas de problème. Moi, je peux signer des choses sur l'ECDSA, mais vous devrez accepter ma zone signée. La véritable question, c'est si je fais cela, me croirez-vous ? J'essaie donc de voir. SI j'utilise l'ECDSA, quel résultat va valider cette signature ? Lorsque vous utilisez Google Ads pour mesurer le réseau du côté de l'utilisateur, les publicités sont de plus en plus utiles. Elles sont très simples et font ce que vous faites d'habitude, c'est-à-dire chercher une URL. C'est un peu spécial parce qu'elles ont une composante DNS et une composante Web. La composante DNS dépend de moi. Pour ce qui dépend du nom, il es unique est utilisé une seule fois. Google agit très bien parce que si vous avez une publicité qui n'attire personne, Google veut vous aider à obtenir de l'argent avec votre publicité.

Dans ce cas-là, la publicité cherche cinq URL avec un nom unique. A chaque fois qu'un utilisateur essaie de résoudre cela, ces enquêtes arrivent sur mon service. J'essaie donc d'avoir des contrôles avec des tests.

Le contrôle absolu, c'est aucune signature DNSSEC du tout. Ensuite, des signatures basées sur le RSA. Troisième test, qu'est-ce qui se passe si je vous donne quelque chose qui est volontairement cassé ? Vous ne devriez pas croire ce que je vous dis, vous devriez accepter ce RSA et je répète ces deux tests en utilisant exactement le même mécanisme, en utilisant l'ECDSA P-256.

Voilà ce à quoi à ça ressemble en termes d'URL, avec des étiquettes communes, et voici donc les cinq URL différentes. C'est pourquoi si vous avez vu la publicité, vous essayez de résoudre ces cinq noms de domaine différents que vous voyez en fond.

Il y a une vue simple et la réalité. La vue simple, c'est je vous pose une question qui est transmise au serveur et le serveur vous répond. Ça, c'est très simple : une requête, une réponse.

Avec la validation DNSSEC, c'est un peu plus de travail mais ça reste simple. Vous me posez une question, je vous renvoie une réponse signée, vous validez cela d'abord en demandant l'enregistrement DS, puis la clef zone. Donc ce que je devrais

voir, c'est si vous validez, je devrais voir ces trois requêtes plutôt qu'une. Voilà ce que je devrais voir. Je vous envoie cela et je devrais voir trois requêtes pour ces trois enregistrements.

Le DNS, ce n'est pas du génie informatique, mais c'est un fouillis. Il y a des serveurs, des réplications de requêtes, tout ce qui peut se produire s'y produit. Il manque des choses parce qu'il n'y a pas de TTL. On ne sait pas ce qui se passe exactement, mais c'est un fouillis de choses, chaque chose ayant son propre calendrier.

Vous voyez ici un exemple très simple de cette réverbération. Moi j'envoie une question et les cinq résolveurs suivants me posent tous une question que j'ai envoyée initialement au client unique. Le premier résolveur est opéré par le fournisseur de services Internet du client. Ensuite, il y a une requête qui est validée. Après, c'est Google et c'est un *slave engine* de Google, avec la clef DNS DS DS. Je n'ai pas aimé le premier DS. C'est un peu étrange. Il y a un deuxième *slave*, 145, qui semble travailler avec le premier *slave,* parce que là il manque deux clefs. Ensuite, le deuxième résolveur est également impliqué et s'il manquait quelque chose, il y a un autre résolveur Google qui me demande l'enregistrement. Donc, en fait, le fait que ces trois adresses Google qui appartiennent au même esprit, ça c'est bizarre. Et ces 200 résolveurs qui font partie du même FSI se demandent ce qui se passe ici, donc plutôt que d'avoir trois requêtes et trois

réponses, vous voyez qu'il y a 12 requêtes et 12 réponses. C'est difficile à croire, mais on a l'impression qu'il s'agit de validation.

Voyez cette diapo. Pourquoi est-ce qu'il y a autant de requêtes ? Parce qu'elles ont été mal signées. Donc le premier résolveur 25522468 dit « voilà, je n'ai pas pu le faire ». Alors, il ne dit pas cela parce que dans le DNSSEC, on ne dit pas qu'on ne peut pas faire ça, mais il dit « server failed » (« échec du serveur »). Donc on essaie Google et Google dit « non, je ne suis pas serve fail », et « serve fail » sur le DNSSEC, c'est vraiment pas bon, parce que ça donne lieu à beaucoup de requêtes.

L'ECDSA, comment pouvons-nous voir combien de gens se penchent là-dessus ? La première est simple et concerne surtout les statistiques. Je compte le nombre de requêtes clefs DS et DNS et les réponses. Cela fonctionne durant 45 jours. J'ai fait [765 millions] de tests auprès de personnes, vraiment les publicités Google passent vers beaucoup de gens. Toutes ces personnes ont vu la publicité, 27% avaient le DNSSEC dans le RSA et ont vu la publicité. V6 est vraiment très jaloux de ces chiffres. L'ECDSA, 23%, c'est un peu bas comme chiffre. On continue et on va plus vite, je n'ai plus le temps.

Donc ce qui se passe, c'est qu'un sur cinq pouvant faire RSA ne feront pas ECDSA. Un sur cinq, c'est mieux sur mieux. En septembre 2014, c'était un sur trois qui pouvaient faire le RSA et

pas l'ECDSA. Nous nous améliorons si on regarde les statistiques.

Maintenant, je vais parler plus en détails. Je vais essayer de faire plus de recherches pour vous. Ce que je regarde ici, c'est la requête critique qui dit ECDSA et vient des infos DS. Si vous regardez les mots de nos anciens, si vous voulez, si vous regardez un peu, l'important c'est via les informations DS.

Ensuite, c'est vraiment quand je vois quelque chose dans le DS que je ne connais pas, j'abandonne. Ce qui m'amène vers le vraie réponse en utilisant une participation beaucoup plus détaillée. Un client sur six utilisant des résolveurs et utilisant le DNSSEC n'utilise pas le RSA pour valider l'ECDSA. Est-ce que c'est efficace ? Voilà, c'était mon résumé.

Je voulais vous dire, si vous habitez en République Dominicaine, vous avez 90% d'échec. Si vous habitez en Nouvelle-Zélande, vous avez aussi un pourcentage très élevé. Si vous habitez en Afrique du Sud, 75% d'échec, c'est mauvais ici. Donc même s'il y a vraiment une mauvaise réponse d'un sur six, pourquoi est-ce que cela fonctionne ainsi ? Nous avons pu identifier des résolveurs individuels. La plupart de ceux qui ne supportent pas ECDSA sont gérés par des compagnies téléphoniques et dans ce secteur, on sort les choses d'une boîte, on enlève l'emballage et on commence à utiliser l'outil, sans savoir ce qu'il y a dans la

boîte. Donc quel résolveur contribue au taux d'échec que nous avons ? Si vous aviez des gens qui comprenaient l'idée et la technologie, nous n'aurions pas ce problème.

J'ai fait ça en moins de temps que prévu, merci.

DAN YORK : Merci, Geoff. C'était très intéressant d'entendre ces informations. Est-ce que vous voulez parler, Jim, du côté opérateurs de registre ?

JIM GALVIN : Nous allons vous donner probablement de mauvaises nouvelles ou des nouvelles dont vous préféreriez qu'elles soient meilleures, mais je suis là pour vous donner de bonnes nouvelles.

En fait, du côté des opérateurs de registre, nous avons un rôle critique dans cet espace. Les opérateurs de registre sont eux-mêmes des consommateurs de ces technologies, et à cause de cela et comme nous signons des TLDs, nous devons trouver des solutions disponibles. Il est donc important de savoir que les opérateurs de registre ont des exigences qui viennent de deux endroits. Les normes qui sont, bien sûr, en cours d'élaboration. Nous avons une liste d'algorithmes de validation.

Par ailleurs de l'autre côté, en tant qu'opérateurs de registre et surtout en tant que gTLDs, nous sommes des parties contractantes de l'ICANN et des exigences proviennent des politiques de l'ICANN et nous devons y faire très attention quelquefois.

Mais en dehors de cela, il y a de bonnes nouvelles. Certaines choses sont faciles à régler. Des choses qui peuvent être faites pour pouvoir soumettre ces algorithmes aux exigences.

En tant qu'opérateurs de registre significatifs, nous avons énormément de fournisseurs et de TLDs que nous soutenons, donc nous avons besoin d'un service générique pour fournir un service à tout le monde.

De l'autre côté, dans l'espace où les opérateurs de registre contribuent, il nous faut assister les bureaux d'enregistrement, surtout dans l'espace gTLD. Parce qu'encore une fois, des exigences sont mises en place et il faut les suivre par rapport à l'ICANN. Il y a des règlements à mettre en place. Nous devons permettre aux bureaux d'enregistrement qui ont des serveurs DNS, veulent de l'assistance et ont des algorithmes, nous devons les aider à obtenir ces infos DS et à les mettre dans la zone TLD pour qu'elles soient disponibles. Cela ne fonctionne pas toujours, nous voudrions l'améliorer.

A notre avis, nous savons que nous avons l'avantage, nous voulons soutenir les TLDs, des TLDs différents, et encore une fois, pour nous, les restrictions sont limitées, en ce qui concerne ce que les bureaux d'enregistrement doivent faire. Nous accepterons tous les algorithmes validés parce que du côté des exigences de l'ICANN, on ne le permet pas. Il a quelques questions en termes d'inopérabilité avec les bureaux d'enregistrement. Certains opérateurs de registre préfèrent des infos clefs pour les mettre dans la zone TLD donc les bureaux d'enregistrement nous posent problème là-dessus. Il faut que les choses soient valides et régulières.

C'est la bonne nouvelle, certains opérateurs de registre sont plus focalisés, certains fournisseurs ont une variété de types de restrictions et ne vont donc pas forcément accepter l'algorithme, mais vous verrez que dans le nouvel espace gTLD, surtout ceux qui soutiennent cela, il y a moins de restrictions, et c'est ce qui fonctionne bien pour nous.

Donc, en résumé, ce que je peux dire, c'est que nous avons des requêtes qui nous viennent de l'extérieur, ce ne sont pas forcément des exigences technologiques. Si la technologie est là, nous sommes là pour la soutenir, mais nous devons suivre des normes qui nous disent ce que l'on peut faire. Il est donc important de garder à l'esprit que notre espace, dans cet

écosystème, est conduit pas les politiques que nous devons suivre vis-à-vis de notre relation contractuelle avec l'ICANN.

Ce sont des problèmes faciles à régler, c'est la bonne nouvelle. Nous voulons être de bons acteurs et de bons partenaires.

Je vous passe la parole pour que vous, vous parliez des choses négatives.

DAN YORK : Merci, Jim. Vous avez entendu parler de ce que nous devons faire pour pouvoir changer les algorithmes, nous avons entendu Geoff en parler, pour ce qui est de la validation. Nous avons Jim dire que les opérateurs de registre veulent bien le faire et appliquer ces changements. Maintenant Olafur va nous parler de ce qu'il observe dans ce processus. Puis nous passerons à Ondrej qui nous parlera des nouveaux algorithmes qu'il veut lancer. Ensuite nous aurons des questions-réponses. Moi j'ai des questions d'ailleurs, mais j'attends aussi vos questions, pensez-y.

Nous passons à Olafur.

OLAFUR GUOMUNDSSON: Nous avons déployé des nouveaux algorithmes DNSSEC cette année, non pardon l'année dernière, ça a été une longue année. Il s'agit de choses que nous avons trouvées.

Je suis désolé si je ne suis pas aussi amusant dans ma présentation que mes collègues ce matin, mais nous ne pouvons pas être aussi bons qu'eux, désolé. Je vais essayer d'être poli pour les interprètes. On m'a déjà disputé au Brésil parce que je parlais trop vite.

Prochaine diapo, s'il vous plaît. Nous sommes les premiers à faire cela à grande échelle. Nous travaillons donc très dur pour que les autres nous suivent, parce que nous pensons que nous faisons ce qui est bien pour des raisons très variées. La raison que nous avons apprise, c'est que le modèle d'enregistrement de l'ICANN qui a été copié par beaucoup de TLDs est cassé, parce que les opérateurs DNS n'existent pas dans ce modèle alors que ce sont eux qui devraient propager cette information au lieu de passer à travers la chaîne des bureaux d'enregistrement. On peut regarder avec une vue très simple le DNS, ce qui est beaucoup plus compliqué que ce que que les gens qui élaborent les politiques [peuvent comprendre]. Les serveurs d'autorité et les résolveurs clients, ils doivent travailler ensemble de façon très harmonieuse. Il n'y a aucun problème entre eux, pas de bugs, pas de délais dans les mises à jour, non, et personne ne se préoccupe des brevets.

Prochaine diapo. Beaucoup de ces systèmes utilisés par les gens pour publier des informations dans le DNS sont basées sur ce qui s'appelle des systèmes de provision. Il y a comme des fichiers utilisés par les gens, plein de choses, plein de façons de le faire. Toutes ces choses utilisées – quand quelque chose doit être publié dans le DNS, toute organisation doit faire ses propres mises à jour pour ces outils sur cette interface afin de publier quelque chose de nouveau. Cela ne s'applique pas seulement au DNSSEC. Donc le DNS est devenu – bon, vous verrez ça plus tard, vous verrez ce que ça devient plus tard.

Passons à la prochaine diapo. Comme Dan l'a dit tout à l'heure, pourquoi est-ce que les gens n'utilisent pas les bons algorithmes ? Il peut y avoir des moments, au niveau de l'opérateur de registre, où il a des règlements qui disent « nous permettons ces algorithmes ». Alors le logiciel n'est pas assez bien entretenu ou le HSM ne le supporte pas et il n'y a pas de développeurs, puisqu'il y a des gens qui utilisent le HSM, le HSM ne supporte pas les nouveaux algorithmes.

Il peut y avoir aussi des politiques nationales qui dictent ce qui doit être fait. La direction ne fournit pas les ressources nécessaires, un opérateur de registre a eu besoin d'un an pour soutenir l'algorithme numéro 13 parce qu'il n'avait pas assez de ressources. Je ne vais pas donner de noms. Pour être juste, il est très difficile d'expliquer aux dirigeants qu'il y a des bénéfices à

faire ces nouvelles choses. Ils vous disent « est-ce que ça va augmenter vos revenus ? », on leur dit non. Ils nous disent « est-ce qu'on va avoir meilleure allure sur le marché ? », peut-être. « Est-ce qu'il va y avoir des bugs ? », peut-être. Passez au prochain sujet, ils ne veulent pas en entendre parler. Donc tout le monde pense que ce n'est pas leur problème.

Nous avons aussi ce problème de déploiement pour la chronologie crypto. En supposant qu'il n'y ait aucun problème de brevet et que nous avons seulement affaire à la communauté académique et qu'on accepte que cette technologie crypto est ok. Je vais lui accorder dix ans, peut-être même sept ans. Il y aura des gens intéressés qui vont vouloir commencer plus tôt et d'autres qui voudront le faire plus tard.

Le nouvel algorithme sera défini d'ici dix ans, avant que l'IETF le standardise. Je pense que pour ce que ce soit inclus dans les librairies, cela prend entre deux et douze ans. Bien sûr, pour les spécifications DNSSEC, ça dépend de l'IETF.

Maintenant on parle des cycles de lancement et du logiciel DNS. Pour le 13, 14, 15, quel que soit le nouveau numéro d'algorithme que nous allons utiliser, de façon optimiste, on parle d'un cycle de plus de deux ans. Si nous parlons du logiciel «Entreprise », on parle de six ans. Je vois encore qu'il y a encore des BIND ouverts encore à trois - quelque chose qui a été lancé à moins de trois,

presque moins de trois. Donc c'est le cycle pour tous ces niveaux d'Entreprise, au niveau du logiciel d'organisation, c'est fait quand quelqu'un est prêt à le faire et insiste pour que le travail soit fait.

Prochaine diapo. Si nous devons rajouter les nouveaux algorithmes, c'est une seule tâche : motiver le reste du monde pour qu'il nous suive, ce qui est très difficile à faire. Nous ne pouvons pas présumer que les gens savent ce qu'ils font. Comme on l'a dit tout à l'heure, si on fait de l'installation quelque part, est-ce qu'ils comprennent exactement ce que l'on fait ? Nous n'en avons aucune idée. Puis il y aura beaucoup de gens qui diront que ça ne se passera jamais ou que ça ne fonctionnera jamais, alors que ça marchera.

Prochaine diapo. Nous pouvons obtenir l'attention des gens de temps en temps, mais pas toujours, donc il faut vraiment qu'on ait une bonne raison d'introduire ce nouvel algorithme. Il faut avoir de plus petites signatures, des algorithmes plus puissants, qu'il soit plus rapide, avec des propriétés de sécurité aussi bonnes que celles d'aujourd'hui. Il faut trouver les bonnes raisons, les quantifier et surtout éduquer les gens qui sont dans l'industrie du DNS et sont opérateurs de DNS. Ce n'est pas un statut quo, les choses vont changer de temps en temps et jusqu'à ce qu'on puisse amener les cryptographes à inviter des

algorithmes qui ne sont pas, disons cassables, nous serons dans cet espace.

Prochaine diapo. Il doit y avoir une bonne raison, comme je vous l'ai dit, donc il ne faut pas laisser tomber les algorithmes dont on pense qu'ils sont meilleurs. Il faut comprendre vraiment, mettre à la retraite les anciens algorithmes, et ce serait bon si on pouvait retirer l'algorithme numéro 4. Nous devons avoir de meilleurs paramètres et nous devons être capables de démontrer que les choses fonctionnent. Cela va prendre beaucoup de temps, donc nous travaillons comme James la limace.

DAN YORK : Merci, Olafur. Maintenant qu'Olafur nous a expliqué pourquoi tout cela va prendre beaucoup de temps ou que cela n'arrivera pas du tout, on va maintenant demander à Ondrej pourquoi on doit s'assurer que les choses fonctionnent. Je ne sais pas si nous sommes d'accord ? On est d'accord, en fait, donc on ne va peut-être pas se battre.

ONDREJ SURY: Je suis Ondrej Sury, je suis de CZ.NIC et je voudrais parler des nouvelles courbes du DNSSEC. Je suis désolé pour les petits caractères, je ne vois même pas les diapos. De toute façon, il y a

un travail fait par [Daniel Bernstein] qui est vraiment très connu dans l'industrie ; c'est une revanche pour lui d'introduire son algorithme dans le DNSSEC. Si vous connaissez cette courbe, elle a été faite par lui, par [Tanja Lange] qui vient d'une université allemande et elle prouve qu'il y a une différence entre les propriétés des différentes courbes. Elles sont définies par un ensemble d'exigences pour que les algorithmes de courbes elliptiques soient sécurisés. Je ne suis pas un chercheur dans la sécurité, je lie les points les uns avec les autres.

Prochaine diapo. Il y a un autre ensemble d'algorithmes avec des propriétés différentes de l'ECDSA. L'EdDSA a de bonnes performances, des performances élevées même si pas aussi élevées que le travail fait pour l'ECDSA, mais c'est quand même assez intéressant. Ça ne demande pas un nombre unique pour la signature, c'est vraiment de petites clefs que je définirais dans le DNSSEC. Les formules sont unifiées de façon puissante, donc elles sont valides sans exception. L'algorithme est résistant à la collision.

Prochaine diapo. Voici deux courbes qui ont été adoptées par le groupe qui s'occupe de la cryptologie à l'IETF. La courbe ed25519 and et le courbe ed448, qui s'appelle Godlilocks. Elles ont été définies en 2006 et en 2014. 2006, ce n'était pas la date de votre présentation ? Bon, ensuite, elle a été adoptée par

l'IETF. Donc, ça va, nous sommes sur la bonne voie. Alors la cible est de 128 bits pour la cible sécurité.

La deuxième courbe va plus vite encore, parce qu'elle a été définie en 2014 par Mike Hamburg, elle est encore plus puissante d'ailleurs. C'est comparable au RSA 15000 qui est un chiffre très important.

Il y a donc deux versions préliminaires pour le DNSSEC, pour les clefs DNS. J'ai soumis la deuxième au groupe de travail hier, au groupe de travail CURDLE. Elle sera peut-être adoptée. Pour la seconde, pour la ed25519, il y a consensus pour l'utilisation au DNSSEC. Si vous avez le temps, révisez le document.

On est dans l'attente de l'adoption de ces versions préliminaires, la version IETF EDDSA. La deuxième version préliminaire a été soumise hier. Il y a un opposant qui s'appelle Paul Hoffman. Si vous pensez qu'il y a une autre façon d'utiliser ed448, venez au groupe de travail CURDLE nous le dire afin qu'On sache quoi faire. Il y a plusieurs options sur la table. Peut-être peut-on fusionner les deux, ça m'est égal, mais nous devons prendre une décision à la fin de la journée. Il devrait y avoir une version préliminaire à venir, quelque chose qui va donc éliminer les vieux algorithmes qui ne sont pas utilisés en ce moment.

Prochaine diapo. Je pense que déjà beaucoup de choses ont été dites, donc je dirai qu'il y a eu un atelier de travail à Buenos Aires

organisé par le DNS-OARC, où on a invité plusieurs revendeurs. Donc vous êtes invités à participer au prochain atelier qu'on organisera.

On sait que ça prend beaucoup de temps, c'est qu'une fois qu'il y aura roulement de clefs dans dix ans, la clef de racine, on pourra utiliser peut-être cela comme algorithme. Quand je dis dix ans, je crois que je suis un peu optimiste.

DAN YORK : Merci, merci Ondrej. Oui, effectivement, quel sera le calendrier ? 2026 pour la prochaine KSK ? Ecoutez, j'ai une question pour Ondrej. Vous avez mentionné l'atelier de travail DNS-OARC, est-ce que vous pouvez en parler un peu plus, pour dire ce que vous voulez faire ?

ONDREJ SURY : Oui, c'était mon idée. Dans mon équipe, il y a des gens de côté des opérations et on devrait parler plus du cycle de vie de déploiement. J'aimerais continuer cette discussion pour voir comment faire en sorte que ça aille plus vite, parce qu'il y a des gens qui sont capables de le faire, donc il y a un problème avec le DNS qui empêche de la faire. Je pense donc qu'il est temps de changer le paradigme avec lequel nous travaillons. Ce sera peut-être dur mais il faut changer ce paradigme et on doit être

souples en termes d'algorithmes dans le DNSSEC pour faire en sorte que les choses fonctionnent à l'avenir. Entre la définition d'un algorithme et son application, beaucoup de temps peut s'écouler.

PAUL HOFFMAN : En fait, le gros problème, c'est la certification. Est-ce que vous êtes conscients de cela ? Un programme a récemment été lancé pour revoir la méthodologie pour le travail de certification. Avec cela, pourrez-vous aller plus vite pour permettre l'application des algorithmes ? Parce que ça, ça prévoit une mise en œuvre d'ici deux ans.

DAN YORK : Donc ce que vous dites, c'est que - qu'est-ce qui empêche cela, quels sont les facteurs qui empêchent cela ?

PAUL HOFFMAN : Il y en a deux en fait. On envoie des mises à jour régulières, les mises à jour pour les algorithmes, ce n'est pas le problème pour nous. Ça, c'est une première chose très importante. D'ailleurs, j'ai oublié la deuxième. Attendez, je vais m'en souvenir.

DAN YORK : Oui, effectivement, ça fait partie de votre réponse. Comment faire les choses plus vite ? Parce que vous, votre navigateur travaille de telle manière et peut travailler d'une autre manière. En tout cas, il obéira aux instructions que vous lui donnez. Dans le cadre du DNSSEC...

ONDREJ SURY : Je me souviens. Si vous êtes une grande société, ce sont les juristes qui nous retardent, en fait. C'est le problème des juristes.

DAN YORK : Vous parlez de Google ?

WARREN KUMARI : Je pensais que vous alliez proposer des messages textes pour dire « voilà, votre système n'est plus à jour, etc. Veuillez utiliser autre chose ».

DAN YORK : Est-ce qu'on peut le faire ?

WARREN KUMARI : Oui, bien sûr, on peut le faire.

INTERVENANT NON-IDENTIFIE : Autre question, si vous le permettez. Je voulais répondre à quelque chose qu'a dit Olafur. Je voulais insister sur un point, parce que je sais que dans ce genre d'ateliers, on préfère se concentrer sur les aspects techniques, mais ici à l'ICANN, c'est important de réitérer quelque chose qui a été dit auparavant. à cet atelier de travail, dans les réunions précédentes. Olafur l'a dit ici en fin d'intervention, et je voulais insister dessus, mettre le doigt dessus.

Il existe réellement un problème fondamental ici en termes de soutien par rapport à tout ce qui a trait au DNSSEC. C'est le fait que les fournisseurs de service DNS ne sont pas reconnus en tant qu'entité distincte dans l'écosystème, en tout cas dans le système ICANN.

C'est facile pour moi de dire « Vous savez quoi, moi, je ne vais pas entraver votre travail, ce n'est pas mon problème », et la plupart des opérateurs de registre ne s'y opposeront pas. Certains, pour des questions juridiques intéressantes, s'y opposeront peut-être, mais ce ne sera pas le cas de la majorité. Donc, même si ça peut être vu comme faisant partie du problème et que c'est quelque chose qu'on ne peut pas fournir, dans les politiques de l'ICANN, on ne peut pas le faire. Il s'agit de ne pas perdre cela de vue, en ce qui concerne la possibilité de déployer tout cela. Donc merci Olafur de l'avoir mentionné. Je voulais simplement le répéter. Je sais que vous en avez parlé

lors de vos précédents ateliers de travail, mais je voulais insister sur ce point. Merci.

DAN YORK : Oui, Geoff, vous savez provoquer, alors allez-y, je vous donne la parole.

GEOFF HUSTON : Alors, pour ce qui est de cette courbe elliptique et la cryptographie, les résolveurs n'acceptent pas tous ces courbes. Pourquoi ? Parce que dans le monde de la cryptographie, il y a toute une série de monocultures. Il est vrai qu'un grand volume de logiciels utilise des bibliothèques. Alors ce qui est intéressant ici avec la cryptographie à courbes elliptiques, c'est que pendant longtemps, jusqu'à, me semble-t-il, au début ou au milieu des années 2000, il y a eu un litige dans le domaine de la propriété intellectuelle pour savoir à qui appartenait cette courbe elliptique de cryptographie. Ça a donc donné lieu à un certain nombre de paquets de logiciels pour laisser cette cryptographie en dehors du paquet. Tout ce qui tournait autour de cela à l'époque, peut-être que c'était Red Hat 3, je ne sais pas, ça a donné lieu au fait que les premières versions n'incluaient pas cette courbe elliptique et ça a duré plus de dix ans.

Nous pensons que si un paquet apparaît aujourd'hui, il inclura la courbe elliptique, donc pourquoi est-ce que les utilisateurs continuent de promouvoir des choses qu'ils ne comprennent pas ? Parce qu'il existe des choses très vieilles parfois, et la combinaison d'incertitudes par rapport aux droits d'utilisation par rapport aux droits de propriété intellectuelle qui constituent un gros problème pour nous.

A cela s'ajoutent tous les problèmes de normalisation et le cycle extrêmement long par rapport aux résolveurs DNSSEC. Ça, c'est vrai aussi bien dans le domaine des opérations que pour beaucoup d'opérateurs ISP, ce type de résolveurs a un cycle de vie limité et ne peut être utilisé qu'une seule fois.

DAN YORK : Combien de gens ont un routeur à la maison, ce qu'on appelle un routeur ? Vous voyez de quoi je parle, n'est-ce pas ? Parmi ces gens, combien l'ont actualisé récemment ? Nous sommes vraiment très au point, ici. Alors, au cours de la dernière année – vous en avez acheté un autre ? D'accord. Autre question, vous avez tous une famille, vous l'utilisez à la maison. Combien de membres de votre famille, d'après vous, ont actualisé ce routeur ? Vous, vous répondez à toutes les questions. Ce sont les premiers élèves de la classe, .CZ et autres. Donc, bien sûr qu'il faut actualiser.

Pour ceux qui n'appartiennent pas à la République Tchèque ou à l'Europe, qui peut répondre ? Non, je crois que j'adresse à un public qui n'est pas le bon.

Robert ?

ROBERT MARTIN-LEGENE : Alors, je suis un citoyen anonyme. Si vous avez une ancienne installation de serveur que vous voulez actualiser, peut-être qu'il y a quatre ans, on n'avait pas besoin de validation pour utiliser le CC.

DAN YORK : Oui, vous voulez dire que la grande majorité des utilisateurs ne mérite pas cela, c'est cela ?

ROBERT MARTIN-LEGENE : J'ai dit que j'étais anonyme.

DAN YORK : Vous voulez répondre ?

ONDREJ SURY : Oui, je voulais répondre au commentaire de Geoff.

Oui, il y a des litiges touchant aux droits de propriété intellectuelle en lien avec les algorithmes dans le rapport dont j'ai parlé.

INTERVENANT NON-IDENTIFIE : Oui, 2013 et 2014.

GEOFF HUSTON : Il n'y a pas de litige par rapport à l'utilisation aujourd'hui, outre Warren.

INTERVENANT NON-IDENTIFIE : Oui, je ne peux même pas en parler avec mes avocats par email.

DAN YORK : Dani.

DNAI GRANT : Du point de vue des bureaux d'enregistrement et des opérateurs de registre, pourquoi faire des validations sur ces algorithmes ?

INTERVENANT NON-IDENTIFIE : Alors vous donnez une liste aux gens et vous validez ?

WARREN KUMARI : C'est parce que les utilisateurs ne sont pas forcément les plus intelligents. Ce qui se passe avec les bureaux d'enregistrement actuellement, c'est que lorsqu'il y a un numéro, 1, 2, 3, etc., c'est très difficile pour les utilisateurs de bien comprendre ce que ces numéros veulent dire. La plupart des utilisateurs n'ont aucune idée de ce que cela veut dire lorsqu'ils voient 13 ECDSA, ils sont perdus, ou ils pensent avoir besoin de 13 copies de cet ECDSA.

Donc il y a plusieurs cases. D'abord, validation. Et lorsqu'il y a une case DS, il faut la cocher. Il faut faire un contrôle, une vérification.

DANI GRANT : Vous avez très peu de choix, mais si vous utilisez ce RPI, vous avec la liberté de le faire ou pas. Mais pourquoi il y a validation, en fin de compte ?

[JIM GALVIN]: Ici, faudrait faire la part des choses entre les questions, parce qu'il y a une variété de points de vue là-dessus.

Du point de vue des opérateurs de registre, il est vrai que pour nous, nous n'avons de restriction particulière par rapport à ce que vous faites, donc on vous laisse faire tout ce que vous voulez, à condition qu'il y ait validation de l'algorithme.

DANI GRANT : C’est justement la question que je pose : pourquoi faut-il valider cela ?

[JIM GALVIN] : Vous avez raison, d’un point de vue pratique, on n’a pas besoin de le faire, mais on essaie de respecter les normes. Donc de mon point de vue, vous ne devriez pas être autorisés à faire quelque chose que la communauté ne considère pas comme étant valide. On essaie de faire notre possible pour que ça ne se produise pas. Donc une fois que vous avez vérifié ce genre de choses, on peut discuter du bienfondé de cela ou non, mais d’un autre côté, parfois, si vous êtes opérateur de registre, si vous prenez la clef et créez l’enregistrement DS au nom de l’utilisateur, il y aura peut-être des restrictions par rapport à ce que vous allez faire là. Et là, il y aura certainement des limites pour l’algorithme que vous pourrez utiliser et il faudra l’appliquer.

C’est une limite de ce côté-là et l’une des raisons pour lesquelles on ne prend pas de clef mais seulement le DNS. On fait ce type de vérifications du bon état de santé de cela.

DAN YORK : Et ensuite, on a tellement assaini l'esprit des gens sur le fait qu'il fallait passer par cette vérification et ce contrôle qu'il y a une vérification des limites.

[JIM GALVIN]: Une dernière chose. Malheureusement, parfois, un opérateur de registre en particulier, ça peut être un état, aura son propre choix à faire d'utiliser ou pas son propre algorithme. Ça, c'est à prendre en considération, il faut l'accepter.

DAN YORK : On a une question dans la salle, puis sur le tchat.

[MARK ELKINS ?] : Je voulais répondre à deux choses. D'abord, nous avons un service clientèle. Donc on ne laisse pas les clients faire des choses réellement stupides.

Deuxièmement, notre vérification de l'état de santé (« sanity checking » en anglais), on le fait aussi. Par rapport à ce qui a été dit par Olafur, nous avons aussi ajouté un petit bouton pour dire « obtenir mes enregistrements DS ». Donc par rapport aux services, aux noms de domaine, voici la clef, si c'est l'enregistrement DS que vous voulez obtenir, le voici. Pas besoin de faire un copier-coller. Oui, effectivement, c'est parce que

nous, opérateurs de registre, on parle aux bureaux d'enregistrement et aux titulaires de noms de domaine.

DAN YORK : Oui. Alors je vois qu'il y a une question.

JULIE HEDLUND : Non, en fait, ce n'est pas une question mais un commentaire d'Antoine [Gershwin].

Certains opérateurs de registre limitent les algorithmes parce qu'ils veulent être à même d'exclure les anciens algorithmes une fois qu'ils ne sont plus sûrs. Leur objectif est de faire autant d'argent que possible. Ces opérateurs de registre peuvent avoir différents objectifs, comme la confiance, la sécurité et vouloir contrôler leur image publique dans le domaine. Il n'y a pas de TLDs qui s'adaptent à tout le monde, ils ne sont pas capitalistes, démocratiques, communistes ou multi-parties-prenantes. Il faudrait mettre en œuvre les nouveaux algorithmes plus vite et enlever les algorithmes non sécurisés et les remplacer par leur algorithme parent.

DAN YORK : Oui, très bon commentaire. Robert ?

ROBERT MARTIN-LEGENE : Non, non, je ne suis plus anonyme. Donc, Robert de PCH.

Je me demandais si quelqu'un avait déjà fait l'expérience de la non-conformité ou plutôt du fait que des gens ne respectent pas les instructions données par rapport à la sécurité de l'algorithme.

GEOFF HUSTON : L'IETF devrait le retirer de la liste et ensuite nous, on l'enlève. A cet égard, on ne veut pas être vus comme l'organe police dans le monde ou chargé des cryptographes.

INTERVENANT NON-IDENTIFIE : Donc finalement ils restent sans signature plutôt qu'avec une signature inappropriée ?

INTERVENANT NON-IDENTIFIE : Outre les algorithmes pour cryptage, il y a d'autres algorithmes et lorsque vous [avez le type 1], ça s'élimine.

Autre question que j'aimerais poser. Pensez-vous que l'On devrait utiliser les types multiples ?

DAN YORK : Oui, vous avez raison. Vous vouliez faire un commentaire final ? Non, ce n'est pas la peine ? Bon.

Je ne sais pas si on a résolu quelque chose ici, mais je crois qu'on a parlé de défis, ce qui est une bonne chose. Et je crois que ce que je vous encouragerais à faire, c'est de regarder le rapport de projet d'Ondrej pour renforcer le DNSSEC.

On a parlé également des moyens de renforcer le déploiement et je vous inviterais à réfléchir pour le prochain atelier de travail sur le DNSSEC aux solutions qu'on pourrait apporter pour faire en sorte que ça aille plus vite.

Si vous voulez participer à cet atelier de travail, avant la réunion de l'IETF de Buenos Aires, n'hésitez pas à parler à Ondrej.

Merci. Les membres du panel suivant peuvent venir à la table.

INTERVENANT NON-IDENTIFIE : Il reste une veste dans la salle, si quelqu'un la veut, c'est vraiment une super veste qui vient de Washington. Taille extra-large, 5 dollars.

RUSS MUNDY : Russ Mundy, SSAC. Nous allons maintenant avoir la dernière séance de la journée. Nous allons parler du roulement de clefs dans la zone racine. Tout d'abord, je vais parler de ce que leSSAC a publié au sujet du roulement de clefs.

Geoff Huston vous parlera des résultats de l'équipe de conception qui a été créé l'année dernière. Le rapport a été publié. Lundi ? Je crois que c'était lundi. Le rapport est donc disponible pour le public.

[Ensuite, avec Warren Kumarie, de] Google, nous allons recevoir des perspectives de l'impact pour l'utilisateur lorsqu'il s'agit du roulement de clefs, et puis il y en a qui ne sont pas reliés à la validation pour Google. [Warren] viendra vous parler, il connaît beaucoup choses et pourra vous en faire part.

En tout premier, parlons de l'avis SSAC et des commentaires sur le roulement de clefs.

Nous allons du SAC 63 qui est le SAC du roulement de clefs DNSSEC dans la zone racine. Tout d'abord, une série de discussions a eu lieu pendant un an et demi, mais le SSAC a souligné cela comme étant un sujet très important pendant plusieurs années. Nous voulons donc encourager la communauté à commencer à travailler dans les temps. Donc nous avons commencé à travailler sur cela en 2012 et cela a été publié en 2013.

Il y a donc plusieurs domaines sur lesquels nous avons écrit des documents, sur tous les sujet intéressants que l'on devait examiner pour participer à ce roulement. Alors que le temps

passe, il y a des choses qui sont importantes, qui pourraient avoir un impact et qui vont changer.

Parmi les documents dont on va parler avec ce panel, celui-ci est le document le plus vieux et avait été publié en novembre 2013. Je vais passer directement aux recommandations. La première recommandation souligne le fait que le personnel de l'ICANN et les partenaires de gestion de la zone racine devraient mettre quelque chose en place. Ces trois parties, le NTIA, l'ICANN et les partenaires de gestion de zone racine devraient mettre en place une campagne de communication pour prévenir le monde entier que les choses seront mises en œuvre.

Encore une fois, le personnel de l'ICANN devrait mener, encourager et soutenir le développement de test pour examiner l'impact du roulement sur ce qu'on appelle les « middle boxes » et sur les autres machines qui seraient impactées par ce roulement, surtout que pour ces machines « middle boxes » ne soient pas laissées de côté ou cassées quand le roulement survient. Donc le personnel de l'ICANN devrait travailler de façon rapprochée avec la communauté afin de décrire ce que sera la cassure et cela est vraiment une inquiétude pour le SSAC.

Nous savons qu'il y aura des problèmes causés par le roulement. Nous n'avons pas encore défini ces problèmes, nous pensons qu'il serait mieux de demander au personnel de l'ICANN de nous

dire ce que ces problèmes vont être. Mais c'est important d'observer ces phénomènes, ainsi si vous avez plus de problèmes que vous ne l'attendiez, vous pouvez agir.

La dernière recommandation. Si quelque chose arrive ou ne fonctionne vraiment pas bien et que ce soit un échec, vous devez pouvoir revenir en arrière à l'étape précédente. Vous avez besoin d'avoir mis en place des déterminations pour savoir qui va prendre ces décisions, quels sont les paramètres qui seront utilisés pour prendre cette décision. Parce que, jusqu'à présent, rien n'est mis en place. On ne sait que faire une roulement de clef en amont, parce qu'on n'a jamais eu à le faire pour la racine elle-même. Il faudra donc peut-être revenir en arrière et il y aurait alors des choses à faire pour être prêts. La dernière recommandation est qu'on devrait récolter autant d'informations que possible et essayer de comprendre quelles seraient les informations importantes à récolter, pour que durant ce roulement, vous ayez assez de données à utiliser pour pouvoir comparer avec le prochain roulement à venir. Vous devez récolter tout ce dont vous avez besoin pour apprendre et mieux faire les choses la prochaine fois. Voilà donc nos cinq recommandations.

Si nous pouvions passer à la prochaine diapo. Ensuite, nous avons le rapport SSAC 73. Nous avons soumis nos commentaires

dans une version préliminaire du rapport de l'équipe de conception dont Geoff parlera tout à l'heure.

Dans ce document, nous avons mentionné que l'équipe de conception n'avait pas inclus dans la version préliminaire les informations liées au SSAC 63. Voilà donc un groupe qui travaillait sur la conception technique du roulement de clefs et un groupe qui avait rassemblé plusieurs informations déjà sur cela, et on n'a pas l'impression qu'il y ait corrélation entre les deux. On s'est rendu compte de cela et on voudrait suggérer qu'il serait important d'incorporer ces détails. On demande aussi au conseil d'administration de nous donner une mise à jour sur l'état des choses avec le SSAC 63 en ce moment. Comme vous le voyez, il y a beaucoup de choses en cours avec le SSAC.

Les diapos sont à l'écran, je voudrais passer là-dessus assez vite pour qu'on puisse rester dans les temps. Prochaine diapo. Nous attendrons la fin des présentations du panel avant de recevoir vos questions.

On va passer la parole à Geoff.

GEOFF HUSTON : Merci, Russ. Je suis Geoff Huston. Je vais passer assez rapidement sur toutes les diapositives. Voilà donc une chose importante dans ma présentation, parce que nous sommes

arrivés à un moment où approximativement un utilisateur sur six ne pourra pas résoudre un nom s'il n'a pas été bien signé avec le DNSSEC. Cela veut dire que si vous mettez votre signature dans le DNSSEC, une personne sur six ne vous verra plus. Donc si vous marquez la racine de la validation, voilà où se trouvera l'impact. Voilà le momentum que nous avons pour l'utilisation du DNSSEC. Si la signature n'est pas bien faite, beaucoup de gens sur l'Internet ne pourront pas résoudre ce nom. C'est exactement ce que nous voulons. C'est donc un chiffre intéressant et important parce que si vous vouliez demander aux gens si on fait notre roulement de clefs de façon négative, ces gens auront de sérieux problèmes de DNS ce jour-là, ce qui ne serait pas une bonne chose.

Nous revenons en arrière. Il y a cinq ans, cinq ans et neuf mois. Il y avait eu un problème dans la presse parce que des choses avaient été signées au mois de juin de cette année-là. Voici donc un document critique qui est un certificat de la déclaration de pratiques du DNSSEC publié à l'ICANN, sur ce qui allait être fait avec cette clef. C'est une déclaration importante, parce que sans cette déclaration, cette clef publique n'est qu'un ensemble de bits. On va prendre cette clef privée, la mettre sur toutes les portes qu'on va trouver et puis vous ne pourrez pas lui faire confiance. La seule raison pour laquelle vous devriez lui faire confiance, c'est ce document parce qu'il s'agit d'un engagement

de l'ICANN sur la manière dont ils vont gérer tous ces bits. Donc vous ne devriez faire confiance à ces bits que si l'ICANN se conforme à son engagement. Ces engagements de l'ICANN ne leur ont pas été imposés. Tout est très bien énuméré dans ce document et voyez la partie qui est encerclée dit que ce roulement – excusez-moi, je n'arrive pas à lire ce que j'ai sur l'écran – chaque zone racine dont le roulement s'exécutera le sera avec une série de clefs comme prévu, ou après cinq ans d'opération. Cela veut dire beaucoup de choses, cinq ans d'opération, de fonctionnement. Pour nous, pour l'équipe de conception, cela veut dire au cinquième anniversaire de la création de la clef. Ici, dans ce cas-là, 2015, une fois arrivé en janvier 2015, il était clair qu'on ne pouvait pas le faire mais on savait qu'il y avait un engagement de ce côté-là pour qu'on puisse le faire. Il fallait que cela fonctionne, parce qu'on s'était engagés et c'était l'engagement de confiance pour cette clef. Si on ne l'avait pas fait, on aurait eu un problème.

Un peu d'historique. Il y a deux clefs dans la zone racine. On ne parle pas des clefs pour signer la zone. Cette clef pour signer la zone fait l'objet d'un roulement tous les trimestres, donc au 1er janvier, 1er avril, etc. Cette clef fait l'objet d'un roulement automatique, disons. La nouvelle clef est publiée pour dix jours, la clef change, ensuite cette clef est gérée par Verisign

conformément au contrat que nous avons au niveau opérationnel.

La raison pour laquelle ils peuvent le faire, c'est qu'il y a une clef au dessus qui s'appelle la KSK, qui est utilisée pour signer la clef, pour que vos résolveurs puissent suivre cela magiquement, sans rien avoir à faire, c'est automatique. La clef de signature de clef est différente, c'est ce dont tous les résolveurs ont une copie, c'est dans votre machine, dans la mienne, si nos deux machines font la validation DNSSEC bien sûr, ça fait partie des données.

La vraie clef, la clef privée est gardée hors ligne dans un endroit très sécurisé, il y a des chiens de garde, tout ça. Excepté en Californie où les choses sont très relax. Nous avons vu ça à Amsterdam.

Ensuite, ICANN n'est pas le seul acteur, il y a un prolongement avec le Département du Commerce américain qui est un des partenaires, et bien sûr Verisign est aussi un partenaire. Nous avons été formés en tant qu'équipe de conception l'année dernière et toute cette partie aide à avoir une bonne conception pour permettre le roulement de cette clef. Un peu d'historique, Russ vous en a parlé tout à l'heure, il y a des consultations qui n'incluaient pas l'équipe de conception en 2012, puis nous avons eu une recherche d'ingénierie détaillée en 2013, ensuite une étude SSAC en 2013 et une équipe de conception de

roulement de clefs en 2015. Nous en avons beaucoup discuté en 2015. Nous voulions savoir comment les choses fonctionnaient, nous avons vu aussi une version préliminaire publiée pour commentaire en août et en octobre, nous avons préparé notre rapport final, jusqu'au mois de novembre d'ailleurs.

En premier, le roulement de clefs est important parce que tout le monde a une copie de la clef. Comment est-ce qu'on rend les choses automatiques ? Comment tout le monde obtient-il la nouvelle clef pour remplacer la nouvelle clef ?

Il n'y a rien au dessus de cela, il n'y a pas de façon automatique de le faire, il n'y a pas de mécanisme de confiance que l'on puisse utiliser, donc c'est le problème. Le problème aussi, c'est que si on se trompe, notre validation ne sera pas bonne et on aura la vieille clef. Ce qu'on essaie de faire, c'est de signer avec une clef différente. Ça s'appelle « serve fail », ce qui veut dire échec, ça veut dire qu'on est dans un trou noir. Il faut comprendre les protocoles. Donc si les protocoles sont suivis, ça vous dit que vous ne recevrez pas de réponse, c'est un échec dur, pas un échec doux.

Ce qu'on fait, c'est utiliser un autre truc de cryptographie, si vous voulez. On s'attend à ce qu'aucune clef ne soit compromise quand on arrive au roulement de clefs, mais ça ne marche pas si la clef est compromise. On s'attend à ce que tout se passe bien.

Comment on développe la confiance en la nouvelle clef ? C'est qu'elle soit signée par la vieille clef en laquelle on a confiance, on sait qu'elle peut signer la nouvelle clef qui sera donc bonne. C'est un mécanisme que nous utilisons, c'est documenté dans le RFC 5011.

Si on publie cette nouvelle clef et qu'on l'inclue dans la zone racine, mais que vous signez cette clef avec l'ancienne clef et que vous laissez tout cela là pendant un moment, si vos résolveurs suivent bien, je dis bien si, et encore une fois s'ils suivent le rôle de cette clef, on se dit « ah, la nouvelle clef va dire si elle charge ces nouvelles valeurs et que je les mets dans le cache des anciennes valeurs, ainsi on peut avoir les deux signatures », puisque c'est très dangereux de le faire, il ne faut pas laisser de vieilles données dans votre résolveur. Si j'arrive cinq ans plus tard et je trouve l'ancienne clef, et que je lui fais confiance, là on a un gros problème. On essaie donc de faire un nettoyage public et de révoquer l'ancienne clef. On la republie, mais là il y a un bit dans la signature qui dit que si on la trouve dans le cache local, on peut la retirer, il ne faut pas l'utiliser. Voilà donc les étapes.

Cela prend trois trimestres, neuf mois. C'est fait exprès. En haut, vous voyez la clef qui signe la zone, qui est en rotation tous les trimestres. On publie l'ancienne clef pendant dix jours, puis on

passe à la nouvelle clef de zone pour 70 jours, puis les dix jours suivants la nouvelle clef pour signer la zone est publiée.

En bas, vous avez le processus pour la clef qui signe la clef, pour le premier trimestre, au dixième, la nouvelle clef est introduite sans être utilisée, seulement introduite. Au premier jour du deuxième trimestre, la vieille clef va disparaître. Je sais que je dépasse mon temps, mais ce n'est pas grave. Donc la vieille clef va disparaître. Ce que vous avez à ce moment-là, c'est seulement la nouvelle clef. Si vous n'avez pas encore utilisé cette nouvelle clef, vous avez un problème. Puis ça continue et si tout va bien, le plan veut que la nouvelle clef soit publiée et on vous dit de détruire la vieille copie.

Voilà donc les trois points critiques, les trois étapes critiques : le pré-chargement, le roulement critique et le point de non-retour, comme vous le voyez à l'écran. Donc on s'attend à ce que cela fonctionne, n'est-ce pas ? Si tout le monde fait les choses correspondantes. Donc le RFC 5011 est soutenu pas les résolveurs. Nous savons que les réponses et tout se passera très bien, n'est-ce pas ? Voilà, bien sûr, ça on en parle même pas.

Comme vous le voyez à l'écran, le premier problème, c'est que certains résolveurs vont vous dire qu'ils gèrent leur clef de confiance manuellement. Peu importe ce que vous faites au niveau de la zone racine, cela va prendre beaucoup de

configurations pour changer la clef. Ils ont un problème, soit ils font attention ou bien oubliez tout, ils seront en échec. C'est le premier problème.

Le deuxième problème, c'est quand ces réponses deviennent plus importantes et que le DNS ne peut pas gérer de gros paquets. La voie du réseau entre les deux ne peut plus fonctionner. Vous ne recevrez peut-être pas de réponse, le réseau ne pourra pas forcément transporter toutes ces réponses.

Alors première préoccupation technique : certains de ces résolveurs ne soutiennent pas le roulement de clefs. Combien ? On ne sait pas. Combien d'utilisateurs ? On ne le sait pas non plus. Que vont-ils faire alors pour valider les échecs ? D'abord, vous allez faire du « thrashing », essayer, essayer. J'ai des preuves de cela ici. Sinon, on va vous dire non, simplement non. Il n'y a pas de réponse à aucune question, non tout simplement.

Que feront les utilisateurs quand il y a un retour résolveur ? Certains vont être des résolveurs non validant et non, ça veut dire non, ça veut dire noir, dans cette situation. On ne peut donc pas tester cela pour vous à l'avance. On a essayé tout type de choses pour voir comment s'immiscer et voir comment on peut traiter ce genre de résolveurs. On ne peut pas, on ne sait tout

simplement pas comment faire, et on va le découvrir lorsque ça se produira. Ça, c'est la réalité des choses.

Là, il y a beaucoup de choses en jeu autour du DNSSEC. Toutes les requêtes ont un ensemble DNSSEC ok, 87%, je vous le disais, ce qui fait beaucoup de DNS. 33% des requêtes DNSSEC ok tentent aussi de valider la réponse et la moitié utilisera un résolveur qui validera, l'autre moitié se verra dire non, ce qui veut dire non. On sait tous que tout ce qui est de moins de 1500 octets ne marchera pas. Au delà de 13500 octets, les choses se corsent et ce qu'on observe, c'est qu'environ 6% des requêtes reçoivent un bout tronqué dans les réponses et ils vont devoir utiliser les TCP. Tous les résolveurs n'aiment pas utiliser le TCP et il y a un taux d'échec de 1 à 2% environ. .ORG, de l'autre côté, utilise une clef DNS à 1650 octets, je ne sais absolument pas quelle est leur expérience, personne n'a dit que c'était affreux ou que ça n'avait pas marché. On a donc ces informations conflictuelles qui disent que 1 à 2% mourront, .ORG semble résister à 1650 octets, c'est l'internet, tout peut se produire. On ne sait pas non plus combien utilisent le RFC 5011. Donc certaines choses vont échouer. D'abord, résolveur non validant. Certains résolveurs peuvent donner une validation, sinon il ne se produira rien.

Cette diapo a été faite un peu avant le changement. J'allais vous montrer le rapport avant qu'il soit publié, parce que moi j'étais

un peu fâché qu'il ne soit pas publié, mais l'ICANN a décidé de le publier lundi. Donc ça, c'était dimanche, or lundi l'ICANN a décidé de le publier, il l'a donc été depuis.

Là, vous le voyez encore à l'écran, je vais vous laisser lire ces recommandations. Diapo suivante s'il vous plait. Attendez, recommandation 16, ce qu'on dit à l'ICANN. Est-ce qu'il y a une façon de mesure, de voir si ce problème est pire que ce à quoi on s'attendait ? Si on obtient plus de 50% d'utilisateurs qui continuent à utiliser ces points critiques, alors il est peut-être temps de réfléchir bien à une solution immédiatement. Ça, ça a été notre meilleure réponse à un dommage grave, après trois jours. Ça, c'est contestable, mais ce qu'on essaie de faire, c'est quelle est la mesure du dommage ? C'est une bonne mesure ça.

Voici le calendrier qu'on propose. A l'époque où ce rapport n'avait pas encore été publié, le 1er avril, ça semblait agressif, mais ce n'est pas aussi dur que cela semble l'être. Les neuf premiers mois, c'est la cérémonie des signatures de clefs, aucun changement pour la zone racine. Mais on donne neuf mois pour ouvrir la clef, avoir la cérémonie de signature de clef, faire tout cela puis roulement de clefs, et les choses se corsent le 1er janvier avec plus de clefs. Le 1er avril 2017, il n'y aura plus de vieilles clefs. Voilà comment ça fonctionne. Donc si tout se passe bien et sans dommages, tout devrait s'achever en septembre.

Que pouvez-vous faire ? Il y a quelque chose que vous pouvez faire et même que vous devez faire. Si vous voyez sur vos résolveur quelque chose qui ressemble à cela, vous pouvez aller vous recoucher. Vous faites du bon boulot parce que maintenant les choses marcheront.

Diapo suivante, là vous avez un problème. Si vous voyez ce message, il faut être attentifs ou sinon vous mourrez et on ne pourra rien faire.

Voilà ces deux diapos. Si vous utilisez les clefs, faites très attention au cours des deux années à venir. Si le calendrier change, il faut que vous le sachiez parce que c'est vous qui allez gérer cela. Si vous avez ce premier message, c'est bon. Si vous avec le deuxième, vous aurez des problèmes.

RUSS MUNDY : Merci pour cette excellente présentation. Des questions ? On passe aux questions. Warren dit que Geoff a déjà dit tout ce qu'il voulait dire. Donc on va passer aux questions maintenant.

ROBERT MARTIN-LEGENE : Merci. Robert, PCH.

Du point de vue des clefs, ça veut dire aussi qu'il faut bloquer les fichiers. Si vous ne l'avez pas configuré, ça ne marchera pas de toute façon.

Pouvez-vous revenir à la diapo sur le calendrier, avec les couleurs ? En fait, j'avais une question sur cette diapo. Au début du deuxième trimestre, lorsque vous commencez la signature de clef, vous dites lorsque vous retirez la première clef.

GEOFF HUSTON : Il est dit qu'en 2016, les enregistrements seront signés par la nouvelle clef et que les contenus de ces enregistrements de ressources seront la clef de signature sortante. Tout cela a été pensé pour minimiser la taille de la réponse. Il s'agit de la voie minimale qui ne délivre pas d'informations redondantes dans la réponse clef. C'est la plus petite taille qu'on puisse trouver. En dépit de cela, lors de la troisième clef, il faut remplir avec deux signatures, l'une révoquée, l'autre non. Donc ce point est de 1297 octets. Là vous aurez un problème.

ROBERT MARTIN-LEGENE : Peut-être que vous avez un RSSAC avec un TTL et que vous retirez l'ancien KSK, et là vous avez un problème, c'est ça ?

GEOFF HUSTON : Si vous avec une gestion de clefs automatique, la nouvelle clef, parce qu'elle fait partie de votre clef fiable, vous avez validé l'enregistrement DNS à ce moment-là.

ROBERT MARTIN-LEGENE : Donc avec .UK, comment je fais ?

GEOFF HUSTON : Mais .UK est signé, donc il n'y a pas de problèmes.

ROBERT MARTIN-LEGENE : Peut-être.

RUSS MUNDY : Justement, c'est le genre de choses qu'on regardait dans le RFC 5011, mais en tout cas ces discussions sont très encourageantes. Je suis sûr qu'il y aura d'autres questions dans la salle. Non ? Oui, allez-y.

[ABDEL FAI ?]: Bonjour, je suis [Abdel Fai ?], je viens d'Arabie Saoudite. J'ai une question concernant l'algorithme et la longueur de la clef pour la racine. Est-ce qu'elles vont changer, ces longueurs ?

GEOFF HUSTON : Pourriez-vous – en fait j'ai des questions que vous auriez dû poser, qui figurent à la fin de ma présentation. Attendez, attendez. Non, allez-y. Et en fait, je vais vous donner un prix parce que vous avez justement posé l'une de ces questions. La voici.

Est-ce qu'on devrait aussi opérer un changement d'algorithme ? Il est vrai que nous sommes moins préoccupés si nous utilisons l'ECDSA parce que le gros problème au niveau des paquets disparaît. Si vous passez à l'ECDSA, alors la réponse sera beaucoup plus petite.

Là, en fait, on essaie d'être conservateurs et de changer une chose à la fois, mais il existe une approche plus agressive de modification du protocole aussi. C'est la première fois que le monde est en train de faire face à un changement de la KSK. Donc soit on est conservateurs, soit on veut apporter de grandes réponses. Tant que les choses restent les mêmes, y compris la taille de la clef de la zone racine, alors le dommage sera minimal, mais ce sera bon, d'après moi. Là, si les choses passent à une plus grande échelle, on a des problèmes. Et nous avons pensé que nous ne pouvions pas ignorer l'ECDSA mais qu'on devait envisager ce qui pourrait se passer si on modifiait le protocole.

RUSS MUNDY : Pour ajouter quelque chose, le SSAC 63 en a parlé en interne et on n'a pas de détails là dessus, mais le résultat, c'est qu'il y a un rapport qui dit que vous devriez faire le roulement de clefs d'abord et ensuite l'algorithme, mais une chose à la fois.

GEOFF HUSTON : Personne dans la salle par rapport à la taille de la clef ?

RUSS MUNDY : La longueur n'a pas été étudiée.

GEOFF HUSTON : Les avis qu'on a reçu de la part des experts en algorithmes figurent dans le rapport : ne pas modifier cette longueur. Alors par rapport aux 1024 bits et aux implications sur le fait de changer la KSK, etc., d'utiliser telle ou telle autre, ça figure dans le rapport.

RUSS MUNDY : L'une des questions importantes, c'est qu'il faut que les gens surveillent avec grand soin leur système. Il faut diffuser ce message, il faut que les gens soient très prudents et surveillent les choses de près.

WARREN KUMARI : Moi j'ai travaillé avec Russ sur SSAC 63 et je suis d'accord avec toutes les recommandations qui figurent ici. Il est important qu'il y a d'autres documents qui font presque les mêmes recommandations que le document SSAC 63. Il y a eu au moins deux périodes de commentaire public, dont celui du RZM. Donc il est intéressant de voir que la communauté technique semble être toute sur la même longueur d'ondes, en disant qu'il faut avancer, et je crois que jusqu'à présent, en tout cas tous les rapports que j'ai vus, ont suggéré la même chose. C'est-à-dire maintenir le RSSAC actuel.

RUSS MUNDY : Y-a-t-il d'autres questions ? Dan ?

DAN YORK : J'aimerais remercier cette équipe de conception KSK et les remercier pour toutes les heures consacrées à l'élaboration de ce document, merci.

GEOFF HUSTON : Paul, vous êtes là ? Y-a-t-il d'autres personnes de l'équipe de conception ? Ondrej est parti. Paul et Ondrej, merci beaucoup à vous deux.

WARREN KUMARI: Etant donné qu'on a du temps.

RUSS MUNDY : Non, on n'en a pas.

WARREN KUMARI : Vous dites que 16% des gens ne pourront pas résoudre les réponses invalides. Vous dites aussi qu'il y a beaucoup de résolveurs qui servent ces gens. Mais ça laisse encore beaucoup de gens qui sont potentiellement en situation de risque. Vous parlez d'un certain pourcentage après trois jours, ce qui est acceptable. Mais j'ai l'impression que ça fait beaucoup de gens qui ne pourront pas faire fonctionner leur DNS. Comment expliquez-vous cela ?

GEOFF HUSTON : J'adorerais vous donner un chiffre zéro. Aucun dommage après trois jours et tout va bien fonctionner. Je ne pense pas que ce soit réaliste dans le monde de la technologie, avec les variations dont on est témoins. Même si maintenant on observe des dommages DNSSEC, ça apparaît comme un chiffre raisonnable. Ce qu'on essayait de dire, c'est que si on ne peut pas mesurer ces choses, on doit être en mesure de donner une fourchette, parce que ce ne serait pas une mesure fiable si on passait en dessous des 10%, donc fixer un calendrier raisonnable, ça aussi

c'était difficile. Comment est-ce que vous pouvez faire ? Au pif ? Parce que s'il y a un réel dommage, il faut pouvoir se retirer, mais voilà ce sur quoi on s'est basés.

RUSS MUNDY : Merci. J'aimerais remercier les membres du panel et j'aimerais inviter toutes les personnes à aller voir l'url qui figurait à l'écran et à examiner ce document en détails parce qu'il y a des informations particulièrement importantes pour les gens que ça intéresse. Donc, merci Geoff, merci Warren.

DAN YORK : Nous arrivons vers la fin de notre séance. Je remercie donc tous les gens qui sont ici, certains d'entre vous sont là depuis 9h du matin, je vous applaudis, on s'applaudit soi-même d'ailleurs.

Nous voudrions résumer la séance en faisant des suggestions afin que vous puissiez nous aider. Je vais donc dire que si vous êtes un opérateur de TLD ou de ccTLD, on vous demande de signer votre TLD. Nous avons entendu dire durant la journée qu'il y a beaucoup de ressources disponibles. Si vous êtes dans cette région d'Afrique, vous avez l'AFRINIC qui viendra faire des ateliers chez vous. Si vous n'êtes pas en Afrique, il y a d'autres ressources venant de l'ICANN et qui vous permettront de faire ces mêmes ateliers. Nous demandons aussi que les gens

reçoivent les enregistrements DS afin de travailler avec les bureaux d'enregistrement. Nous avons des statistiques, vous avez vu le diagramme que l'on avait à l'écran, et nous aimerions que tous les TLDs pertinents soient inclus. Nous demandons aux opérateurs de TLDs de suivre ces étapes.

RUSS MUNDY : Les opérateurs autres que les TLDs, si vous opérez des serveurs DNS, faites le DNSSEC. Ce n'est pas si difficile que ça et comme vous l'avez entendu aujourd'hui, il y a énormément d'aide et de soutien, de ressources dont vous pouvez bénéficier.

Les gens, dans cette communauté, veulent vraiment aider. Si vous avez un problème, vous pouvez vous tourner vers ces laboratoires, ces ateliers pour voir qui a parlé de quoi. Je peux vous garantir que si vous envoyez un courriel, vous recevrez une réponse avec beaucoup d'informations.

Les statistiques sont importantes, nous aimerions bien collecter plus de données pour voir ce qui se passe dans l'espace DNSSEC. Si vous êtes un ISP, démarrez les validations. Nous aimerions que cela augmente, nous aimerions voir plus de validations, c'est un point critique parce que si nous recevons des retours de sociétés, quand on parle de signatures qui disent « pourquoi devrions-nous signer puisque nous ne voyons pas de validations ? » et si on peut leur montrer les chiffres et leur

montrer combien de validations sont faites et où, c'est une réalité, vous devez le faire. On a donc besoin de plus d'engagement. Nous devons passer de 14, 15% à des pourcentages plus élevés.

C'est très simple, il suffit de permettre aux gens de le faire. Vous devez prendre conscience qu'à cause de vous, certaines personnes ne le font pas. Il faut préparer votre personnel de soutien pour qu'ils puissent accélérer les choses.

Il faut donc signer votre zone aussi, nous aimerions que vous promouviez le protocole DANE. On n'en a pas parlé beaucoup cette fois-ci, mais nous encourageons les gens à promouvoir ce protocole.

Si vous êtes un fournisseur de site Web ou de contenus, signez vos zones. Si vous êtes un opérateur de site Web, il y a une chance que si vous opérez votre site Web, vous opérez certainement votre support DNS. Si vous avez besoin d'aide pour la gestion de votre site, allez voir ceux qui opèrent les machines et dites leur que tout soit signé. Vous voulez aussi soutenir DANE. Allez voir vos vendeurs et assurez-vous qu'ils sont au courant que vous voulez le faire. Heureusement, avec le temps, les choses seront plus faciles, beaucoup plus de vendeurs le soutiennent mais beaucoup de nos vendeurs ont attendu et sont venus nous voir d'ailleurs, on nous a dit

« personne ne nous demande ». C'est la même réponse que nous avons reçu sur la validation, personne ne demande de validation, personne ne demande de DNSSEC. Demandez à vos vendeurs et à tous les services auxquels vous achetez.

DAN YORK : Ce que tout le monde faire, nous vous demandons d'utiliser le DNSSEC vous-mêmes, d'utiliser la validation, de signer votre propre domaine, faites ce que vous pouvez en votre nom pour que cela soit fait. Nous aimerions que vous partagiez les leçons retenues disons. Nous aimerions que vous partagiez vos expériences. Nous vous avons entendu des choses intéressantes ici et aussi durant la journée technique. Nous aimerions vous proposer de venir à l'ICANN 56 où que cela se passe et aussi à l'ICANN 57. On continuera à travailler à partir de cela.

Comme Julie l'a dit, des choses officielles se passent quand le conseil d'administration vote, mais bon… Ça dépend où on en sera. Bien sûr, nous aurons un panel régional, cela dépendra de l'endroit où nous sommes. Par exemple, ici nous avions des gens d'Afrique et donc en fonction de l'endroit où nous serons la prochaine fois, nous pourrons demander aux gens de la région de nous rejoindre. Nous voulons que vous aussi puissiez le faire.

On m'a demandé aujourd'hui s'il y a une façon de rester connectés aux gens entre les réunions. Il y a une liste de

diffusion que nous appelons la liste de coordination du DNSSEC, DNSSEC-coord, vous pouvez la rejoindre et partager vos informations.

Nous avons aussi une téléconférence mensuelle, le premier jeudi de chaque mois, sauf pour ce mois-ci bien sûr. Mais d'habitude, dans la plupart des cas, c'est le premier jeudi du mois. Nous discutons de ces questions, nous essayons de voir comment accélérer le déploiement et vous pouvez tous participer. Bien sûr, vous devez rejoindre la liste de diffusion pour pouvoir être prévenu de ces téléconférences.

Je voudrais remercier un groupe de personnes. Nos commanditaires, Afilias, Sara, Dyn et SIDN et nous voudrions les applaudir.

Sur ce, je voudrais vous dire que nous attendons encore de trouver un nouveau sponsor pour nous aider pour la fin de 2016, ainsi qu'un sponsor pour la réunion de mise en œuvre que nous aurons plus tard. Donc gardez cela en tête.

Je voudrais aussi remercier Julie et Kathy qui nous ont aidés pour que tout cela fonctionne très bien aujourd'hui.

Si vous voulez plus d'informations, voici des sites Web à l'écran : DNSSEC-deployment.org, Ainsi que les deux autres sites Web qui sont inscrits à l'écran. Le comité de programmation. Vous êtes

d'accord, on peut réparer le problème ? Il n'y a pas de .INTERNETSOCIETY, ça n'existe pas, c'est InternetSociety.org/deploy360. Il y a donc une erreur à l'écran.

Il y a aussi un lien vers la communauté DNSSEC pour que vous puissiez trouver la liste de diffusion et les statistiques nécessaires.

Merci à tous.

RUSS MUNDY : Un grand merci à notre département technique et à nos interprètes. Merci beaucoup.

DAN YORK : Avec les acronymes et tous les gens qui parlent très vite, ils ont eu beaucoup de travail aujourd'hui.

Sur ce, nous devons clore la séance et nous devons quitter cette salle assez rapidement, nous avons 15 minutes. Merci beaucoup et à la prochaine réunion ICANN 56.

[FIN DE LA TRANSCRIPTION]