KOBE– Atelier sur les DNSSEC (1 sur 3)
Mercredi 13 mars 2019 – 09h00 à 10h15 JST
ICANN64 | Kobe, Japon

RUSS MUNDY : Et bien, il est 9:00 du matin. Nous allons attendre encore quelques instants parce que la salle est un peu loin du reste des salles. Alors on va attendre quelques minutes avant de commencer. Merci. Je crois qu'il y a suffisamment de places, alors je vous invite à vous s'asseoir près de nous.

JACQUES LATOUR : Bonjour. On est prêts à commencer la séance. Bienvenue à l'atelier du DNSSEC à Kobe. Nous allons commencer avec la présentation que nous faisons normalement sur de déploiement du DNSSEC autour du monde, sa mise en œuvre à l'échelle mondiale. Qui est ici pour la première fois ? Ah oui, voilà, il y en a plusieurs, de nouveaux participants à ces ateliers. On a de nouveaux visages dans la salle.

Voici les membres du comité de ce programme de cette séance. Comme je vous le disais, voici donc les membres du comité de ce programme. Je vous parle un tout petit peu de cet atelier. On se réunit une fois par semaine et puis après, on prépare le

programme pour le prochain atelier. C'est un atelier que nous faisons tous les ans. Pendant toute l'année, nous essayons d'apprendre sur la version de l'atelier précédent pour améliorer les questions qui seront présentées dans la prochaine version de l'atelier. C'est quelque chose de très important.

Aujourd'hui, on a un déjeûner. Il y a beaucoup de sponsors. Steve travaille justement pour trouver des fonds pour trouver des sponsors afin de financer le déjeûner du DNSSEC. Merci aux sponsors de financer notre déjeûner.

Hier, il y a eu un évènement sur le DNSSEC en charge du registre local JPRS. L'atelier DNSSEC est une initiative conjointe entre le comité consultatif sur la sécurité et la stabilité de l'ICANN, le SSAC, et l'ISOC, Internet Society avec son programme déploiement 360, *deploy 360* en anglais.

Aujourd'hui, on est organisé en trois blocs principaux. Tout d'abord, la séance avec les membres du panel comme d'habitude et là, les personnes de la région parlent de la mise en œuvre des DNSSEC et des initiatives y afférentes. Puis, on fera une pause. Et avant le déjeûner, il y aura encore un autre panel du DNS sur TLS, DNS sur HTTPS. C'est une séance vraiment intéressante. Par la suite, il y aura un espace de questions et réponses, et puis le déjeûner. Vous devez avoir ce coupon pour

pouvoir déjeûner. Si vous ne l'avez pas, vous ne pourrez pas déjeûner. Je crois qu'on en a suffisamment pour tout le monde.

Après le déjeûner, nous aurons une séance spéciale pour parler du roulement de la KSK dans la zone racine. Nous verrons à quelle fréquence on le fait ; nous allons établir si ce sera fait une fois par semaine ou quelle en sera la fréquence.

Nous allons voir maintenant la mise en œuvre du DNSSEC dans le monde entier. On va voir des chiffres, des chiffres, des statistiques et plus de chiffres.

Dans les derniers mois, vous voyez une tendance descendante avant le roulement de la KSK. Mais maintenant, il y a une croissance. Et le 19 % des statistiques que vous voyez ici affichées sur l'écran font la résolution du DNSSEC. C'est un test d'APNIC pour mesurer dans le monde entier la capacité de résolution de DNSSEC de la part des résolveurs. Ici, vous pouvez voir des statistiques de l'Asie sur la mise en œuvre des DNSSEC. Il y a la Micronésie avec 66 % et puis après, cela se réduit au fur et à mesure, le nombre de validations. Puis vous avez les données de ceux qui utilisent le DNSSEC contre les fournisseurs internet qui utilisent leur propre serveur de DNS.

Dans cette diapositive, on voit un autre graphique. À gauche, on voit le .com avec un grand nombre de domaines signés. Je crois que c'est près de 800 000, 876 000 pour .com, .nl avec 640 000 et

puis .net avec environ 100 000. Pardon, le deuxième alors c'était .sc puis .net avec 100 000 et puis le domaine suivant, .arpa, à 4 000. On doit beaucoup travailler pour parvenir à ce que les domaines aient cette validation ou cette signature de DNSSEC.

ORATEUR NON-IDENTIFIÉ : Ces chiffres ne sont pas corrects. Ils sont erronés.

JACQUES LATOUR : Tu peux nous aider s'il te plaît ?

ORATEUR NON-IDENTIFIÉ : Ce n'est pas bien. Ces chiffres ne sont pas les bons. Il faut les corriger.

JACQUES LATOUR : Merci beaucoup. On a justement besoin de savoir tout cela. Vous devez le dire, vous devez faire les commentaires pertinents.

RUSS MUNDY : Oui, vous avez raison. Voici les résultats de SecSpider.

JACQUES LATOUR : Alors lors de la prochaine séance, on aura de meilleures informations plus justes.

Par la suite, on fait une cartographie qui montre les différentes instances de mises en œuvre des différents ccTLD. Par exemple dans certains cas, on a annoncé qu'il y aura la signature du TLD et dans d'autres cas, on a des enregistrements DS dans la racine. On n'a pas de soutien pour cela. Et pour finir, en vert foncé, vous avez les DNSSEC qui sont en train d'être mis en œuvre.

Voilà donc la carte. Et on a vu des progrès. Il y a cinq ans, il y avait plein de sites ne rouge. Il y en a quelques uns. Il y a des secteurs où il faut se concentrer : en Afrique, dans certaines parties de l'Asie, en Amérique latine. On a différentes initiatives pour que les ccTLD signent les DNSSEC. Ceci exige un travail technique et scientifique qui est simple et assez facile. Il y a le Soudan en Afrique, .sd, qui a annoncé que les DNSSEC seront signés dans son ccTLD. Depuis la dernière réunion de l'ICANN, c'est le seul ccTLD qui a annoncé la signature des DNSSEC, c'est le seul changement que nous avons pu voir.

En Asie, on a du travail à faire. Il y a des registres DS dans la racine. Pour nous, l'enjeu est de voir en quel moment le bureau d'enregistrement accepte les registres DS dans chacun des cas dans ce TLD. Il faut dire à Dan ou il faut envoyer un courriel à liste correspondante de l'ISOC pour informer qu'ils font la validation. Sinon, on ne pourra pas connaître ce type de situation. Lorsqu'il n'y a pas de registre DS dans la racine, c'est plus simple.

Dans cette carte, vous voyez là un site qui est en vert plus clair... Non, il y en a deux en vert un peu plus clair. Quels sont ces sites ? C'est la Croatie ? Bon. Il faut travailler pour arriver au 100 % de la mise en œuvre.

STEVE CROCKER : Je crois qu'en Scandinavie, dans cette région-là, il y a une toute petite île.

RUSS MUNDY : Il y a un petit site entre la Suède et la Finlande. Je crois que c'est .ax. Je ne sais pas si c'est bien prononcé.

ORATEUR NON-IDENTIFIÉ : Oui. Et on devrait commencer rapidement pour pouvoir travailler par rapport à la mise en œuvre.

JACQUES LATOUR : Ah bon. Alors peut-être devrait-on mettre une autre couleur sur la carte. De toute manière, on fait des progrès.

En Amérique latine, on est dans la bonne direction. Ils sont ciblés sur une plus grande quantité de signatures DNSSEC, alors il faut travailler là-dessus.

Je pensais que le Groenland devait être vert foncé. Il faut voir ce qui s'est passé. Voilà, c'est la dernière chose que nous avons reçue de l'Amérique du Nord. Vous pouvez télécharger la carte à partir de ce lien que vous voyez affiché sur l'écran. Et si vous connaissez des ccTLD dans la région qui font des progrès ou qui signent le DNSSEC, veuillez nous le faire savoir dans la liste de diffusion correspondante.

Alors l'ISOC travaille aussi dans un projet de l'histoire des DNSSEC. Vous pouvez aller sur ce lien que vous voyez à l'écran pour mettre à jour l'information si vous le trouvez utile.

Ceci dit, c'est la fin de ma présentation et maintenant, je vais répondre à vos questions.

RUSS MUNDY : Je ne sais pas s'il y a un participant dans la salle qui puisse répondre à propos de la carte ?

ORATEUR NON-IDENTIFIÉ : Oui, avec plaisir, je vais vous donner cette information sur tout ce que nous étudions, ce dont on fait le suivi. On a un corpus de données qui a un grand nombre d'informations. Nous pouvons donc vous donner tous ces renseignements, toutes ces données.

ORATEUR NON-IDENTIFIÉ : Oui parce qu'il y a beaucoup de signatures de DNSSEC.

RUSS MUNDY : On passe la parole au nouvel orateur. Comme vous voyez, on a quatre membres du panel de la région. Je ne sais pas si on a les diapositives pour cette section ? Génial, alors on va commencer par l'ordre de la liste dans le programme. Kenny Huang de Taïwan va faire la première présentation.

KENNY HUANG : Je suis le PDG de TWNIC. Je ferai une introduction très courte sur l'introduction du DNSSEC à Taïwan. Voilà ici la tendance du DNSSEC dans le monde. Prochaine diapositive s'il vous plaît. Voilà. Il faut appuyez là.

L'introduction sur la structure et les activités de la gouvernance de l'écosystème de l'internet. Les structures de la gouvernance concernent un modèle d'encouragement, d'incitation à la promotion des technologies. Nous devons tenir compte de trois composantes. La première, c'est la demande du marché ; la deuxième, c'est le réseau, aussi bien le fournisseur upstream que le fournisseur downstream. Cela représente le modèle de règlementation du modèle de gouvernance, le fait d'avoir un modèle de régulation qui promeut suffisamment d'utilisation de technologie.

Au point de vue du marché, il y a une très faible demande de résolution de DNSSEC sur le marché. Donc c'est assez faible à ce point de vue. On a développé de DNSSEC depuis l'IETF par la promotion du déploiement partout dans la région.

Au point de vue de la hiérarchie, le gouvernement de Taïwan soutient le développement du DNS. TWNIC a développé le processus de signature de .tw. Mais le contrat avec le bureau d'enregistrement de TWNIC ne demande pas la mise en œuvre de DNSSEC.

Comme vous le voyez, il y a la liste des bureaux d'enregistrement de TWNIC. Il y a une marque sur le registre qui marque coché qui indique quels sont les registres qui ont mis en œuvre le DNSSEC. Il n'y en a que six qui ont mis en œuvre le DNSSEC. Nous avons un dialogue avec ces registres pour voir quel est le problème et comment nous pouvons les encourager pour qu'ils mettent en œuvre le DNSSEC.

Là, nous voyons des statistiques de DNSSEC, surtout pour le deuxième niveau. Comme c'est le cas de .com, nous avons presque 0 % ; pour .edu, on est presqu'à 10 % de mise en œuvre du DNSSEC. Il y a donc beaucoup de travail à faire pour promouvoir le DNSSEC dans .tw.

Parlons donc maintenant des commentaires opérationnels nous permettant d'améliorer la mise en œuvre du DNSSEC. Le

DNSSEC permet d'atténuer les attaques de l'homme du milieu mais ne garantit pas la sécurité. En fait, un site malveillant ou un nom malveillant est une situation fréquente. Le DNSSEC n'ajoute pas beaucoup de valeur. C'est pourquoi les grands serveurs sont en quelque sorte réticents par rapport à la mise en œuvre. Le DNSSEC est trop neuf pour eux, même cela existe depuis des années. Dans leur expérience opérationnelle, ils préfèrent avec des configurations ou des déploiements de logiciels plus simples. Si quelque chose ne va pas, ils disent que c'est la faut du DNSSEC et cela peut leur faire perdre leur présence complète du internet.

À Taïwan, nous devons beaucoup travailler pour atténuer les situations à risque. Quelle est notre stratégie de pénétration ? Nous avons trois dimensions. La première concerne l'application de contrats pour justement impliquer les bureaux d'enregistrement et leur demander de donner leur soutien au DNSSEC. Nous avons vu qu'il y a des objections et nous allons continuer à parler avec les bureaux d'enregistrement pour continuer à appliquer le DNSSEC par l'application du contrat.

Deuxième composante, c'est le renforcement des capacités. Nous avons fait beaucoup formations sur le DNSSEC parce que c'est pratique et opérationnel pour les opérateurs. Nous continuons à travailler sur les ressources pour le renforcement des capacités.

Et la troisième composante, c'est l'hébergement du DNSSEC. Si un bureau d'enregistrement ou même un titulaire de nom de domaine qui au bureau d'enregistrement qui n'a pas d'hébergement, nous pouvons dans la situation actuelle leur fournir l'hébergement du DNSSEC.

Voilà notre présentation très simple. Si vous avez des questions, je suis là pour vous répondre. Merci beaucoup.

RUSS MUNDY : Merci Kenny.

Bruce, voulez-vous prendre la parole ?

BRUCE TONKIN : Bruce Tonkin de AUDA. Merci Ross. Je voudrais maintenant faire une mise à jour sur la mise en œuvre du DNSSEC en Australie pour le site .au.

Il y a plusieurs années que cela a été fait mais l'adhésion à cela était assez faible. Il n'y a eu qu'environ 1 400 domaines qui ont été signés sur un total de 3 200 000 noms de domaine. Un grand nombre de noms ont été analysés de façon individuelle pour avoir une idée des organisations qui ont signé. Les sociétés connues en Australie, il n'y en a que trois parmi elles qui ont signé le DNSSEC. L'une d'elles, c'est un cabinet conseil, un autre,

c'est Accenture et un autre, c'est Scania Il n'y a pas de banque, il n'y a pas d'organismes gouvernementaux ayant signé. Il y a donc eu très peu de signatures. À l'exception de ces entreprises, il y a un faible nombre de magasins, quelques titulaires de nom de domaine, quelques sociétés d'hébergement qui ont signé leur zone avec le DNSSEC. Il y a une forte concentration sur le marché sur ces trois bureaux d'enregistrement. Un peu plus de 80 % du marché offre le DNSSEC mais ce n'est pas quelque chose qui soit diffusé parmi les clients. Si l'on est une petite entreprise et on ne connaît pas le DNSSEC, on s'adresse aux titulaires de nom de domaine et on voit qu'il n'y a pas de zone signée. Cela se fait par les équipes de service d'après-vente plutôt que sur une interface en ligne. C'est une ressource qui permet de signer en ligne. Le processus est compliqué, donc.

À l'exception de ces trois grandes entreprises, l'autre grande catégorie est celle de l'industrie de la pornographie. Il semblerait que pour eux, la sécurité est plus importante que pour les banques.

La question que l'on se pose est de savoir pourquoi l'adoption du DNSSEC a été tellement limitée. J'en ai parlé à l'une des grandes entreprises de télécommunication en Australie et de leur point de vue. Il y a si peu de résolveurs de DNSSEC sur le marché vérifiant les signatures des DNSSEC dans le résolveur, ils craignent le fait que les clients ne puissent pas arriver sur les

sites et ils vont rendre coupable Telco, qui est l'entreprise justement de cette défaillance dans le service. Et le grand concurrent de Telco pourrait donc prendre sa place. Donc les compagnies ou les entreprises qui ne maintiennent pas les signatures du DNS de manière adéquate bloquent leurs clients, ce qui donne une mauvaise image du service. On se demande pourquoi on ne peut pas accéder à ce site et on suppose qu'il y a un problème avec Telco. La réputation pour eux, c'est une question de compétitivité.

Le problème en Australie est qu'il faut que les ISP les plus importants commencent à vérifier collectivement les signatures de DNSSEC et la résolution de DNSSEC. Cela inciterait les banques et d'autres institutions à commencer à signer leur zone.

L'une des initiatives en Australie à l'heure actuelle est la suivante. Nous avons un projet pour lequel nous donnons notre soutien pour développer un site pour vérifier le nom des entreprises qui mettent leur nom de domaine. Nous vérifions le site web des entreprises pour voir quelles sont les caractéristiques de sécurité dont ils disposent ou pas. Donc c'est l'une des choses à expliquer aux gens, cette question de la signature du DNSSEC.

Mais nous avons aussi besoin d'un autre type de vérification. On est tenté d'enregistrer ici les signatures des grandes entreprises

et organiser des sites web avec des signatures fausses. Quand on voit apparaître cela, on débarque sur une page sur laquelle on ne devrait pas se trouver et ensuite, on a un message qui dit qu'il faut contacter l'ISP parce qu'il n'y a pas les résolveurs nécessaires. Cela, c'est du côté du client, ce qui pousse le client à aller voir son ISP. Il y a certains sites qui lors de la visite, quand les gens se rendent sur ces sites-là, les gens voient apparaître cet avertissement sur une configuration inadéquate de l'infrastructure.

Une des tendances en Australie est de commencer à utiliser les résolveurs publics, le résolveur de Google est très intéressant. Un autre comme Quad9 est très intéressant. Le gouvernement australien ne s'inquiète pas beaucoup d'avoir une zone signée. C'est la deuxième plus grande zone qui n'a pas de signature. L'autre est gov.au. Nous en sommes au processus de la signature pour .au et le gouvernement a présenté un appel d'offres pour le service des résolveurs que devraient utiliser les agences du gouvernement. Le résolveur du DNSSEC toucherait à un taux d'efficacité, bloquerait les accès aux sites avec un logiciel malveillant ou d'autres problèmes. Ces résolveurs vérifieraient aussi la signature du DNSSEC. Donc sur le domaine gouvernemental, il y a un petit progrès mais c'est un progrès lent.

En général, nous n'avons pas beaucoup de noms de domaine signés et l'une des raisons pour cela, c'est l'absence de résolveurs en Australie entre les ISP des entreprises de télécommunications vérifiant le DNSSEC. C'est pourquoi nous devrions travailler collectivement pour utiliser des résolveurs appropriés sur le réseau.

RUSS MUNDY : Est-ce que vous avez des questions à lui poser ? Paul.

PAUL : Par rapport à la réputation des entreprises de télécommunications, j'imagine qu'il s'agit plutôt d'une inquiétude à propos des coûts. Ma question est la suivante. Les chiffres sont des chiffres datant d'il y a deux ans de Comcast. Il y a 3,2 millions de noms de domaine par jour qui sont vérifiés. Il y a une question liée au DNSSEC. La direction de Comcast ne se ferait pas de souci si elle pouvait faire payer 25 $ par interrogation. Je dirais que le coût de soutien d'un ISP au cas où une zone se serait agrandie a fortement décru. Je ne sais pas, si nous avons 500 millions d'interrogations par jour générant 24 incidents par mois, c'est plutôt bon.

BRUCE TONKIN : Ce serait utile de le savoir.

PAUL : Il faudrait que je parle avec l'équipe de Comcast.

BRUCE TONKIN : C'est une comparaison du service et de son coût.

RUSS MUNDY : Un commentaire que j'aurais dû faire au début. Nous sommes dans une salle où vous avez un service de traduction simultané. Nous allons donc vous demander que vous essayiez de parler lentement pour que les interprètes puissent vous suivre et interpréter. Nous devons toujours dire nos noms quand nous commençons à parler. Moi, je suis Russ Mundy et j'ai une question pour Bruce.

Si l'on tient compte des statistiques sur l'adoption sur le travail d'APNIC, bien sûr, on a travaillé avec d'autres mais ces statistiques sont surtout fournies par Geoff. Est-ce que cela inclut l'utilisation des résolveurs publics du DNSSEC ? Est-ce qu'il y a eu des interactions avec Geoff ou quelqu'un dans l'organisation de Geoff pour voir s'il y a des informations possibles basées sur ce travail que vous faites qui pourraient être utilisées pour convaincre les ISP si l'on tient compte du fait que les ISP n'ont pas les données du flux du trafic qu'ils

voudraient parce qu'ils n'ont pas de DNSSEC ? Ils vont sur Google ou 999 pour faire la validation ?

BRUCE TONKIN : Je ne sais pas si la défense de la signature permettrait d'obtenir davantage de trafic. C'est cela que vous voulez dire ?

RUSS MUNDY : Les personnes se servant de Google ou un autre résolveur public ne le font pas avec DNSSEC. Est-ce que cela pourrait être considéré comme une bonne comparaison ? Parce que souvent – je ne devrais pas dire souvent – mais la raison pour laquelle les gens travaillent avec le service public, c'est parce qu'ils obtiennent des données et les documents nécessaires pour travailler. Alors les fournisseurs de service internet peuvent acquérir des informations, des données en provenance du trafic si vous avez un référentiel de données du trafic.

BRUCE TONKIN : Je crois que Geoff a été consulté pour ce projet. De ce site web, pour travailler avec des petites entreprises pour vérifier leur nom. Cela est basé sur le travail des Pays-Bas, des sites web où l'on met un nom de domaine et que l'on fait plusieurs essais, plusieurs vérifications. Nous travaillons avec Geoff. La question est de savoir comment déterminer la qualification, la notation

du DNSSEC ? Est-ce que DNSSEC vaut 1 point, deux points ? Nous avons ce débat internet pour établir un système de notation. Si nous pouvions avoir une combinaison des données Comcast et des rapports de Geoff, nous pourrions présenter cela aux décideurs techniques des ISP pour qu'ils puissent avoir des données valables qui pourraient être utiles.

WARREN KUMARI : Warren Kumari, Google.

Une correction par rapport à quelque chose que Russ a dit. Au moins, l'un des grands fournisseurs du DNS n'a pas reçu d'information. Si nous regardons une déclaration des questions de privacité de 8.8.8, la question à se poser est pourquoi nous fournissons ce service. Nous le faisons parce que bon nombre des résolveurs des ISP, soit ils présentent des réponses ou bien ils sont très lents. La raison pour laquelle Google fait cela, c'est parce qu'un internet plus rapide signifie que plus de gens peuvent s'en servir pour se connecter si Google gagne plus d'argent. Ce n'est pas altruiste, évidemment, mais c'est un service que nous gérons pour que les gens puissent obtenir des réponses rapides.

Oui, d'accord mais je devais le dire parce que les avocats m'y obligent.

BARRY : Une autre correction très réduite de ce qu'a dit Russ. C'est des interprètes, pas des traductrices comme on l'a dit. C'est très important. Et ici en plus de l'anglais, nous avons le français et l'espagnol. Malheureusement, nous ne pouvons pas faire le japonais.

RUSS MUNDY : Une autre question ou d'autres commentaires pour Bruce ?

[Applaudissements]

Merci Bruce. Très bien.

Maintenant, nous avons la présentation de David Morrison de .nz. Oui, c'est l'internet de la Nouvelle-Zélande.

DAVID MORRISON : Bonjour à tous. Je vais faire ma présentation. Je vous prie de passer à la diapositive suivante. OK.

Je veux faire une présentation pas aussi technique sur l'adoption du DNSSEC en Nouvelle-Zélande. Nous, on a une pratique spécifiée dans notre site web que vous pouvez consulter. Mais je vous raconte un tout petit peu que nous avons commencé en 2012 avec la mise en œuvre des DNSSEC. Et nous avons évolué dans nos opérations clés. On a réussi à avoir une

très bonne évolution et nous avons un plan de récupération vis-à-vis les désastres et la continuité de nos plans commerciaux.

Nous avons 88 bureaux d'enregistrement autorisés et il n'y en a que deux qui offrent la signature des DNSSEC. Et sept parmi ces 88 offrent ceci pour les enregistrements DS. Alors on a beaucoup de travail à faire encore, comme notre collègue l'a dit, par rapport à .au.

J'essaie de passer à la diapositive suivante. Voilà.

Alors, on a eu du succès à .gov.nz qui a la signature DNSSEC à 41 % des noms de domaine signés, donc c'est un degré acceptable d'adoption. Le gouvernement de la Nouvelle-Zélande a fait un appel d'offres pour les bureaux d'enregistrement et l'une des exigences était justement de fournir le service de DNSSEC parce qu'on est en train de passer à une nouvelle plateforme. Et des 714 000 domaines, on a eu une adoption très réduite, très faible du DNSSEC. Si on voit les noms les plus populaires et on voit le trafic du DNSSEC, on voit que seulement 195 des 100 000 sites web principaux de la Nouvelle-Zélande utilisent cette technologie. Il y a donc beaucoup à faire encore.

On travaille avec notre équipe technique pour avoir le système DANE et le SMTP. Je crois qu'on fait un bon travail à cet égard. On a des fournisseurs de service internet très importants qui

permettent de parvenir à une couverture de 60 % de tous les utilisateurs de la Nouvelle-Zélande qui ont des serveurs validés. Bien.

Nous devons travailler, nous devons éduquer et former les utilisateurs finaux dans les systèmes, les bureaux d'enregistrement, pour que tout le monde comprenne la complexité de cette technologie.

Pendant les dernières années, il y a des nouvelles technologies pour automatiser les processus du DNSSEC. Nous voulons donc éduquer les gens pour qu'ils se rendent compte que ce n'est pas aussi complexe que cela ressemble. Il faut voir aussi la question de l'économie et du changement. Il faut voir, comme dans le cas de l'adoption du protocole HTTP, PDP IPv6, il faut l'aborder de la même manière.

Et pour finir, quant à l'adoption de la part des bureaux d'enregistrement, nous croyons que nous n'allons pas obliger les bureaux d'enregistrement à travailler avec DNSSEC. Nous voulons par contre les encourager pour qu'ils comprennent qu'ils peuvent améliorer leur service en termes de sécurité.

Voilà donc l'aperçu que je voulais vous présenter sur la situation en Nouvelle-Zélande. Merci beaucoup.

RUSS MUNDY : Vous avez des questions à poser ? Oui, allez-y.

JOHN : Quel est le processus pour parvenir aux registres du DNSSEC dans la zone si vous n'avez pas DNSSEC ?

DAVID MORRISON : C'est une question technique et je ne suis pas en mesure de vous répondre en ce moment, mais je peux chercher la réponse et vous la dire plus tard.

RUSS MUNDY : Vous avez des questions pour David ? Moi, j'en ai une.

Vous voyez qu'il y a un haut niveau d'adoption quant à la validation et vous avez dit que ceci est dû notamment au fait que les ISP les plus importants ont adopté la validation. Depuis l'adoption de la validation, vous voyez des modifications dans la quantité de zones signées, c'est-à-dire une plus grande validation entraîne comme résultat un effet mesurable ?

DAVID MORRISON : Non. Étant donné les chiffres que nous avons, cette augmentation n'est pas significative.

RUSS MUNDY : Vous avez des programmes de formation que vous essayez de mettre en place, surtout compte tenu du nombre de validateurs que vous avez déjà ? Peut-être pourriez-vous le faire avec vos collègues de l'Australie dans la région pour éduquer les gens ?

DAVID MORRISON : Nous avons un programme que nous allons commencer à analyser avec un opérateur de ccTLD, avec notre communauté de bureaux d'enregistrement l'année prochaine. Et le DNSSEC feront partie de ce programme en ce qui concerne la question de la sécurité en Nouvelle-Zélande. Nous allons donc l'aborder du côté de la sécurité. Nous voulons aussi travailler avec les bureaux d'enregistrement dans ce but spécifique.

RUSS MUNDY : Quelqu'un d'autre à une question pour David ? Très bien. S'il n'y a plus de questions, nous tenons à vous remercier de votre présentation.

[Applaudissements]

Maintenant, nous allons voir la présentation de Yoshiro Yoneya du JPRS. Il fait partie d'une de nos entités hôtes.

YOSHIRO YONEYA : Bonjour. Je suis membre aussi du conseil d'administration du domaine ccTLD .jp au Japon qui au ne communauté très active. Je vais vous parler de la situation par rapport à la mise en œuvre des DNSSEC et aussi sur nos activités de diffusion.

En premier lieu, je voudrais vous parler de la situation des DNSSEC au Japon et de leur mise en œuvre. Nous avons quelques ISP principaux qui donnent des validations DNSSEC à leurs utilisateurs. Il y en a qui fournissent un service complet et d'autres, un service facultatif, parce qu'il y a un grand nombre d'ISP qui sont toujours préoccupés d'une défaillance des DNSSEC. Parce que si les utilisateurs se voient affectés par ces défaillances du DNSSEC, les opérateurs de soutien doivent aider les utilisateurs. Et les opérateurs de soutien ne connaissent pas la cause racine de la défaillance. Alors comme on l'a également dit, le coût opérationnel devient de plus en plus élevé.

En ce qui concerne la signature des DNSSEC, nous voyons qu'il y a très peu de zones signées au Japon. Là, vous voyez dans le tableau certaines organisations qui sont très importantes et qui ont signé la zone, par exemple les organisations gouvernementales qui ont environ 800 agences, mais il n'y en a que 15 ayant signé le DNSSEC. Vous pouvez accéder au site web correspondant qui va vous montrer tous les détails.

Un grand nombre d'opérateurs de DNS espèrent la mise en œuvre ou attendent la mise en œuvre des DNSSEC. Par exemple, les Jeux olympique de Tokyo en 2020 vont encourager la mise en œuvre des DNSSEC parce que cela constitue une partie importante de la cybersécurité et ceci peut réduire le risque d'incidents liés à la sécurité. Il va y avoir aussi en mai 2019 la réunion du G20 à Osaka et aussi un championnat mondial de rugby cette même année dans notre pays. Tout cela implique le besoin d'avoir un haut niveau de cybersécurité. On utilisera donc le DNSSEC pour protéger les sites web en question.

Puis, on a eu une amélioration dans les services des opérateurs de registre, des bureaux d'enregistrement et des opérateurs de DNS. Nous allons donner du soutien en ce qui concerne la cryptographie de la courbe elliptique. Il y aura aussi du soutien pour la gestion des clés et l'automatisation des DNSSEC ou des DNSSEC automatisés. On n'a encore aucune annonce officielle, mais j'ai contacté les opérateurs correspondants qui m'ont dit qu'ils vont procéder à ces mises en œuvre dont je vous ai parlé. Je suis donc optimiste à cet égard et j'espère que ceci aura lieu dans un avenir proche.

Maintenant, je vais vous parler de nos activités de diffusion pour ce qui est du roulement de la KSK dans la racine. Au Japon, on a commencé à informer et à créer du renforcement des capacités depuis 2015. On a commencé avec la sensibilisation à ce

moment-là, on a travaillé dans des groupes de réseau d'opérateurs qui sont très importants au Japon et puis dans des réunions de communautés du DNS et des opérateurs de DNS.

Parfois, on utilise des termes un peu forts, « fragmentation de l'IP » ou « interruption du service dans tout l'internet ». Pourquoi ? Parce qu'on veut attirer l'attention des gens, on veut les convoquer à ces évènements que nous organisons.

Nous distribuons également des documents en japonais. Nous distribuons des documents techniques. Il y a un comité technique qui a beaucoup de documents en anglais comme l'ICANN et il y en a très peu en japonais. Un grand nombre de nos opérateurs ne parlent pas anglais. Il a été donc important d'avoir ces documents traduits.

Le gouvernement du Japon à travers le ministère de Affaires internes et des communications a encouragé la mise en œuvre des DNSSEC et a encouragé également la préparation pour le roulement de la KSK dans un bon nombre d'organismes gouvernementaux. Ceci a eu un impact très bon et une prise de conscience sur toutes ces questions au Japon. Le résultat, c'est qu'une grande partie des opérateurs de DNS au Japon ont fait des tests de production très efficaces, très effectifs pour l'utilisation du logiciel nécessaire pour la mise en œuvre de ces technologies. Il y en a qui ont été assez critiques des documents

techniques correspondants. Comme corolaire, il a fallu travailler avec les documents techniques de l'ICANN sur les ancres de confiance.

On a également mené des enquêtes ou des sondages au sein de la communauté au Japon. Vous pouvez voir les résultats dans les liens qui sont affichés sur l'écran. Un tiers des ISP, suivant les résultats de ces sondages, a signalé avoir commencé à donner des validations de DNSSEC. La plupart parmi eux a également signalé d'autres caractéristiques sur ces services et a manifesté également s'être préparé pour une défaillance éventuelle du roulement de la KSK. Les opérateurs du Japon ont pris très au sérieux le roulement de la KSK et ils se sont très bien préparés.

Pour ce qui est du roulement de la KSK, on a appris ce qui suit. Comme je vous l'ai dit, nos fournisseurs de service internet se sont très bien préparés pour le roulement. Ils ont également utilisé des documents techniques qu'ils ont trouvé insuffisants. Ils ont donc préparé leur propre scénario. Et je crois qu'il est très important d'avoir ces documents techniques pour de futurs sondages pour de futurs tests. Ils ont eu également un canal pour faire le monitorage, un canal sur Twitter, un blog aussi en temps réel parce qu'ils ont surveillé un évènement en temps réel et ils devaient savoir ce qui se passait au fur et à mesure.

Et pour finir, je voudrais dire que la communication bilatérale entre les opérateurs est très importante parce que ils nous donnent leur point de vue très réaliste, très pratique vis-à-vis de la partie opérationnelle. Et leur connaissance et le partage de toutes ces informations, c'est quelque chose de très important pour nous préparer pour ces évènements et pour que tout fonctionne bien et aussi, pour le succès de la mise en œuvre du DNSSEC.

Merci.

RUSS MUNDY : Merci beaucoup. Il y a des questions dans la salle pour notre orateur ? Yoshiro, merci beaucoup.

JOHN : Vous commencez ou vous envisagez l'automatisation de DNSKEY ?

YOSHIRO YONEYA : Le .jp n'a pas pris ceci en charge mais il y a certains opérateurs et fournisseurs qui se préparent pour la mise en place de DNSKEY.

RUSS MUNDY : J'ai une question pour Yoshiro. Vu cette préparation si exhaustive des ISP pour le roulement de la KSK, je ne sais pas si cette information a été partagée, si vous avez suivi des procédures de test par écrit, si vous avez partagé ces documents mais de toutes manière, ce serait vraiment bien d'avoir cette documentation disponible pour des présentations dans de futurs ateliers du DNSSEC. Alors s'il y a des documents ou des présentations disponibles et si vous voulez les partager, nous allons les recevoir avec plaisir.

D'autre part et compte tenu du degré de préparation et du nombre limité de signatures que vous avez réussi à avoir, je ne sais pas si je me souviens bien des chiffres mais il y avait environ 800 agences gouvernementales. Alors vous croyez qu'il y aura une amélioration ou une plus grande quantité de zones signées avant les évènements dont vous avez parlé, surtout de la part du secteur gouvernemental ?

YOSHIRO YONEYA : Par rapport à votre premier commentaire, un grand nombre d'opérateurs japonais sont très timides et ils ne veulent pas expliquer leurs expériences ou les partager avec le grand public. Alors si on peut garantir leur anonymat, alors là, oui, on peut partager nos expériences. Et j'espère que l'on aura

prochainement une interprétation et traduction japonais-anglais.

Comme je l'ai mentionné, les Jeux olympiques sont un évènement international et ces jeux seront le moteur de la signature de la zone des DNSSEC pour les organismes gouvernementaux parce que les informations que l'on donnera aux touristes, aux journalistes sont très importantes pour nous au Japon. La privacité et la confidentialité des données sont très importantes aussi, le respect de la vie privée, parce que si l'on publiait des fausses informations sur un faux site web, l'utilisateur doit être protégé. Il faut protéger l'utilisateur des informations fausses. J'espère donc qu'un grand nombre d'organismes gouvernementaux et certains portails de nouvelles signent leur zone de DNSSEC et possèdent la certification correspondante.

RUSS MUNDY : Une dernière question à propos de ce sujet. Avez-vous vu un accroissement de l'adoption des DNSSEC, surtout pour ce qui concerne DANE et l'encryptage du courriel ? Est-ce que vous avez vu des modifications des tendances ? Il n'y a rien de particulièrement visible ?

YOSHIRO YONEYA : Je ne vois pas du tout DANE.

RUSS MUNDY : Merci beaucoup Yoshiro.

[Applaudissements]

Encore une fois, au nom de toutes les personnes présentes, je veux remercier les membres du panel de leurs présentations qui ont été très utiles et très intéressantes. C'est une information de première main de ce qui se passe. J'espère que nous pourrons nous aider mutuellement et avancer.

Je vois que nous sommes en avance par rapport à notre programme. Cela permettra à Bruce de finir sa présentation et d'aller prendre notre café à temps. Donc Bruce, si vous voulez reprendre votre présentation sur la transition du DNSSEC ? Voilà.

BRUCE TONKIN : Bien sûr. Pour répondre à une questions posées auparavant sur le fait de savoir si une petite entreprise met une entrée du DNSSEC et que le registre ne peut pas répondre à cela, la réponse générale en Australie, cela devrait être transféré à un registre qui le possède. Sur le marché, il y a différents registres et bureaux d'enregistrement qui fournissent différents services.

Il faut donc profiter de l'occasion pour transférer les noms à un fournisseur de service possédant le DNSSEC. Ce serait a réponse la plus générale.

Premièrement, quelques antécédents. Nous sommes le backhand du registre .au. Nous avons fait la transition au registre backhand en 2018 et nous opérons plusieurs serveurs comme com.au, net.au, gov.au et edu.au. C'est le nom des serveurs qui sont nés aux États-Unis, .com, .net, .mil, etc. Donc nous nous occupons de l'opération du TLD de .au. Nous nous occupons des enregistrements et nous nous occupons de l'outsourcing des opérations au troisième niveau.

Nous avons fait la transition de 3,2 millions de noms de domaine dans de nouveaux registres et l'objectif était de compléter cela pour le 1er juillet. Il y a eu des problèmes dans cette transition. D'abord, c'était la transition la plus grande de l'histoire, c'était plus de 3 millions de noms, et cela a eu des complications à plusieurs niveaux.

Nous avions non seulement des noms au second niveau mais aussi au troisième niveau et au quatrième niveau pour beaucoup de registres, et même au cinquième niveau. Nous avions des écoles dans l'état de New South Wales dans le domaine de l'éducation. Donc la transition des noms de

domaine en plus des registres se faisait à des niveaux multiples ; parfois, c'était cinq niveaux de transition.

Donc le registre a fait sa migration le 1er juillet et l'approche que nous avions voulu avoir par suite de la complexité consistait à compléter autant que possible dans le mois préalable au 1er juillet pour que la fin de la migration requiert le moins possible de choses, avoir 48 heures pour cette coupure. Et nous avons réussi à le faire sur 24 heures parce qu'une bonne partie du travail avait déjà été faite.

Quant aux registres du DNSSEC, nous avons enregistrés les nouveaux services avec le nouvel opérateur en parallèle avec les serveurs de noms de l'opérateur précédent. Nous avons commencé aussi à introduire la plupart des registres au fur et à mesure que nous traversions les différentes couches pour pouvoir les mettre en fonctionnement en tout cas et pour permettre la propagation de la constellation de services autour d'eux. Nous avons pu mener à bien une bonne partie des tests à l'avance. Nous avons fait d'abord un test en backhand avant de faire le test en production pour vérifier que la configuration serait appropriée.

Voyons donc quelles ont été les étapes. Je sais que la plupart d'entre vous dans cette salle, vous êtes des experts mais j'ai pensé que ce serait bon d'avoir une documentation de

l'approche que nous avons utilisée. Le premier pas, c'était le roulement de nos clés à une fréquence plus élevée que celle que l'ICANN utilise. Nous avons eu un roulement des clés que nous faisons toutes les années. Nous avons fait plusieurs roulements des KSK au cours des dernières années. Nous avons fait le roulement de la ZSK tous les trimestres, donc tous les trimestres, nous faisons le roulement de la ZSK. Ce que nous avons dit, c'est que nous ne devons pas faire un roulement de la ZSK au beau milieu de la transition. Donc le première point était de disons bloquer ou geler ces roulements.

La prochaine étape, c'était la génération des nouvelles KSK, créer des nouvelles clés pour les niveaux tenant compte du fait que nous n'avions pas la transition du niveau supérieur parce que cela concernait le .au du niveau supérieur. Mais nous avons fait la transition des niveaux inférieurs, .com, .net, etc. Pour chaque niveau, nous avons créé de nouvelles KSK, ZSK et pour les registres qui n'étaient pas trop importants.

Nous avons envoyé ces clés à l'opérateur de registre actuel. Il a publié les clés sur la zone. Et pour comprendre la hiérarchie, nous avons publié un registre de DS. L'opérateur actuel présente ou publie le registre de la clé au prochain niveau de .au et pour les niveaux suivants, et cela a été publié le 5 juin, c'est-à-dire presqu'un mois à l'avance par rapport à la transition qui allait se faire le 1er juillet. À ce moment-là, nous avions déjà publié les

registres de DS à tous les niveaux de la hiérarchie, à l'exception de gov.au que nous avions réservé pour le jour de la transition. Nous n'avons pas signé gov.au pendant ce processus.

D'autres détails. Le nouvel opérateur a configuré les serveurs de noms en parallèle avec l'opérateur existant. Le nouvel opérateur a commencé à publier les zones qui avaient été signées par l'opérateur précédent. Cela a commencé le 25 juin. Avant cette date, ils recevaient des copies de la zone et on faisait un *query* du serveur de noms et le serveur de noms pouvait voir que la réponse était active. Les registres SOA, le public pouvait voir ces services avant cette date. Mais le 25 juin, nous avons mis les registres des serveurs de noms et le public pouvait commencer à signer les zones. Ensuite, nous avons réduit les temps de vie avec les différents registres de DS ainsi que le SOA. Nous avons réduit la durée de vie à 300 secondes. Nous avons fait cela le 20 juin.

Une semaine avant la publication des zones courantes sur le serveur, nous avons réduit le TTL de certains registres dans certains registres, ce qui nous a permis d'effectuer les modifications assez vite.

L'opérateur actuel a cessé de fournir ses services dans les zones le 26 juin. À ce moment-là, le nouvel opérateur avait tous les serveurs de noms de DNS publics mais l'opérateur créait les

zones qui étaient stabilisées chaque jour avec de nouveaux enregistrements de noms. Et l'opérateur préalable fermait les zones en utilisant l'infrastructure de signature de clé.

Ensuite le 30 juin, nous avons bloqué les bureaux d'enregistrement pour qu'ils ne puissent pas faire de modifications dans le registre. Là, on les a bloqués pour éviter les modifications ou les changements dans la zone. Le nouvel opérateur a commencé à générer les zones et à les signe en utilisant ses propres clés. Nous avons encore les registres de DS des clés précédentes de l'opérateur précédent qui étaient publiées sur la zone. Mais nous signions et nous utilisions l'infrastructure de la signature de clé du nouvel opérateur. Cela a été fait le 30 juin.

Et ensuite le 1er juillet, nous avons commencé le basculement de la migration. Et là, l'opérateur a publié les registres avec ses propres clés de signature. Après cela, nous avons éliminé les registres DS et DNSKEY des zones et nous avons augmenté là la durée de vie à 900 secondes. Voilà donc les modifications ou les étapes.

Maintenant, des changements plus fréquents. J'ai parlé de la fréquence de roulement des clés. Pour .au, nous faisons cela une fois par an. C'est une erreur là, on devrait lire KSK sur l'écran. KSK, c'est 2 048 octets et la ZSK, c'est 1 280 octets. Il y a eu une

demande du gouvernement pour augmenter le niveau d'encryptage pour ce qui est de la longueur de la clé. Nous avons donc mis en œuvre ce changement pour que la KSK puisse atteindre 2 048 bits. C'est assez solide si on considère que ce roulement se fait une fois par trimestre. Je voudrais savoir ce que font les autres par rapport à la longueur de leur clé, s'ils ont augmenté la taille du paquet comme nous le faisons. Je voudrais savoir quelles sont donc les autres actions ou mesures prises. Nous l'avons fait en suivant les recommandations du gouvernement australien.

Voilà, je crois que c'est tout. Nous sommes juste à temps pour le café.

RUSS MUNDY : Merci Bruce. Je vois des questions. Paul ?

PAUL : Quel est l'algorithme dont vous vous servez pour les clés ?

BRUCE TONKIN : Nous venons de mise à jour les modules de signature et nous supportons un algorithme de courbe elliptique. Mais en fait, nous ne voulons pas trop changer de choses en même temps. Ce que nous changeons en ce moment, c'est la longueur de la clé.

Mais l'idée est d'aborder des algorithmes à courbe elliptique aussi.

PAUL : Ce sera un autre exercice très intéressant. Je vous souhaite bon courage et bonne chance.

BRUCE TONKIN : C'est une zone vraiment vaste et l'infrastructure critique en Australie est importante. Nous voulons donc voir d'abord comment le font les autres aves des zones plus petites et nous allons ensuite le faire progressivement.

KATHY : Nous avons une participation à distance. « Je m'appelle Zeinab Mohamed, NextGen. J'ai une question pour Bruce et pour Yoshiro. Est-ce qu'il y a une collaboration avec les universités ou les institutions académiques leur permettant d'augmenter leurs connaissances et que les petites entreprises et les utilisateurs soient plus nombreux pour signer leur domaine ? » Voilà la question.

YOSHIRO YONEYA : Pour être franc, nous avons consulté le public et les universités et le monde académique fait partie du public. Mai nous n'avons

pas de séances ou de tutoriaux particuliers pour la société ou pour les petites entreprises parce que la portée est assez réduite et les ressources sont limitées. Alors ce type d'activités n'a pas encore été mené à bien. Si la mise en œuvre des DNSSEC était plus vaste, nous pourrions mener à bien ces activités mais pour le moment, ce n'est pas le cas.

DAVID MORRISON : En Nouvelle-Zélande, nous n'avons pas non plus d'activités sur l'espace académique des DNSSEC. Mais nous avons travaillé avec les groupes d'opérateurs pour faire un travail de sensibilisation, d'éducation dans nos organisations sur la validation. C'est quelque chose que nous avons exploré et nous aurions une réponse semblable. Nos ressources sont limitées mais nous espérons bien pouvoir effectuer des modifications l'année prochaine.

BRUCE TONKIN : Nous n'avons pas non plus une grande participation des universités sur les DNSSEC. Si l'on considère la liste de noms qui ont été signés, je vois qu'il y a une université qui a signé. C'est l'université Bond University au nord de l'Australie. Aucune autre université n'a signé sa zone. Mais cela est disponible sur .au.edu pour ceux qui voudront s'en servir. Je crois qu'il faut dire que les rapports avec les universités s'établissent plutôt au niveau du

département des politiques. C'est un peu comme au sein de l'ICANN où il y a davantage d'avocats que de techniciens ou d'experts.

RUSS MUNDY : Un commentaire que j'ai à faire à propos de cette question, c'est qu'il y a de plus en plus d'universités qui développent et qui font la promotion de leurs programmes d'études et leur programme en général sur la question informatique. Je travaille pour une entreprise qui a des rapports avec des universités pour beaucoup de sujets. J'ai vu beaucoup de programmes d'études, beaucoup de cursus avec des thèmes tels que le développement du DNSSEC, les fondements du DNSSEC. On pourrait même obtenir le soutien des étudiants pour des programmes de mentorat, etc.

BRUCE TONKIN : Il y a un membre du conseil universitaire, Nigel [inintelligible] de l'université de New South Wales. Levez la main. Oui, bien sûr, nous avons des rapports avec les universités.

DAVID MORRISON : Nous avons un contact avec les universités. Dans le domaine de la recherche, il y a un programme de subventions pour la recherche. Dans l'avenir, nous pourrions peut-être encourager la

recherche pour ce qui est de l'adoption des DNSSEC. Nous devons donc continuer à évaluer cet espace et cette possilibité.

RUSS MUNDY : C'était la seule question en ligne ? Kathy, est-ce qu'il y a d'autres questions pour Bruce et pour cette dernière présentation ? Voilà.

Donc je dois dire que nous avons été vraiment ponctuels, c'est presque l'heure du café. À 10:30, nous reprendrons notre travail. Merci beaucoup Bruce.

[Applaudissements]

**[FIN DE LA TRANSCRIPTION]**