YEŞIM NAZLAR : […] clé, en ce mercredi 19 octobre 2016, à 19 heures UTC. Il n'y aura pas d'appel puisqu'il s'agit d'un webinaire, mais j'aimerais rappeler tout le monde de bien indiquer son nom avant de prendre la parole, pour la transcription et également pour que les interprètes puissent vous interpréter dans les lignes interprètes.

Nous avons l'anglais, le français et l'espagnol lors de cet appel. Merci à toutes les personnes présentes. Je repasse la parole à Tijani.

TIJANI BEN JEMAA : Merci beaucoup Yeşim. Bonjour à tous. Merci d'être présents à ce wébinaire.

Comme vous le savez, il y aura un changement du roulement de la clé de signature de clé à l'ICANN, donc pour le DNSSEC. Et donc nous nous sommes dit que cet évènement était d'une importance suffisante pour que nous organisions ce wébinaire.

Je vais donc commencer par donner la parole au personnel pour les détails administratifs et ensuite, nous pourrons commencer. Yeşim ?

YEŞIM NAZLAR : Merci beaucoup, Tijani.

Nous avons donc la présentation dans la salle Adobe. Pendant le wébinaire, si vous avez des questions, nous vous encourageons à les taper dans la partie Q&A, donc à gauche sur la fenêtre, on va à gauche.

Il y aura également une partie questionnaire, donc soyez prêts à répondre aux questions du petit test de la fin de notre appel.

Voilà. Je vous repasse la parole Tijani.

TIJANI BEN JEMAA : Merci beaucoup, Yeşim. Comme je le disais, il s'agit d'une activité très importante. Et donc la communauté d'At-Large va prévoir un certain nombre d'activités pour informer notre unité constitutive. Nous avons donc avec nous le vice-président de la recherche et le responsable technologique de l'ICANN qui nous fera une présentation sur cette question du roulement de la clé de signature de clé.

Donc la clé de signature de clé est en fait la clé cryptographique la plus importante dans le DNSSEC. Et comme vous le savez, le DNSSEC nous protège des activités frauduleuses, de l'usurpation de données, et de détournement vers des sites frauduleux. Donc voilà pourquoi nous avons invité Ross, pour nous donner davantage d'informations là-dessus, et il va donc nous parler de cette clé de signature de clé. Allez-y.

MATT LARSON : C'est en fait Matt Larson qui est là. Je suis président de la recherche et de [inaudible] technologique. Merci beaucoup à tous de m'avoir accueilli pour cette présentation et je vais maintenant commencer.

Alors, vous avez peut-être entendu dire que nous allons bientôt changer au sein de l'ICANN les paramètres d'intégration dans le DNSSEC, et pour un certain nombre d'opérateurs de réseaux, cela pourra créer un besoin d'actions. Donc au sein de cette discussion nous allons parler assez

rapidement du fonctionnement du DNSSEC, comment cela fonctionne, et qu'est-ce qui se passe en termes de roulement de KSK. Et je laisse un petit peu de temps à la fin pour vos questions.

Alors, nous allons d'abord aborder la question de savoir comment fonctionne le DNSSEC. Je crois que tous vous connaissez le DNS, alors je vous donne des exemples très brefs. Quelqu'un peut par exemple demander une [IT] pour un nom de domaine, donc exemple w.com, et ensuite on a une adresse IPv6 qui apparait, qui correspond à ce nom de domaine, alors le DNSSEC c'est simplement une signature cryptographique, une signature numérique, par-dessus les données, par-dessus la réponse.

Validation du DNSSEC. Alors il s'agit d'un processus [d'infection] de cette signature numérique pour s'assurer qu'elle est valide du point de vue cryptographique, et cette signature vérifie l'authenticité des données. Pour valider la signature, il faut une clé publique. Alors la clé publique a généré la signature, et la clé privée permet de la valider.

La raison pour laquelle le DNSSEC existe c'est que le protocole du DNS est en fait assez crédule et facilement dupe. Donc lorsqu'on envoie une requête DNS, et qu'on n'a pas le DNSSEC, en fait, il faut faire confiance à la réponse que l'on reçoit en retour. On ne peut pas savoir si la réponse qu'on a reçue vient réellement du lieu auquel on a posé la question au début. Cela veut dire qu'on peut obtenir des réponses usurpées, des réponses fausses, et donc avoir de fausses informations.

[inaudible] les mesures, nous nous sommes rendu compte qu'il y avait des moyens d'éviter cette usurpation, mais malgré tout, la protection n'existe pas. Donc grâce au DNSSEC, nous pouvons maintenant faire

confiance aux réponses parce que nous avons en fait une preuve cryptographique comme quoi ce que vous avez reçu est la même chose que ce qui existe dans la [zone], mais que ces données n'ont pas été modifiées par le biais d'un autre serveur que celui du client.

Donc non seulement le DNSSEC évite l'usurpation, mais cela est également une base d'extensions de protocole à venir, l'utilisation du DNS à venir, et donc cela permet de fournir un environnement sécurisé pour le DNS. Donc sécurisation des transferts de l'email, introduction de clé publique dans les emails, et également supplément d'opérations de certificat x.509. Donc tout ceci peut être inclus au DNS également.

Le DNSSEC comporte trois types d'enregistrements qui contiennent les données de la clé cryptographique ; alors là c'est un petit peu compliqué. Désolé. Mais je crois que si on devait tout refaire, je pense qu'on n'aurait pas nécessairement conçu le système de cette manière, mais ce qui se passe est que chaque zone est signée et protégée par le DNSSEC. Et il y a en fait une paire de clés. Premièrement la clé de signature de clé, et cette clé de signature de clé signe toutes les autres clés dans la zone. Et puis il y a d'autres clés en fait qui correspondent à des clés de signature de zone qui produisent les autres signatures qui sont validées.

Ensuite, on a l'enregistrement de signature de délégation, et comme je le disais, à la base c'était censé simplifier les affaires, mais quoi qu'il arrive, c'est une sécurisation des systèmes qui existent. C'est ça la chose qu'il faut retenir.

Alors je rentre un petit peu dans les détails de ceci lors d'une diapositive à venir. Alors, ce que nous avons ici c'est comment on valide une

signature numérique ? On a les données DNS en haut, donc là, un enregistrement avec l'adresse IPv6 donc www.exemple.com, ensuite il y a la signature numérique qui fait partie du DNSSEC et qui est créée sur l'enregistrement. Et pour valider cette signature, nous avons besoin de la clé publique qu'il a créée. Et une fois qu'on a toutes ces informations, on peut valider. Et validation, ça veut dire est-ce que les données sont authentiques ? Est-ce qu'elles sont valides ?

Donc comme vous le voyez, vous avez besoin de la clé publique en orange pour valider, mais la vraie question ici c'est comment est-ce qu'on fait confiance. Bien sûr qu'on peut obtenir cette clé du DNS, mais comment est-ce qu'on fait pour savoir si on peut lui faire confiance ? Et donc voilà pourquoi nous sommes là aujourd'hui. Voilà pourquoi nous allons parler de l'ancre de confiance de la racine.

Donc le DNS nécessite une chaine de confiance, pour qu'il y ait en fait une confiance par rapport à la clé qui se trouve en bas. Il faut en fait commencer par une clé à laquelle on fait confiance, l'ancre de confiance, cette clé-là. Donc si vous regardez en haut à droite, vous avez la KSK de racine, ça c'est l'ancre de confiance que tout le monde utilise aujourd'hui.

Alors ancre de confiance, qu'est-ce que ça veut dire ? Ça veut dire que dans votre validateur de DNSSEC vous avez validé et vous dites je lui fais confiance à cette clé quoi qu'il arrive. Ensuite, il y a processus de validation qui [inaudible]. Basés sur cette clé, on valide donc grâce à cette première clé la clé [DSK] ensuite le .com, de [ds.com] et ensuite le .com KSK, et vous voyez donc que je ne vais pas tout vous détailler. Si vous suivez les flèches, vous voyez que c'est une chaine de confiance,

une chaine de signatures. Et en fin de compte, au bout de cette chaine, on arrive à la signature, et on peut donc faire confiance à exemple.com [gsk]. Dans ce cas on peut faire confiance à ce cas que nous avons là à l'écran. Donc l'adresse www.exemple.com.

Donc je vois qu'il y a beaucoup d'informations, mais cela j'espère permets d'illustrer un petit peu l'importance de cette ancre de confiance. Et la KSK de racine c'est vraiment le point de départ qui permet de valider toutes les autres données qui font partie du DNS. Donc c'est pour ça qu'il est important de bien savoir à quoi correspond cette KSK de zone racine.

Alors il y a énormément de TLD qui sont [signés], donc il y a beaucoup d'informations qui existent dans la zone racine, et ce qui est important de retenir, c'est que ceci renforce ce que je disais tout à l'heure comme quoi le KSK de zone racine est très important, parce qu'il y a énormément de choses qui sont signées sur la base de cette clé.

Donc comme je le disais, l'ancre de confiance c'est en fait toute clé dans laquelle un opérateur place beaucoup de confiance aux fins de vérification d'authenticité. Alors il est possible que vous faites plus confiance à une ancre de confiance simplement parce que vous avez installé un logiciel spécifique et que vous avez confiance, ou alors vous pouvez le configurer vous-même. Vous avez fait des recherches. Vous avez trouvé une ancre confiance, etc., mais quoi qu'il arrive, ce qui se passe, c'est que vous faites confiance à cette ancre de confiance.

Alors je ne vais pas entrer dans les détails là-dessus. Il y a d'autres ancres de confiance qui existent. Vous pouvez utiliser une autre clé, configurer d'autres clés qui seront vous ancres de confiance comme

validateur, mais ce processus n'est pas courant. L'ancre de confiance KSK donc est la plus importante et c'est sur celle-ci que nous allons nous concentrer aujourd'hui.

Alors, maintenant je vais parler un petit peu du fonctionnement du DNSSEC. Alors la zone racine est compliquée puisqu'il y a de multiples organisations qui coopèrent pour gérer cette zone racine. Donc l'ICANN se charge des questions opérationnelles, de la KSK de racine, et VeriSign se charge de la [ZSK] de racine. La zone de racine KSK est uniquement utilisée une fois par trimestre, parce qu'elle change, et lorsqu'elle change, il faut qu'elle soit resignée par la KSK de racine. Donc une fois par trimestre, la KSK est utilisée pour cette signature. Donc ces activités fonctionnent séparément, mais en fait elles sont coordonnées. L'ICANN et VeriSign travaillent en étroite collaboration pour gérer tout ceci dans la zone racine.

Alors la KSK racine a été créée en 2010 lorsque la zone racine a été signée pour la première fois. Il y a des [inaudible] matériels de sécurité qui ont été mis en place, et il y a deux lieux de gestion de clé où sont rangées les KSK avec une excellente protection par rapport à l'accès. Et on pourrait parler de ceci, de la manière dont fonctionne la KSK de zone racine, mais ce qu'il faut retenir, c'est donc qu'elle est très bien protégée.

Alors il y a différentes manières d'atteindre la KSK de racine. On peut le faire grâce à une requête DNS, mais en fait ce serait une demande qui ne serait pas protégée.

Comme c'est le début, il est difficile d'utiliser une autre clé pour la valider. Vous pouvez obtenir cette KSK de zone racine sur le site de

l'IANA. Je peux utiliser un certificat x.509 et je peux donc obtenir l'ancre de confiance de la clé de zone racine. Il y a un certificat qui existe donc c'est une des manières que l'on peut utiliser pour arriver à la KSK. Autre possibilité, faire confiance aux informations que l'on reçoit lorsqu'on installe un logiciel de validation de DNSSEC. Je l'ai déjà dit tout à l'heure.

Donc il est prévu de changer la KSK de zone racine, et ça, c'est important, parce qu'en fait c'est la première fois que nous effectuons un tel changement. Nous avons utilisé cette première KSK de zone racine qui a été créée en 2010, donc il y a 6 ans. Et le plan en fait va créer un précédent puisqu'il y a beaucoup de parties qui pourraient être impactées, puisqu'il faudra changer cette clé pour tout le monde.

Alors il est tout à fait possible qu'un processus soit mis en place pour qu'un changement automatique de la clé soit effectif, mais ce qui est important, si on s'occupe de logiciel de validation de DNSSEC, c'est qu'il faut s'assurer que même si le changement est automatique, en fait, il faudra quand même s'assurer que le changement est effectif.

Et il est impossible de savoir le nombre de personnes qui s'occupent de la validation DNSSEC. Il n'y a pas de liste qui existe. Donc l'une des choses que cherche à faire l'ICANN, c'est de communiquer le message par rapport à ce que nous faisons maintenant, d'informer la communauté par rapport à ce qui se passe et par rapport au point où nous en sommes.

Les gens demandent souvent pourquoi est-ce que vous changez la clé puisqu'il n'y a pas d'amélioration si elle va changer, et il n'y a pas de problèmes. Et c'est vrai. Il n'y a pas de problèmes. Il n'y a pas de faiblesses, de lacunes. Mais je pense que c'est en fait une question

d'hygiène cryptographique de changer cette clé, donc on ne peut pas la garder pour toujours. C'est un peu comme votre département des TI qui vous demande de changer votre mot de passe de temps à autre.

Il faut qu'il y ait un plan parce que de changer cette clé pendant des circonstances normales, parce qu'il ne faudra pas se trouver dans une situation où on est obligé de changer cette clé, et de le faire de manière soudaine et imprévue sans nous être exercés à le faire. Donc il nous faut avoir un plan déjà en place au cas où. Alors, pourquoi ne pas faire un [inaudible] ? Eh bien, cela a un impact sur toutes les personnes qui font de la validation sur Internet, donc on ne va pas faire ça de manière privée.

Alors je mentionnais le nombre de personnes qui vont être impactées. Si quelqu'un n'obtient pas le message, et si quelqu'un ne met pas à jour son logiciel avec la nouvelle clé, Eh bien son logiciel va penser que toutes les réponses reçues sont mauvaises ou représentent une attaque puisqu'aucune des signatures ne sera validée, il n'y aura pas en fait de chaine de confiance parce qu'il n'y aura pas un bon point de départ. Et donc cela voudra dire que toutes les résolutions de DNS vont arriver à un échec.

Alors maintenant je vais parler du projet en ligne. Ça, c'est intéressant si vous êtes quelqu'un qui effectue des évaluations de DNSSEC. [Jess Houston] qui fait des recherches à [APNIC] a justement étudié la question et publié des statistiques comme quoi 15 % du trafic DNS dans le monde entier utilisaient la validation. Alors je dois mentionner que la signature de DNSSEC n'est pas affectée, mais en fait il y a deux grandes parties dans le DNSSEC. Il y a la partie signature, les informations DNS

sont publiées sur des serveurs, et le DNSSEC doit être signé. Et lorsque l'on recherche des informations DNSSEC sur un serveur, il faut qu'elles soient revalidées, et nous parlons uniquement de la deuxième portion de validation. Donc la signature de DNSSEC n'est pas affectée par ceci. Il y a uniquement la validation des informations qui donc est affectée.

Donc si vous vous occupez de validation de DNSSEC, vous devez revoir les configurations et les processus. Étant donné que nous n'avons jamais fait ceci auparavant, il est important d'informer tout le monde.

Alors, pour vous donner un petit peu un historique, l'ICANN a organisé un panel d'experts de la communauté avec le personnel de l'ICANN pour organiser le travail. Il y a eu un rapport qui a été publié en mars 2016 et ensuite le personnel s'est occupé de mettre au point des plans suite aux recommandations qui ont été faites. Et pour des raisons de transparence, fin juillet, nous avons essayé tous les plans sur l'URL que vous voyez affichée sur la diapo de liaison des cinq plans qui existent. Et nous encourageons toutes les personnes qui sont intéressées par le sujet à consulter les plans. Les plans sont extrêmement détaillés, et il y a beaucoup plus de choses sans doute qui peuvent intéresser.

Alors ceci représente donc [inaudible] la plus importante puisque parle ici du rôle même de la nouvelle KSK, du moment où on passera de l'ancienne nouvelle, et on est prévue pour le 11 octobre 2016 — Pardon 2017. Donc bien sûr que c'est dans un an, ce n'est pas aujourd'hui, mais étant donné l'importance de ce projet, étant donné le nombre de personnes qui vont être affectées, nous commençons de manière précoce à communiquer là-dessus pour que les gens soient informés.

Je ne vais pas entrer dans le détail des plans en eux-mêmes et de ce qui va se passer, mais nous travaillons lentement. Nous n'avons pas de cérémonie de clé de signature de clé. Et nous faisons tout notre possible lors de cette — des cérémonies trimestrielles. Nous avons donc décidé de ne pas nous presser, de prendre nos précautions, pour effectuer le travail. Donc il n'y aura pas de changement des paramètres, des paramètres cryptographiques. Nous changerons la clé de manière à ce qu'il y ait des mises à jour de protocole défini dans RFC 5011, c'est le mécanisme automatique dont je parlais tout à l'heure, donc de mise à jour des ancres de confiance. Alors voilà comment ça fonctionne.

Lorsque vous publiez une ancre de confiance, vous avez donc lancé une ancre de confiance qui signe la nouvelle ancre de confiance. Et donc, il y a un validateur qui veillera à ce que l'ordre de confiance à laquelle on fait confiance signe une nouvelle ancre de confiance qui n'a jamais été connue. Et au bout de 30 jours d'observation de ceci, le validateur se dira la nouvelle ancre de confiance est légitime ; et donc, il va faire confiance à cette nouvelle ancre de confiance. Donc là, c'est la bonne nouvelle de ce projet. C'est-à-dire que tout validateur de DNSSEC qui suit ce protocole, ce protocole de mise à jour automatique, ce validateur automatiquement va mettre à jour les informations avec la nouvelle ancre de confiance. Cet antre de confiance sera signé et au bout de 30 jours, le validateur se rendra compte que cette nouvelle ancre de confiance est légitime et il va donc configurer ceci.

Nous pensons que pour beaucoup, en fait, il n'y aura rien à faire parce que l'ancre de confiance sera mise à jour de manière automatique. Et comme je le disais, nous intégrons aussi dans les évènements normaux que nous avons actuellement. Elle inclut également beaucoup de textes,

beaucoup de vérification de manière que le processus soit vérifié au fil du temps, au fur et à mesure, et de manière à bien mesurer l'impact de ce que nous faisons.

Alors, il existe quand même une préoccupation ; c'est la taille des réponses. Il y a une réponse. Donc par rapport à toutes les clés de DNS, toutes les clés de la zone racine en elle-même, cette réponse est en fait assez importante, 1425 octets pendant le projet. Et ça, ça représente un maximum du point de vue historique. Il n'y a jamais eu une réponse de la zone racine qui a jamais été aussi importante.

Et donc, lors de certaines expériences, surtout avec l'IPv6, il semblerait qu'il pourrait y avoir un problème. Donc les expériences suggèrent une chose, après, dans la pratique, du point de vue opérationnel, du point de vue d'autres personnes qui travaillent sur le DNSSEC, il semblerait qu'il n'y ait pas de problèmes.

Alors ce n'est pas très clair, mais pour des raisons de prudence, nous allons bien surveiller tout ceci quand même. Donc les questions concernant la fragmentation d'IPv6 ont une taille maximale de support IPv6 est de 1285, c'est-à-dire qu'il est possible que quelqu'un ne peut pas recevoir une réponse plus grande que cela de la zone racine pour vérifier l'identité. Dans ce cas-là, les paquets doivent être divisés en fragments, et il est possible que différentes parties n'arrivent pas à la personne à laquelle ils étaient destinés, donc il y aura un problème au niveau de la vérification.

Si vous êtes intéressés par cela, je pourrais partager davantage de détails avec vous. À titre personnel, je dirais que cela ne me préoccupe pas beaucoup. Il y a d'autres zones qui utilisent le DNSSEC avec des

réponses générées lorsque les paquets sont plus grands que la taille de réponse admissible par la zone racine. Cela ne pose aucun problème opérationnel, et comme je disais c'est utilisé dans le cas où on sait que les fragments d'IPv6, les utilisateurs d'IPv6 vont être utilisés. Des fois, il y a ces parties qui n'arrivent pas à leur destination, et nous savons qu'il est possible de surmonter cette difficulté parce qu'il est possible de suggérer que cela ne pose pas de problème, que cela ne s'arrêterait pas.

Donc vous voyez ici ces tailles qui augmentent, et cela vous montre l'importance de la date 11 octobre 2017 et c'est la date à laquelle tout cela sera fait.

Donc la résolution du DNSSEC cessera de fonctionner à partir de cette date-là si vous n'avez pas la résolution appropriée. En tant qu'opérateur, il est important de savoir comment configurer ces ancres de confiance. Donc pour mettre à jour ces ancres de confiance, comment le faire dans le logiciel ? Eh bien ça peut être fait manuellement, ou à travers un logiciel de configuration. Peut-être que cela pourrait être intégré au logiciel qui est fourni par le développeur du logiciel ou il pourrait bien sûr y avoir également une organisation ou une société qui distribue un logiciel qui fait cela. Et il faut vérifier que quelqu'un fasse ce suivi, autrement il pourrait y avoir une manière de le faire sans même devoir s'en occuper. Mais il est important de toute façon de savoir comment mettre à jour le DNSSEC.

Comme je disais, si vous utilisez le protocole de mise à jour automatisé, ça va se faire tout seul. Je ne parlerai pas de la gestion des ancres de confiance négatifs. Nous travaillons avec les développeurs et les distributeurs d'outils et de logiciels de DNS parce que nous

reconnaissons qu'un nombre des sociétés qui développent ces logiciels et ces outils intègre déjà l'ancre de confiance à leurs logiciels. Donc par exemple, certains intègrent l'ancre de confiance au logiciel lui-même, où ils l'incluent dans les fichiers de configuration modèles. Et les personnes qui utilisent le logiciel tel que les personnes qui assurent la distribution du logiciel de DNSSEC sont des organisations qui pourraient bénéficier de ce logiciel. Donc nous travaillons déjà avec ces sociétés pour leur faire savoir que l'ancre de confiance va changer pour qu'elles mettent à jour les logiciels et qu'elles envoient ce paquet de mises à jour aux utilisateurs.

Donc voilà déjà une partie des mesures qu'il est possible de mettre en œuvre pour mettre à jour le logiciel, mettre à jour l'ancre, leur demander de mettre à jour le logiciel. Nous travaillons également avec les développeurs de code qui met en place des essais pour assurer que les protocoles soient mis à jour automatiquement. Et nous travaillons également sur le développement d'un modèle d'essai pour les opérateurs eux-mêmes qui leur permettra de savoir si la version qui est installée, qui est donc en fonctionnement, peut gérer correctement ce protocole de confiance.

Voilà la fin de présentation. Vous avez ici des liens qui vous permettront d'accéder à davantage d'informations. Il y a beaucoup d'informations également sur le site Web de l'ICANN. Il existe également une liste des allusions que vous pouvez rejoindre si cela vous intéresse.

Et cela dit, je serais prêt à répondre à vos questions.

TIJANI BEN JEMAA : Merci, Matt, de cette présentation. Bon je pense que c'est un est assez difficile, assez technique. C'est important, mais il est important de mettre à jour ces ancres de confiance et que tout le monde sache que cela sera fait. C'est important pour l'ensemble du système.

Donc, y a-t-il des questions ?

MATT LARSON : Je vois une question dans la salle de chat. Il demande quelle est la taille des clés de signature de clé. Cela ne va pas changer. L'ancre de confiance actuelle est de 48 bytes, comme le sera la prochaine ancre.

TIJANI BEN JEMAA : Merci. D'autres questions ? Si vous n'êtes pas sur Adobe Connect, vous pouvez également demander la parole.

HEIDI ULLRICH : Tijani, c'est Heidi au micro. Je vois Olivier qui lève la main, mais Tijani, je vais vous demander de parler plus fort ; on ne vous entend pas bien. C'est très difficile de vous entendre. Merci.

TIJANI BEN JEMAA : Très bien. Merci Heidi. Olivier, allez-y.

OLIVIER CRÉPIN-LEBLOND : Merci, Tijani. Merci beaucoup de ces informations, de cette présentation. C'est très utile de voir une partie du travail qui n'est pas

visible au niveau de la sécurité. Et il est bien de voir que vous continuez de travailler pour stabiliser le système davantage.

On parle vite de clé, de mise en place des nouvelles clés ; serait-il possible que cela ne fonctionne pas, ou qu'il y ait des problèmes à résoudre dans le processus de roulement de la clé, et quelles seraient les solutions dans ce cas-là ?

MATT LARSON : Bonne question, Olivier. Merci.

Nous sommes en train d'adopter des propositions, d'une part à travers la mise en place de dispositions qui nous permettent d'invertir les modifications et de voir avec un trimestre d'avance quelles sont les modifications nécessaires. Donc puisqu'on travaille à l'avance, au cours du processus nous créons différentes versions. À chaque fois que l'on importe des changements, donc s'il est nécessaire de revenir en arrière, à la version précédente de la clé, on pourrait le faire.

On espère que ce ne sera pas nécessaire, mais si besoin, on pourra le faire.

Donc vous demandez qu'est-ce qui pourrait échouer. Ce qui nous inquiète le plus est la possibilité d'avoir une personne qui ne reçoit pas le message et qui par conséquent ne met pas à jour ces validateurs. La résolution du DNS ne fonctionnerait donc pas, comme j'ai dit tout à l'heure.

Mais ce qui est bien est qu'il est tout simple de résoudre cela. La personne n'a qu'à mettre à jour son ancre de confiance. Donc pour un

fournisseur de services Internet, par exemple, ça pourrait être utile en tant que solution lorsqu'un client appelle pour dire que sa clé de validation ne fonctionne plus.

Bien sûr pour mettre à jour le DNS, il est très facile de faire cela. Et on prévoit déjà la situation à laquelle, par exemple, il pourrait y avoir un fournisseur de logiciel qui n'a pas mis à jour son logiciel. Mais cela ne devrait pas avoir lieu. Si vous commencez à travailler dès aujourd'hui, vous devriez avoir une version mise à jour de l'ancre aussitôt qu'elle devient disponible.

Donc la solution la plus simple est de mettre à jour l'ancre de confiance. Ce qui nous inquiète, en tout cas, est la possibilité qu'il y a des utilisateurs qui n'utilisent pas le protocole automatisé d'ancre de confiance, et qui par conséquent, ne mettent pas à jour automatiquement leurs définitions, et qui ne le font pas manuellement. Là, il pourrait y avoir un problème, mais c'est facile à résoudre.

D'autre part, les fournisseurs de services Internet ou fournisseurs de logiciel principaux qui gèrent la plupart du trafic de DNS assurent la validation du DNS. Mais nous savons qu'ils connaissent bien cette modification, qu'ils sont au courant, donc on ne devrait pas avoir un problème à ce niveau-là.

Aux États-Unis, les fournisseurs de services Internet valident le DNSSEC pour leurs consommateurs, et ils savent bien que cela aura lieu. Donc les principales sociétés qui devraient s'occuper de mettre à jour leur système de validation sont celles qui fournissent ces services pour les clients. Et ils sont des partenaires, des membres des groupes de travail.

Donc en termes généraux, on pense que ce n'est que les petits utilisateurs, ou les opérateurs qui n'ont pas tellement de clients qui mettent à jour manuellement leurs définitions qui pourraient avoir des problèmes.

Donc les principaux fournisseurs de services Internet qui poseraient le plus de risques pour les utilisateurs ne devraient pas avoir de problèmes en ce sens.

TIJANI BEN JEMAA : Merci, Matt. Y a-t-il d'autres questions ?

Bien sûr, tout le monde sait que bien — si on ne changeait pas ces clés, on pourrait avoir — même si on ne les changeait pas, on n'aurait pas de sécurité. Ces clés sont utilisées depuis très longtemps donc il faut les mettre à jour. Cet ensemble de clés a été utilisé depuis six ans, et les personnes savent qu'il est nécessaire de les mettre à jour pour assurer la sécurité du système.

Olivier, est-ce que vous levez la main ?

OLIVIER CRÉPIN-LEBLOND : Oui, Tijani, merci. J'ai une autre question sur ce sujet. Merci.

Oui. Il y a de grandes organisations qui devront s'occuper de cela, qui fournissent ce service pour leurs consommateurs, et vous dites qu'il y a également de grandes organisations qui assurent cela pour leurs clients.

Est-ce que vous avez d'autres informations concernant les types de présentations ou les mesures qu'il faudrait prendre ? Quel devrait être

— je ne demande pas un document de questions fréquentes, mais je voudrais savoir si vous avez un document qui soit une liste de vérification de ce qu'il faut absolument faire, qui pourraient être utile pour les opérateurs qui ne sont pas à 100 % au courant de cette initiative.

On sait que le DNSSEC d'habitude est mieux compris parmi les personnes qui gèrent des domaines et qui les mettent en œuvre, mais bien sûr les connaissances des utilisateurs ont des limites. Donc est-ce que vous prévoyez d'avoir un document de ce type ? Sachant bien sûr que cette modification est substantielle.

MATT LARSON : C'est une bonne question. Nous comptons préparer des ressources qui expliquent comment configurer les ancres de confiance dans les différents systèmes.

C'est dans les serveurs de noms en général que la validation est faite le plus. Donc c'est sur les problèmes qui pourraient être expérimentés à ce niveau-là qu'on travaillera pour aider les personnes à comprendre comment modifier leur ancre de confiance, ou encore mieux, pour leur expliquer comment mettre en place une automatisation de la mise à jour de cette ancre de confiance, pour qu'elle sache comment être toujours à niveau.

OLIVIER CRÉPIN LEBLOND : J'ai une autre question, si vous permettez. La question suivante pour moi est quel serait l'impact de tout cela sur les TLDs et les zones de clés qui ne sont pas signés.

MATT LARSON : L'impact que ça a sur eux correspond au fait que la zone racine est signée, et que la zone racine comprend par conséquent des signatures. Donc vraiment, ça pourrait avoir un impact sur tout le monde.

TIJANI BEN JEMAA : Merci Matt. Yeşim, vous levez la main ?

YESIM NAZLAR : Merci, Tijani. Nous avons reçu une question dans la partie de Q&A, est-ce que je pourrais la lire ? Je suis Afifa du Bangladesh. Je pense qu'il y a des personnes qui ne connaissent pas bien cette modification. Est-ce que vous prévoyez d'avoir des moyens de communiquer tout cela dans les régions les plus éloignées ?

MATT LARSON : Oui, bien sûr. Nous essayons de voyager partout dans le monde, par différentes versions de cette présentation pour rejoindre la communauté des opérateurs de partout dans le monde. Par exemple, un collègue le présentera à l'ile Maurice au sein d'AfriNIC d'ici quelques semaines. Ça a récemment été présenté auprès d'APNIC. Donc tous les opérateurs de partout dans le monde devraient être au courant de ces modifications.

On s'attendait à ce que cette étape, bien sûr, soit très compliquée, que ce soit une période chargée de travail. Mais c'est normal, en raison de la taille de cette modification.

TIJANI BEN JEMAA : Merci, Matt. Y a-t-il d'autres questions ? S'il n'y a plus d'autres questions, je devrais peut-être donner la parole à Yeşim qui va nous poser certaines questions. On va faire le test.

YESIM NAZLAR : Merci, Tijani. Nous n'avons qu'une question dans cette partie. Je vais vous la lire.

Quelle est la date réelle du roulement de la clé de signature de clé de la racine ? Est-ce le 11 octobre 2017, le 1er janvier 2017, le 11 janvier 2000 17 aout le 11 octobre 2018 ? Je vous prie de voter.

MATT LARSON : La réponse correcte, le 11 octobre 2017.

YESIM NAZLAR : Merci. Voilà la fin de ce questionnaire. Tijani, je vous redonne la parole

TIJANI BEN JEMAA : Merci, Yeşim. Y a-t-il d'autres questions pour Matt ?

HEIDI ULLRICH : Tijani, on avait une question de Glenn sur le chat.

TIJANI BEN JEMAA : Allez-y. Oui. Lisez-la, s'il vous plait.

HEIDI ULLRICH : Très bien. « Sur la question de l'IPv6, on a vu une mise en place qui n'était pas pareille partout dans le cas des différents opérateurs. Est-ce que vous prévoyez d'être plus diligents cette fois-ci » ?

MATT LARSON : J'espère que oui. Nous allons faire de notre mieux pour nous assurer que tout le monde met en place ces modifications. Je dirais que la différence entre les exigences de l'IPv6 et ce cas-là est le fait que toute mesure prise pour la mise en œuvre de l'IPv6 ne devrait pas avoir eu d'impact nécessairement sur les utilisateurs, alors que le roulement de cette nouvelle clé de signature de clé aura un impact sur tous les utilisateurs. Ce ne sera pas nécessairement un impact immédiat le jour même de la mise en — du roulement de la clé, mais si quelqu'un veut faire cette validation, mais ne roule pas la clé, et n'a pas un système qui roule la clé en [sonnant] automatiquement, on va se rendre compte que quelque chose ne fonctionne pas. On va devoir prendre des mesures pour corriger cela. Mais comme je disais tout à l'heure, c'est tout simple de le faire.

TIJANI BEN JEMAA : Merci, Matt. Y a-t-il d'autres questions ? Oui. Olivier, allez-y s'il vous plait.

OLIVIER CRÉPIN LEBLOND : Merci, Tijani. J'ai une autre question et je voudrais savoir pourquoi il faut faire augmenter la taille de la clé. Je ne sais pas très bien si Matt a

expliqué pourquoi il était nécessaire. Peut-être que ce prolongement n'est pas nécessaire, qu'on pourrait avoir le même type de clé à partir de ce nouveau roulement, n'est-ce pas ?

MATT LARSON : Non. Ce n'est pas la taille qui va changer. Ce sont des clés de 2048 bytes aujourd'hui et demain. Mais ce qui pourrait être déroutant pour vous est de savoir qu'il y a eu une modification récente de VeriSign au niveau de la clé de signature de clé pour la zone racine qui en septembre est passée à 2048 bytes, et bien sûr, ça a provoqué des réponses plus prolongées de la zone racine et cela aurait eu des problèmes. Que l'on sache, ce n'était pas le cas. Mais à partir de maintenant, les KSK de la zone racine et la VSK sont toutes les deux de 2048 bytes et elles continueront à garder cette même taille.

OLIVIER CRÉPIN-LEBLOND : Oui, mais vous avez dit que la clé de signature de clé de la zone racine allait passer à une autre taille, à 2048, et qu'auparavant, c'était une clé de 1049 bytes. Et en 2015, elle était passée à 1055 pendant quelques jours.

MATT LARSON : Oui, oui. Je vois. Malheureusement, je n'ai pas inclus des informations dans cette présentation. Ce serait plus facile de l'expliquer si on avait ces informations à la main, mais ici on parle de la taille des réponses lorsqu'il y a des requêtes de la zone racine au niveau des clés [ZSK]. Une fois qu'il y a une ou deux [ZSK] suivant le moment spécifique en, parce que lorsque la [ZSK] sera roulée, il y aura deux c lés dans la zone racine.

C'est pourquoi lorsqu'on roulera la [KSK], il y aura également deux clés qui vont coexister dans la zone racine. Donc normalement, on a une [ZSK] et une [KSK], mais il y aura un moment au cours de ce processus auquel il y aura deux [ZSK] et deux [KSK]. À ce moment-là, la taille des réponses sera de 1425 bytes. Mais ça n'a rien à voir avec les chaines cryptographiques de la clé elle-même qui est de 2048 bytes.

OLIVIER CRÉPIN-LEBLOND : Très bien. Je comprends maintenant. Alors est-ce que vous avez déjà fait des essais sur ce réseau avec les différents cas, ou est-ce la première fois que vous allez avoir ce type de scénario ?

MATT LARSON : Non. Ce n'est pas la première fois. Et dans des conditions normales, tout opérateur devrait pouvoir gérer les réponses du serveur de nom, et pouvoir traiter toutes ces tailles qui seraient reçues par le système.

L'inquiétude principale à ce moment-là serait de savoir — c'est le cas auquel un paquet serait plus grand, trop grand, il se pourrait qu'il y ait des problèmes au niveau de la réception. Mais ça va varier bien sûr. Et la bonne nouvelle, comme je disais, est que nous avons fait augmenter la taille de la chaine cryptographique récemment, et donc la taille de la clé [ZSK] devrait avoir la même taille de réponse que la clé de la racine, la clé KSK.

Il y a d'autres TLDs qui valident le DNSSEC d'une manière telle qu'ils envoient des réponses de plus de 1045 habituellement, par exemple le .org.

Le .org habituellement à des paquets de plus grandes tailles, et il n'y a jamais aucun problème. La taille des réponses de la clé [ZSK] est encore plus grande dans certains cas et tout le monde arrive à traiter ces réponses. On ne connait pas de problème en vertu de la taille de ces réponses. Je sens que le type de problèmes que l'on pourrait avoir serait lié à la mise à jour, et passe à la taille des réponses.

TIJANI BEN JEMAA : Merci, Matt. Olivier, vous levez toujours la main ? Non. Plus d'autres questions ? Merci. Merci, Olivier, et merci beaucoup Matt Larson, notre présentateur, qui est le président de recherche du bureau de CTO de l'ICANN qui nous a donné une présentation magnifique.

C'est une question, un sujet, compliqué, un peu technique, mais il faut que l'on comprenne qu'au moment où cette modification sera mise en œuvre, il aura des personnes qui pourraient être affectées par l'utilisation de l'ancien DNSSEC. C'est pourquoi il est important de savoir quelle sera la modification.

Cette présentation a été donc nécessaire pour At-Large et pour les utilisateurs finaux.

Matt Larson, encore une fois merci. J'espère qu'on aura une nouvelle mise à jour une fois que le roulement de la clé de signature de clé aura été fait. On espère avoir des mises à jour à chaque étape. Matt, je vous remercie encore de cette présentation.

Je voudrais également remercier l'équipe technique, le personnel de l'ICANN, et je vous remercie tous d'avoir participé à cette téléconférence. Merci. Ce séminaire Web est maintenant fini.

YESIM NESLAR : Cette réunion est maintenant finie, et la connexion audio sera terminée. Merci d'avoir participé. Ayez une bonne fin de journée. Au revoir.

**[FIN DE LA TRANSCRIPTION]**