MONTREAL – Atelier sur les DNSSEC (1 sur 2)
Mercredi 6 novembre 2019 – 13h30 à 15h00 EDT
ICANN66 | Montréal, Canada

DAN YORK : Bonjour à tous. Bienvenue à l'atelier DNSSEC. Dave, vous voulez commencer ? Non, très bien. Donc tout devrait être prêt pour commencer. Merci d'avoir préparé les diapositives. Notre séance devait commencer à 13:30. On a pris un petit peu de retard. Je pense qu'on est prêts à pour commencer ?

ORATEUR NON-IDENTIFIÉ : Quantum Computers va arranger tout cela.

DAN YORK : Seulement si on inclut le blockchain. Très bien. Sommes-nous prêts ? Très bien.

On est ici pour parler du DNSSEC. Si vous n'êtes pas là pour parler du DNSSEC ou RPKI, etc. vous êtes dans la mauvaise salle et vous devez fuir rapidement. Très bien.

Qu'est-ce qu'on peut dire d'autre ? Si quelqu'un veut passer devant, très bien.

Voilà l'atelier DNSSEC mais vous allez voir que nous avons étendu un petit peu les sujets à aborder pour parler de sécurité. Nous allons

aborder la question de la sécurité et d'autres problématiques également.

Vous voyez sur l'écran certaines des personnes qui vont parler. Vous pouvez lever la main ? Jacques, Andrew, Andrei, très bien. Voilà les personnes qui vont travailler avec nous. Nous avons des appels hebdomadaires pour pouvoir coordonner ce type d'atelier DNSSEC. Nous faisons cela deux à trois fois par an, parfois nous ne le faisons pas dans le forum de politique parce que parfois, il n'y a pas suffisamment de public. Et c'est nous que vous devez remercier ou rendre coupable des sujets que nous allons aborder aujourd'hui.

WARREN KUMARI : BGP.

DAN YORK : Excusez-moi, c'était une blague interne. Très bien.

Quelqu'un d'autre ? Jacques, est-ce que vous avez des recommandations à nous donner ?

JACQUES LATOUR : Vous pouvez vous enregistrer pour manger différents types de poutines pour manger.

DAN YORK : Et vous devrez aller chez le docteur le lendemain pour évaluer le taux de cholestérol. Est-ce que quelqu'un a goûté à la poutine ici à Montréal ? Très bien, vous êtes nombreux.

ORATEUR NON-IDENTIFIÉ : Et il y aura un quizz sur la poutine.

DAN YORK : En 2000, je n'avais jamais entendu parlé de la poutine quand je suis venu au Canada, j'étais à Ottawa. Très bien. Nous ne mangeons pas de poutine aux États-Unis même si on commence petit à petit à trouver des restaurants qui en font. En général, ce sont des *foodtruck*.

Je pense que ce n'était pas le sujet de notre atelier. Voilà, on est un petit peu en dehors du programme. Nous voilà.

Nous voulons remercier les personnes ou les compagnies qui figurent sur l'écran. Les compagnies que vous voyez sur l'écran ont parrainé ou parrainent ce type d'évènement de manière annuelle. Cette fois-ci, il n'y a pas eu de déjeuner parce que notre atelier a lieu après le déjeuner mais en général, ce sont des sponsors qui nous aident aussi pour le déjeuner.

Aujourd'hui à 19:00 à l'hôtel Intercontinental, il y aura une soirée sponsorisée par les personnes que vous voyez sur l'écran. Ce sera une soirée où on pourra boire un verre, etc. Si vous voulez y aller, il faut que vous contactiez Kathy. Elle vous donnera un ticket qui vous permettra de venir à cette soirée. N'hésitez pas à contacter Kathy pour

cela. Merci à tous les sponsors qui nous permettent d'avoir ces ateliers et le faire avec l'estomac plein.

Cet atelier est parrainé par le comité consultatif sur la sécurité et la stabilité. Excusez-moi, je n'ai pas besoin de ce micro. Très bien.

Si vous regardez le programme, tout d'abord, on va parler des indicateurs par rapport au DNSSEC, Daniel Migault va nous parler un petit peu d'un projet de meilleures pratiques pour la validation pour les résolveurs de validation DNSSEC. Russ Mundy va nous faire une introduction sur le RPKI. Combien de personnes ont entendu parler du RPKI ? Très bien. Nous allons parler de cela. Ensuite Kim Davies, il est ici ? Pas encore ? Il viendra nous parler du prochain roulement de la signature de clé. Ensuite, Yoshiro, où êtes-vous ? Yoshiro va nous parler des recherches qui ont été faites. Ensuite, on aura la pause-café et on aura Jaap qui va nous parler de la sécurité. Moi, je vais parler de l'observatoire MANRS. Et ensuite, Mark, est-ce qu'il est là ? Il n'est pas là encore. Ils vont parler du travail qu'ils ont fait sur l'utilisation malveillante du domaine .eu. Voilà le programme et nous allons attaquer directement le premier point.

Dans cet atelier, nous voyons en général les statistiques par rapport à l'utilisation DNSSEC. Et nous voyons qu'il y a une augmentation assez intéressante dans la croissance de la validation du DNSSEC. Vous voyez la signature DNSSEC avec le travail qui est fait par le laboratoire APNIC. Et vous voyez les graphiques qu'ils ont, des statistiques très intéressantes. Vous pouvez voir en détail quelles sont les situations des différentes régions du monde. Ici dans ces graphiques, on voit

quelles sont les parties du monde qui font la plus grande partie de la validation DNSSEC.

Sur la deuxième colonne, vous avez le pourcentage d'utilisation du DNS public de Google. Nous savons que l'utilisation de ce PDNS pour nous donner des informations par rapport à l'utilisation DNSSEC également. Donc le DNS de Google nous montre qu'il y a une utilisation assez importante dans certains pays.

WARREN KUMARI : Geoff a une autre page qui montre...

DAN YORK : Pour le prochain atelier et je regarde Andrew, nous allons voir quel est le lien entre ces éléments. Mais ce qui est intéressant quand on regarde les pays comme la Micronésie en Océanie, on voit un grand pourcentage des requêtes qui viennent valider et un pourcentage important des gens qui utilisent le DNS public de Google, ce qui veut dire qu'il y a là une configuration des systèmes qui pointent vers ce DNS, et cela dans plusieurs endroits du monde.

Ici, vous voyez des statistiques. Wes, où es tu ? Si vous n'avez pas encore vu la page de statistiques améliorées, Wes a réuni des statistiques qui sont très intéressantes. Ici, vous voyez la croissance générale des enregistrements DS. Vous voyez une croissance assez importante dans le nombre général de signatures qui ont lieu par rapport à cet enregistrement. Je ne fais que présenter ces statistiques mais elles figurent dans la page de statistiques.

Victor, merci d'avoir collecté ces statistiques et merci Wes de les avoir présentées sur la page.

Ici, si vous voyez le travail de Viktor, si vous le suivez par courriel, etc., vous verrez qu'il y a beaucoup de domaines qui ont des enregistrements MX et DANE et qui commencent à augmenter de manière significative. On voit que les gens commencent à déployer les enregistrements DANE dans leurs domaines.

RPKI, on va parler de la RPKI. Vous voyez des statistiques qui viennent montrer une croissance dans l'utilisation de la RPKI. Vous voyez une croissance, des bons résultats. Ici, vous voyez les préfixes IPv4 qui sont couverts et je pense que c'est tout pour le moment.

Nous avons vu de nouveaux déploiements DNSSEC de ccTLD. C'est un changement, il y en a de nouveaux qui viennent s'ajouter. Et la liste, vous la voyez sur l'écran.

Ici, vous voyez l'état de situation par rapport au DNSSEC ccTLD. On voit des parties de l'Amérique du Nord. On doit travailler sur ces statistiques.

Nous avons également un certain nombre de ressources qui sont disponibles, des ressources DNSSEC. Il y a le déploiement 360 degrés de l'Internet Society, le DNSSEC-Tools, etc.

Ces diapositives sont disponibles sur la page du site web de l'ICANN66.

Je vais dire merci. Nous pouvons passer au premier intervenant. Donc je vais passer la parole à Daniel.

DANIEL MIGAULT : Je suis prêt.

Aujourd'hui, je vais vous parler des recommandations pour les opérateurs de résolveur DNSSEC. C'est un travail qui est toujours en cours que nous faisons à l'IETF. Nous espérons pouvoir publier un projet de rapport bientôt. Et si vous voulez nous contacter, n'hésitez pas à le faire sur notre liste de diffusion.

Tout le monde connaît l'IETF. Qui ne connaît pas l'IETF ? Très bien. Alors je vais vous l'expliquer.

L'intention de ce projet est de fournir des meilleures pratiques pour les FAI pour qu'ils puissent mettre en place le DNSSEC ; voilà un petit peu la motivation générale.

Kathy, je pense... Ah non, c'est moi-même qui gère les diapositives, excusez-moi. J'allais te dire : « Kathy, tu vas trop vite. »

Alors, le DNSSEC, je pense que tout le monde connaît le DNSSEC mais l'idée, c'est de dire que la confiance DNSSEC repose sur la validation de signature. La signature est un *binding* entre la clé et la signature qui dans le monde DNSSEC veut dire qu'il y a une clé DNSSEC et un ensemble RRSIG. Mais c'est la moitié du problème parce que la validation ne sert à rien à moins qu'on ait une ancre de confiance. Donc il faut avoir cette confiance pour pouvoir générer la signature.

Comment pouvons-nous faire le *binding* de la clé ? Nous utilisons une ancre de confiance qui est aussi une clé DNSKEY. Nous avons une

chaîne de confiance et pour chaque DNSKEY, il y a une validation. Donc chaque niveau de DNSKEY peut changer au fil du temps. Donc une des inquiétudes les plus importantes, c'est comment préserver cette confiance.

Que devrait faire un opérateur de validateur DNSSEC ? Le risque d'avoir une clé malveillante qui soit introduite dans le système, dans ce cas-là, la validation donnera un résultat d'échec pour des raisons inattendues. Toutes ces recommandations sont adressées aux opérateurs pour éviter ce type de risque. Ces recommandations concernent l'approvisionnement, le suivi et la gestion.

Qu'est-ce que c'est qu'un validateur DNSSEC ? On a un moteur de validation qui repose sur des librairies et sur le temps. Donc les messages qui entrent sont validés et ajoutés dans le cache ou bien refusés ou rejetés du cache. Et on a également une configuration où il y a une ancre de confiance. Et ces ancres de confiance peuvent évoluer au fil du temps et on doit les mettre à jour.

Le but de cela est de minimiser l'intervention de ces opérateurs. Nous ne voulons pas devoir instrumentaliser le résolveur. L'idée, c'est de ne pas y toucher. Voilà ce que nous voulons faire dans la mesure du possible, ne pas y toucher. Si vous ne comprenez pas, c'est bon, mais il ne faut pas y toucher surtout.

Ensuite, nous ne voulons pas que les opérateurs aient peur du DNSSEC parce qu'ils ne sont pas des experts ou qu'ils pensent que cela va représenter des coûts supplémentaires. Nous voulons dire si vous menez à bien ces opérations, si quelque chose ne se passe pas bien,

vous n'êtes pas responsable de cela. Et les opérateurs DNSSEC ou les FAI ne doivent pas se sentir responsables de ce qui se passe sur internet.

Si vous voulez éviter les erreurs humaines, la meilleure manière est d'automatiser les opérations. Et pour cela, on se focalise sur la prévention, la configuration et l'identification en amont de tout le problème. Voilà ce que nous recommandons.

Les recommandations concernent trois catégories, dont la vérification de la santé au démarrage, c'est-à-dire vérifier que tout va bien et puis s'arrêter. Et ensuite quand les choses sont en bon fonctionnement, quand le résolveur fonctionne, vérifier régulièrement certains éléments. Et bien sûr, si vous voulez avoir un suivi plus détaillé, il faut avoir une méthode d'investigation. Je dirais qu'investigation, ce n'est peut-être pas le terme approprié. On devrait donc se pencher sur les problèmes en particulier pour comprendre ce qui se passe.

La première recommandation concerne l'écart de temps. Au démarrage, avant de commencer le résolveur, il est important de vérifier le temps de la machine qui héberge le résolveur et de vérifier combien représente l'écart de temps. Et il faudrait qu'il y ait un moyen de savoir quel est le temps prévu pour chaque résolveur. Ce n'est pas quelque chose qu'on doit faire en urgence. Voilà, c'est assez évident.

Ensuite pour les ancres de confiance, on a deux types d'ancres de confiance : il y a l'ancre de confiance positif, c'est une association entre une clé et un nom de domaine auquel l'opérateur fait confiance ; et on a des ancres de confiance négatives, ce sont des noms de

domaine que vous ne voulez pas voir réaliser la validation. Ensuite, les ancres de confiance positives et négatives sont hébergées dans ce qu'on appelle le stockage d'ancres de confiance. En général, quand on parle d'ancres de confiance, on parle d'ancres de confiance positives. Et quand on parle d'ancres de confiance négatives, on doit spécifier de quoi il s'agit.

Gestion des d'ancres de confiance. Vous vous souvenez, on avait dit que leur valeur pouvait changer au fil du temps. Au moment de la configuration, quand vous êtes en train d'approvisionner votre résolveur, il faut indiquer quelle est l'ancre de confiance à laquelle vous faites confiance et vous assurez que le résolveur commence avec cette ancre de confiance. Ensuite, pendant le fonctionnement, lorsque les ancres sont mises à jour, les résolveurs doivent prendre en compte ce changement ou cette mise à jour des ancres de confiance. Ensuite, en tant qu'opérateur, l'opérateur doit pouvoir savoir exactement quelles sont les ancres de confiance qui sont utilisées.

Configuration des ancres de confiance maintenant. Nous voulons éviter que le résolveur commence à fonctionner avec une configuration ancienne d'ancres de confiance, avec une DNSKEY ancienne. Donc les ancres de confiance positive et négatives peuvent être vues comme un processus à deux étapes. D'un côté, l'opérateur doit être capable de dire : « Voilà les ancres de confiance, voilà les noms de domaine auxquels on fait confiance, les noms de domaine qu'on considère comme étant les plus fiables et qui peuvent être considérés des ancres de confiance. » Ensuite, à partir de ce modèle

de confiance, vous devez pouvoir approvisionner les valeurs appropriées.

Donc ce n'est pas que vous avez une configuration et que vous dites : « Je fais confiance à cette clé. » Vous faites confiance à un domaine, un nom de domaine. Et donc la valeur appropriée, la valeur mise à jour doit être incluse dans cette configuration.

Le processus que nous envisageons, on définit le nom auquel vous ferez confiance et les noms par rapport auxquels vous ne voulez pas permettre la validation. Donc ce que vous faites, vous retirez les valeurs appropriées de ces noms de domaine et vous générez un fichier de configuration dans votre résolveur avec un langage générique. Et ensuite, vous mettez ces fichiers de configuration dans les différentes instances de votre résolveur. Le résolveur vérifie l'ancre de confiance puis il commence.

Deux notes par rapport à cela. Avec un processus de ce type, l'avantage, c'est que les opérateurs ne font que définir le modèle de confiance. Je fais confiance à ce nom de domaine et à partir de là, je vais dériver tous les autres.

Ensuite, un autre élément, c'est que comme à chaque fois que vous démarrez votre résolveur vous utilisez les ancres de confiance mises à jour, vous ne devez pas mettre à jour les fichiers de configuration de votre résolveur quand vous avez un changement de clé parce que tout est déjà mis à jour au niveau de votre mémoire. Donc quand vous redémarrez votre résolveur, vous aurez déjà des ancres de confiance

mises à jour et vous n'avez pas le problème des fichiers de système en lecture uniquement qui ne sont pas considérés dans la configuration.

La recommandation pour le démarrage est d'avoir des mécanismes d'avancement de l'ancre de confiance, de *bootstrapping*, pour vérifier automatiquement que vous avez les valeurs mises à jour. Et cette ancre de confiance doit être validée par le résolveur avant qu'il soit démarré, ce qui veut dire qu'on n'enverra pas d'avertissement si tout n'est pas prêt ; c'est cela, l'idée.

Quant à la mise en œuvre des recommandations, nous essayons ici de dissiper les préoccupations. Lorsque les gens voient toutes ces étapes, ils s'inquiètent peut-être. Or, lorsqu'un logiciel de validation du DNSSEC a une ancre de confiance intégrée, puisque ce logiciel pourrait l'avoir, cela veut dire que le modèle de confiance de l'opérateur va faire confiance à ce résolveur, à son fichier de configuration. Et le processus automatique va se faire à travers une mise à niveau du logiciel qui se fait périodiquement. Et ce logiciel, avant le démarrage, va faire une vérification. Ce faisant, on peut compléter toutes ces étapes très simplement.

Si l'opérateur est prêt à avoir une configuration plus complexe, par exemple si ce ccTLD ne fait pas confiance à la racine par exemple ou qu'il y a d'autres limitations, il va devoir mettre en œuvre de son côté d'autres mesures. Or, si la configuration est simple et il me semble que c'est le cas de la plupart des logiciels, vous n'avez qu'à avoir une version mise à jour du logiciel qui fonctionne.

Pendant à la mise à jour de l'ancre de confiance, pendant que le résolveur est en fonctionnement, étant donné que les ancres de confiance changent constamment, il faut pouvoir être en mesure de rouler ces valeurs pendant que vous êtes actif. L'opérateur devrait donc être en mesure de comparer périodiquement ces valeurs avec celles auxquelles il fait confiance de manière à vérifier que ce sont les plus récentes qui sont utilisées pour son ancre de confiance de manière à savoir quelles sont les clés auxquelles il devrait faire confiance. C'est quelque chose que l'on peut vérifier constamment.

Comme je le disais à l'instant, le seul point qui nous inquiète est le cache qui contient l'ancre de confiance. Si le roulement n'a pas été correctement suivi, cela peut être considéré comme un bug, un bug de logiciel. Donc l'idée n'est pas d'essayer de résoudre ce bug mais plutôt d'arrêter, de faire une révision et de redémarrer de manière à corriger la configuration et avoir la bonne configuration. Mais ce n'est pas la peine de faire ces modifications pendant que vous êtes en ligne. Dans un certain sens, la responsabilité de l'opérateur à ce niveau n'est pas considérable.

Quant au rapport automatisé, l'idée ici est que l'opérateur puisse vérifier que les ancres de confiance sont les plus récentes. Et le DNSSEC, vous savez, fait partie d'un monde qui est connecté. C'est pourquoi il faut vérifier que le résolveur – et je vais revenir là-dessus – mais l'idée est qu'il sache et qu'il informe de la clé, de la valeur de la clé qu'il utilise au moment d'informer les autres opérateurs de registre. Donc il faut activer ce type de mécanisme de manière à ce que les serveurs faisant autorité qui sont responsables de faire la

validation, pas tellement la validation mais qui devraient vérifier à ce qu'un nom de domaine soit joignable, qu'ils puissent vérifier que les bonnes ressources soient à disposition.

En ce concernant les ancres de confiance négatives, il faudrait faire un contrôle des défaillances de la signature mais pas de tout le processus entre les défaillances et les ancres de confiance négatives. Donc c'est une décision à prendre que de savoir si vous avez une ancre de confiance négative ou pas. Mais il y aura bien sûr une validation et des vérifications qui seront faites par des personnes, pas de manière automatisée.

En tant qu'opérateur, il ne faudrait pas que vous essayiez de trouver comment insérer une ancre de confiance négative lorsque vous en avez besoin. Et quant à comment gérer cette ancre de confiance négative, cela ne devrait pas être fait pendant que vous êtes actif et en ligne. Tout est bien documenté. Ce n'est pas à vous de trouver les réponses lorsque vous identifier ce problème ; on a une liste de recommandations qui a été publiée.

Et vous devriez pouvoir ajouter ces ancres de confiance négatives non seulement pour les résolveurs qui sont actifs mais également pour le moment du démarrage. Donc il faut des corrélations entre la génération de fichiers de configuration. Et lorsque vous insérez une ancre de confiance négative, il va falloir également qu'elle soit insérée dans le processus qui va générer les fichiers de configuration. Et ces fichiers ne seront pas distribués à travers les mises à niveau du logiciel.

Passons maintenant à l'intervention avec le cache. Vous devriez pouvoir vider le cache ou au moins vider toutes les informations de validation associées aux ancres de confiance. Mais les clés qui sont utilisées dans chaque cache ne sont pas registrées dans une liste, il n'y a pas de registre qui contienne ces informations. Donc même si on vide un nom de domaine qui a été empoisonné, il faut vider tout le cache. Et c'est quelque chose de viable. Il ne faut pas faire trop complexe.

Puis nous avons des clés qui ne sont pas des ancres de confiance mais qui sont les mêmes clés. L'idée ici est d'essayer d'éviter autant que possible d'avoir une clé qui ne valide pas, par exemple qui soit une vieille clé avec un TTL trop long qui ne puisse pas valider les nouvelles requêtes de la zone. Donc c'est ce qu'on essaie d'éviter. À ce moment-là, ce que vous pouvez faire, c'est de prendre le TTL qui n'a pas des valeurs correctes de manière à ce que les enquêtes entrantes n'aillent pas trop au-delà de la longueur de la clé et du TTL.

Si vous voyez un problème au niveau de la clé, vous devriez pouvoir informer de la clé qui est utilisée pour ce type de domaine. Nous utilisons une interface de DNS pour le faire. Nous vous recommandons de le faire également. Et nous vous encourageons à vérifier également les défaillances au niveau de la validation ; cela pourrait être utile pour les cas où il y aura des échecs de validation.

Lorsqu'on utilise des clés de signature qui sont utilisées pour la validation, vous devriez pouvoir distinguer les vieilles clés cryptographiques et les déconseiller de manière à ce que tout le

monde utilise la version la plus récente. Tout cela n'a pas été inclus dans la version préliminaire, je vais y ajouter vos feedback. Mais sentez-vous libre de faire des commentaires directement à travers la liste ou de me contacter également si vous avez des questions à me poser.

DAN YORK : Cette version préliminaire qu'Ed Lewis, Daniel et moi-même avons élaborée est conçue pour aider les gens qui font des opérations de résolveur de DNS comme le disait Daniel pour les aider à avoir une idée de ce qu'il faut qu'elles fassent pour faire la vérification de validation du DNS, quelles sont les différentes étapes de la validation. Parce qu'en général, on parle beaucoup de fichiers de configuration et de validation sans expliquer les complexités qui pourraient s'ajouter. Donc on voudrait vraiment savoir ce qu'en pensent les personnes qui sont ici dans la salle et celles qui sont à distance également pour nous dire si ce sont les bonnes recommandations, si on a un document qui est exhaustif, si l'on donnait ce fichier à quelqu'un qui travaille sur la validation d'un résolveur DNS, si les gens pourraient s'en servir, si toutes les informations y apparaissent, s'il y a des ajouts à faire. Nous avons ajouté nos adresses à la fin de la version préliminaire et vous avez ici lien pour pouvoir consulter le document.

DANIEL MIGAULT : L'idée est de dire si la version préliminaire pourrait être reprise. Et on m'a dit tout à l'heure qu'il y avait un FAI qui faisait la validation de DNSSEC, donc il leur a demandé : « Vous faites la validation du

DNSSEC ? » Et le fournisseur dit : « Non, je n'en était pas au courant. » alors que c'était une validation qui se faisait par défaut, c'était une configuration qui était déjà là. Donc il n'était même pas au courant du fait qu'il faisait la validation DNSSEC.

DAN YORK : Merci Daniel. Je vous encourage tous à consulter la version préliminaire de ce document.

Russ, vous êtes prêt ?

Nous allons maintenant céder la parole à Russ. Vous verrez qu'on ne parle pas du DNSSEC, ce qui semblerait assez étrange pour un atelier du DNSSEC. Mais au cours de la dernière année, le comité de programmes a réévalué notre travail et s'est rendu compte qu'il y a également d'autres technologies liées qui sont également liées au DNSSEC et à ce que nous faisons. Lors de notre dernier atelier du DNSSEC à la réunion précédente, on nous a proposé d'autres sujets à aborder. Donc on a ici visé à aller un peu au-delà du DNSSEC pour discuter de la vie privée, de la validation, etc. pour que tout le monde puisse comprendre complètement de quoi il s'agit. Donc si vous êtes ici et que vous avez un sujet que vous pourriez vouloir présenter groupe, faites-le-nous savoir parce que nous cherchons des propositions pour la prochaine réunion qui aura lieu bientôt.

Russ va nous raconter un peu ce qu'est le RPKI. Pour les intervenants, nous avons également un micro portable si vous voulez circuler

autour de la table. Ce n'est pas obligatoire de venir s'asseoir autour de la table. Russ ?

RUSS MUNDY : Comme Dan l'a dit, on a reçu des demandes d'approfondissement par rapport aux sujets qui étaient abordés ici. Et on sentait que les gens étaient intéressés par ce domaine et nous avons d'ailleurs inclus dans le programme des points d'information sur le routage et autres.

Nous allons présenter maintenant une introduction au RPKI, à l'infrastructure de distribution des certificats numériques. Attendez, la zapette ne fonctionne pas. Très bien.

Pour commencer, je voudrais expliquer ce qu'est la sécurité au niveau du routage. On en parle beaucoup mais où est-ce expliqué ce que c'est ? Il y a eu un travail de l'IETF qui était le premier document approfondi qui abordait les implications de sécurité du BGP dans le RFC 4272 publié il y a quelques années, je ne suis plus très bien à quelle date exacte, mais c'était le premier document publié par l'IETF de la sorte et il est reconnu comme un point de départ pour commencer à mettre en noir sur blanc ce qu'il fallait que l'on résolve.

L'IETF a alors abordé la question des ajouts ou des modifications qu'il fallait ajouter au BGP à travers une technologie cryptographique qui permet la validation des mises à jour des routeurs par rapport à leurs opérations en cours. Et c'est de cela que nous allons parler aujourd'hui. Les RPKI *piece*, ce sont des infrastructures de clés publiques et des ressources.

Il y a un groupe de travail qui s'appelle CIDR qui a déjà complété son travail et ce groupe CIDR a débouché en un groupe d'opérations de CIDR qui est actif et qui publie des spécifications du RPKI à travers des documents de BGP.

Voilà un petit aperçu de ce qu'est la sécurité au niveau du routage pour l'IETF. Il se pourrait que vous ayez entendu d'autres définitions mais je viens de présenter celle de l'IETF. J'ai inclus ces informations ici pour que vous puissiez y revenir par la suite pour voir tout ce qui a été fait, voir tous les incidents qui ont lieu.

D'ailleurs, si vous suivez la liste NANOG, c'est assez décourageant de voir qu'il y a toujours des problèmes de routage qui sont identifiés. Donc la liste est longue. Souvent, ce sont des cas qui sont un hasard, d'autres fois, ils sont intentionnés. Mais le problème, c'est qu'il n'est pas possible de les distinguer les uns les autres.

Aujourd'hui, la sécurité au niveau du routage se fait à travers le FAI qui vous dit : « Faites-moi confiance. Je suis votre fournisseur, je ferai ce qu'il faut à votre place. » Jusqu'à ce que l'on arrive au RPKI. Le déploiement du RPKI avance. Il est publié, on y reviendra un peu plus tard, il y a également d'autres présentations qui abordent la question. Donc il y a un ensemble de pas qu'il faut compléter. D'abord, il faut qu'il y ait un moyen permettant de connecter ou d'unir de manière prouvable en termes cryptographiques que l'entité qui fournit les ressources est valide. Donc cela pourrait être une adresse INTERET PUBLIC, le blocage d'une adresse IP ou un numéro de système par exemple.

Et pour que les gens sur le réseau y fassent confiance, il faut pouvoir déterminer que ces ressources sont utilisées par les entités appropriées de manière à ce que lorsque vous recevrez une mise à jour disant qu'il faut que vous ajoutiez à votre routeur des informations pour pouvoir renvoyer des paquets, les gens qui opèrent ces routeurs doivent pouvoir vérifier que ces mise à jour viennent du bon endroit.

Et en troisième lieu, il y a une vérification du parcours qui est suivi dans le réseau. Donc il faut pouvoir vérifier ce trajet. Il y a des activités en cours qui sont expérimentales, il y a des premières mises à jour de cela qui commencent déjà, mais c'est du travail qui est à compléter, qui est en cours. On en discutera longuement mais en définitive, si vous avez parlé du BGPSEC, c'est cela la troisième étape du RPKI.

Qu'est-ce que le routage internet ? Comment fonctionne-t-il ? Je n'entrerai pas ici dans les détails mais comme vous voyez, il y a des flèches bleues qui pointent vers les petits routeurs qui envoient des paquets dans un sens et dans l'autre qui font passer l'information. Comment faire de sorte que l'interface fonctionne correctement ? C'est cela le routage. Le parcours qui unit le client à gauche avec le serveur à droite, c'est ce que font le routeurs ; c'est eux qui font passer les paquets d'information à travers l'internet.

Vous verrez dans l'image générale qui est répétée ici dans la diapositive suivante qu'il y a également des systèmes autonomes qui s'impliquent également au monde du routage. Ces systèmes autonomes sont des ensembles de routeurs qui sont exploités par une

seule autorité administrative qui sont censés être opérés dans manière consistante, cohérence et cohésive. Ce n'est pas toujours le cas, bien sûr, mais l'idée est qu'ils travaillent ensemble.

Les cercles bleus avec ces flèches AS qui pointent dans un sens ou dans l'autre sont trois systèmes autonomes. On voit ici les systèmes autonomes 5, 6 et 7. Puis il y a des systèmes individuels qui sont des routeurs et qui fonctionnent comme les systèmes indépendants.

Que fait le système du protocole de routeur frontière, la passerelle ? C'est d'unir tous ces systèmes autonomes. À mesure que les informations passent d'un routeur à l'autre, le routeur doit d'abord déterminer dans quelle direction envoyer les informations, les relier aux systèmes autonomes. Et puis lorsque ces systèmes autonomes communiquent, c'est le protocole de routage du BGP qui intervient.

Le protocole de routage du BGP définit où se font les connexions des systèmes autonomes mais ne font pas passer des paquets. Ce sont les routeurs qui s'occupent de cela. Or, les protocoles de routage vont transporter les informations vers les différents routeurs et leur font savoir comment faire circuler ces paquets d'information.

En ce moment, comment savoir que c'est bon ? « Faites-moi confiance, je suis votre FSI et je sais ce que je fais avec le système autonome. Je vais faire ce qu'il faut pour vous. » Mais comment le savoir ? En fait, la question c'est que tout comme le DNS sans le DNSSEC, ceux qui verront la réponse ne savent pas si c'est la bonne ou pas. Alors pour les gens qui pensent au DNS et au DNSSEC et comment

cela fonctionne, de manière très générale, c'est un petit peu la même chose avec le système de routage.

Les enregistrements signés dans le DNS sont un petit peu l'équivalent des ressources signées. C'est ce que vous voyez dans ce schéma. Vous voyez une entité qui est connectée avec le système autonome 5. Ici, le client à gauche veut transporter des paquets vers le serveur qui est connecté au système autonome 4. Donc quand les choses fonctionnent bien, il y a différents chemins qui peuvent être empruntés par les paquets quand ils passent par des routeurs. Le chemin le plus court est la plupart du temps, mais pas toujours, le chemin préféré et c'est celui que va choisir le routeur pour envoyer les paquets.

Si le système autonome 1 reçoit le paquet, il dit : « Très bien. Je vais le envoyer au système 2. » Donc le système 2 le reçoit et il peut envoyer au système autonome 3 pour qu'il le donne au système autonome 4 et ensuite au serveur ou bien il peut choisir de l'envoyer directement au système autonome 6 et ensuite 7 qui, pour être renvoyé aux 3 et au 4. Donc on voit, on peut passer par 1, 2, 3 ou 4. Voilà une explication très simple de comment fonctionne le routage avec BGP.

Mais qu'est-ce qui se passe s'il y a utilisation malveillante ? Il y a un criminel qui se met là et qui dit : « J'ai un paquet pour le système autonome. » Mais il n'y a pas moyen pour le système de routage de savoir qui est le méchant. Donc qu'est-ce qui se passe quand le système autonome 5 dit qu'il y a un chemin plus court que les autres

vers le système autonome 2 ? Le système 2, il va envoyer le paquet au système 5.

Alors, où se trouve le RPKI dans tout cela ? C'est là où nous pouvons voir qu'il faut tout d'abord faire signer de manière cryptographique les ressources signées. Ensuite, les routeurs qui reçoivent l'information pour la mise à jour doivent valider ces informations mises à jour qu'ils reçoivent. Et ensuite, pour le mettre dans un contexte DNSSEC, c'est une signature et faire en sorte que les résolveurs valident. C'est un petit peu cela, la fonction est différente dans le monde réel et la mise en œuvre est différente dans le monde réel. Mais au niveau de la conception, c'est à peu près la même chose.

Donc ce que l'on a maintenant, quand on insère la RPKI et que l'on fait la signature et que l'on valide, le système autonome 2 va voir que la ressource que le système autonome 5 dit pouvoir « enrouter » n'est pas certifiée correctement. Donc le système autonome 2 peut choisir d'envoyer à 3 ou à 4. Donc vous avez une route invalide qui est annoncée parce que la RPKI est utilisée. Et de cette manière, la mauvaise route n'a pas été utilisée.

Voilà un résumé des trois étapes. Tout d'abord, certification de ressources – et cela est analogue à une signature de zone. Vous signez la certification de ressources et vous le rentrez dans la RPKI. La validation d'origine est faite par la machine qui est associée aux systèmes autonomes qui vont valider les mises à jour de routes avant que ces routes actualisées soient utilisées par les routeurs. Eventuellement, on veut avoir le chemin qu'utilisent les routeurs

actualisés et qu'ils soient validés quand ils passent par le réseau parce qu'il y a certaines organisations qui veulent avoir seulement certains chemins qui soient utilisés. Et c'est à quoi sert la validation de chemin.

Où est-ce qu'on génère les certificats et à quoi ils sont associés ? Tout commence avec l'IANA. Les numéros sont alloués aux registres internet régionaux. Ces registres internet régionaux à leur tour vont allouer ces ressources à des entreprises de différents types, que ce soit directement à une entreprise ou à un FAI.

Alors logiquement, les certificats associés à la RPKI commencent actuellement... C'était difficile de faire le schéma mais la chaîne de certificats commence avec les RPKI plutôt qu'avec l'IANA. Il y a cinq racines dans la structure du RPKI mais cela reflète l'allocation des ressources qui commence avec l'IANA et qui passe aux RIR. Et ensuite, les RIR sont les entités qui vont publier les ressources de numéros et qui vont faire fonctionner les certificats RPKI.

La première étape pour une entité, c'est de travailler avec les gens d'où on obtient les ressources de numéros. Il y a plusieurs manières de faire cette certification de ressources. Et il y aura une présentation plus tard qui va rentrer dans le détail. Mais une fois que vous avez cela signé, si vous avez une responsabilité dans le monde du routage, vous devrez valider les mises à jour. Et cela se passe à plus grande échelle au fur et à mesure que l'on avance dans ce monde du routage.

En haut, nous avons les RIR. Et le grand nuage en haut représente des millions de routeurs là dehors qui fonctionnent sur internet. Mais la partie importante de cette diapositive pour la RPKI elle-même, c'est

que la conception est telle que la validation des mises à jour des routages doit être faite de telle sorte que les routeurs ne soient pas chargés ou rechargés avec un traitement de clé cryptographique.

Qu'est-ce que c'est que les RIR ? Ce sont les URL des sites web et il y a plusieurs organisations régionales qui vont collecter toutes les RIR. Et il y a une page de statistiques que vous pouvez consulter pour savoir quelles sont ces statistiques au niveau de la RPKI.

Voilà donc un aperçu très rapide. Peut-être qu'on aura un peu plus de temps pour des questions, mais voilà la présentation que je voulais faire.

DAN YORK : Est-ce qu'il y a des questions pour Russ ? Est-ce que cela vous a aidé à comprendre ce qu'est la RPKI ? S'il vous plaît.

ORATEUR NON-IDENTIFIÉ : Merci beaucoup pour cette présentation. Est-ce que vous pouvez revenir à la diapositive précédente et réexpliquer ceci pour que je puisse vraiment comprendre comment se fait la validation ?

RUSS MUNDY : Les mises à jour BGP sont envoyées aux différents systèmes autonomes. En général, la conception de la RPKI fait en sorte que ces mises à jour peuvent être validées de manière extérieure aux routeurs qui sont ceux qui vont transporter les paquets. Donc la plupart des systèmes autonomes ont une structure selon laquelle ils fonctionnent

de manière cohérente et cohésive et ils construisent leurs tables de routage avant de les mettre dans les routeurs. Et c'est là où vous faites la validation des routages de manière appropriée.

Est-ce que cela vous aide ? Très bien, merci.

DAN YORK : Russ, la RPKI peut être comparée au DNSSEC en ce sens qu'il y a un côté validation et un côté signature. Les mécanismes sont différents mais il y a, comme vous avez dit, cinq racines, ce qui requière cinq changements de clé, etc. Un applaudissement pour Russ et pour sa présentation s'il vous plaît.

Après la pause-café, nous allons parler des nouvelles aventures sur la RPKI, donc on reviendra à ce sujet.

Maintenant, on va parler de ce qui pourrait être le prochain roulement de la signature de clé.

KIM DAVIES : Bonjour. Je m'appelle Kim Davies. Je travaille avec l'équipe IANA et je suis ici aujourd'hui pour vous présenter ce que nous pensons par rapport au futur roulement de la clé KSK.

Juste des informations de contexte. En 2010, nous avons généré la première KSK. Après certaines années, il y a eu l'idée de rouler la clé au bout de cinq ans. Les choses se sont passées et à un moment donné, une équipe de conception a été créée avec des techniciens et des gens de la communauté. Et cette équipe de conception a élaboré

un certain nombre de recommandations pour la mise en place du premier roulement de la KSK. Ces recommandations ont abouti à un plan et ce plan a prévu le roulement de la clé en 2017.

Finalement, cela a été reporté pendant un an en raison de certaines données que nous avions reçues et que nous voulions mieux comprendre avant de lancer le roulement. Finalement, le roulement a eu lieu et nous avons commencé à utiliser cette nouvelle KSK, la KSK2017, le 11 octobre 2018.

Le roulement général – tout le monde sera d'accord – a été réussi. Il y a eu des bouleversements minimaux comme résultat du changement de processus. Récemment, en interne, nous avons déclaré le projet complété avec la destruction finale de l'ancienne clé en août de cette année. Donc le projet est complet et la question qu'on se pose maintenant, c'est comment allons-nous envisager les prochains roulements de clé ?

Nous avons pris une décision par rapport au roulement au moment où ce roulement a eu lieu en 2017 pour essayer de capter l'intérêt de la communauté sachant qu'il y avait beaucoup d'attention focalisée sur le roulement. Et la communauté opérationnelle des FAI et les opérateurs de réseau faisaient très attention grâce aux activités de diffusion et de sensibilisation qui ont été menées.

À l'époque, nous avons fait un effort spécifique pour communiquer le projet de KSK et nous avons voulu avoir des retours par rapport à ces parties concernées pour envisager un mécanisme qui nous permet d'analyser tous ces retours et tirer des conclusions.

Nous avons fini cette opération en août de cette année et ensuite, nous avons commencé à analyser les retours. Nous sommes encore en train d'analyser tous ces retours pour pouvoir élaborer une proposition.

Certains points communs par rapport aux commentaires que nous avons reçus : le roulement de la KSK devrait être un évènement annuel ou quelque chose qui se fasse régulièrement ; possibilité d'avoir des clés d'urgences en backup ; mettre en place un suivi des impacts sur des ensembles de clé plus larges ; et considérer la possibilité d'alterner des algorithmes de création de clé.

Nous avons développé une proposition. Cette proposition vise à créer une approche prévisible pour des roulements futurs, un modèle qui puisse être prévisible, qu'on puisse répéter toutes les X années. Ensuite, nous avons lancé une consultation publique il y a quelques jours qui propose un roulement tous les trois ans. Nous avons considéré les retours, les commentaires et nous croyons que trois ans est un intervalle raisonnable pour faire ce roulement. Nous savons tous que c'est une opération complexe, c'est assez intense au niveau de la complexité ; cela doit être pris en compte. Notre proposition devrait prévoir la publication de notre ancre de confiance au moins deux ans avant le roulement.

Outre ces éléments clés, on dirait que l'approche est très similaire à celle que nous avons adoptée pour le dernier roulement. Et les cérémonies de signature seraient similaires à celles qui ont déjà eu lieu.

Ici, je sais que c'est difficile à lire donc je vais essayer de vous expliquer. Le point clé ici, c'est la phase qui est en bleu, la phase G où la clé est active. Le problème concerne notamment à générer la clé, reproduire la clé. Nous avons deux installations où l'on doit maintenir cette clé. Donc nous la reproduisons dans ces installations. Ensuite, il y a la première signature qui se fait dans la phase C. Ensuite, la phase D, processus de prépublication où l'on voit l'adoption 2015. Et ensuite, il y a une période qui suit. Ensuite, le roulement a un état actif dans la phase D. Et ensuite, la phase F, c'est l'activation pour de nouvelles clés. Et G et H sont des phases où nous révoquons les anciennes clés.

Pour résumer, il nous faut au moins trois trimestres pour pouvoir générer et reproduire les nouvelles KSK. Nous avons au moins sept trimestres où l'on est en état de standby et ensuite, on a 12 trimestres pour arriver à l'état actif, c'est-à-dire à la signature de zone. Ensuite les trois trimestres, on les utilise pour révoquer les anciennes clés et détruire les anciennes KSK.

Quand on regarde le schéma suivant, on voit la cascade des différentes opérations KSK et l'interaction entre elles. Ici, on voit que dans ce modèle, nous avons jusqu'à trois KSK de manière opérationnelle. Je vais rentrer dans le détail tout à l'heure mais c'est pourquoi nous avons pensé qu'un roulement annuel ne serait pas possible, parce que si l'on voit les délais, si l'on considère toutes les étapes, A, B, C, D, E, F, G et H, vous avez beaucoup de roulements qui seraient menés en parallèle.

On a ici quelques autres informations sur le choix de l'intervalle. On nous avait suggéré en général de le faire chaque année comme il nous faut quelques trimestres, comme je le disais, pour la publication de génération, pré-remplissement, prépublication, révocation et destruction. On ne voulait pas avoir plusieurs KSK actives en même temps.

C'est vrai que pour nos opérations, c'est quelque chose de complexe comme je le disais parce que les cérémonies de signature de clé, si vous ne le savez pas, prennent du temps et sont très intenses. Donc à chaque fois que nous avons une cérémonie de clé et à chaque fois que nous y ajoutons des acteurs, cela devient de plus en plus compliqué. Donc on ne veut pas avoir des cérémonies plus tendues si elles prennent quatre ou cinq heures comme elles le font aujourd'hui. Mais si nous avons davantage de cérémonies, il va falloir que l'on interagisse davantage avec les différents éléments qui sont appliqués ici pour détruire, pour signer, pour envoyer des demandes de signature pour chaque clé. Donc cela pourrait prendre sept ou huit heures que de compléter certaines cérémonies. Personne ne veut que l'on prolonge encore davantage les cérémonies. Nous croyons pourtant qu'il est essentiel de participer aux cérémonies pour pouvoir assurer que chaque acteur complète correctement ses responsabilités et exerce son rôle correctement. Donc l'idée ne serait pas de compliquer encore plus le processus et de le prolonger encore plus.

Au moment d'avoir des opérations de signature de clé lors d'un évènement de roulement, Verisign et d'autres opérateurs nous envoient différentes KSR pour avoir des cérémonies et des stratégies

alternatives au cas où il y aurait des problèmes au cours de la cérémonie de manière à pouvoir revenir en arrière dans les étapes et avoir d'autres clés à mettre en œuvre. Donc on a d'autres éléments qui ne sont pas souvent utilisés mais qui doivent être générés également.

Puis outre la gestion de signature de clé en direct, on le fait pour toutes les clés dans les cérémonies. Nous détruisons les clés toutes les quelques années. Nous avons les TCR qui sont introduis, qui sont supprimés, donc cela rajoute à la durée de la cérémonie à chaque fois également et au cycle de vie total.

Nous proposons également que la KSK soit créée plus tôt dans le cycle pour que l'adoption soit plus simple. Cela fournit une période de deux ans pour que les FSI puissent ajouter l'ancre de confiance à leur distribution et avoir ce choix disponible, cela diffère un peu de ce qu'on avait comme plan auparavant. Et puis au cas où l'on aurait besoin d'avoir un roulement non programmé d'urgence, si nous savons que cela est nécessaire, nous serions plus prêts pour précharger cela dans la KSK. Donc cela nous permettrait d'avoir un roulement plus rapide si on avait ces clés en standby.

Les impacts négatifs sur la permission d'avoir des attaques à la clé puisque nous publierons la clé auparavant ont été considérés des impacts négligeables.

L'une des suggestions était d'avoir une clé en standby ou d'urgence, de backup, ce que nous ne suggérons pas de faire en ce moment outre ce que nous avons fait bien sûr d'avoir la capacité en standby en publiant la clé avant dans le processus. On ne suggère pas que ce soit

fait parce qu'on n'a pas des installations correctes pour stocker ces clés. Donc peut-être que cette clé finirait par être partagée avec la KSK et on n'a pas vraiment vu de bénéfices considérables dans le cas où cela serait fait. Donc ce n'est pas vraiment bénéfique vis-à-vis de la complexité que cela rajouterait au système. Mais il faudrait l'étudier de manière plus poussée dans l'avenir. Donc nous considérons cela pour voir s'il serait possible d'avoir d'autre type de stockage ou une KMF qui doit différente. Mais en ce moment, on n'a que deux KMF qui sont conçues pour être identiques. Si on avait ces autres KMF, on pourrait peut-être considérer cela.

Changement d'algorithme. Donc nous sommes d'accord que cela doit être considéré mais nous ne croyons pas qu'il y ait une approche qui soit prête. Ce serait prématuré. Nous proposons donc que l'IANA commence à mettre en œuvre un changement d'algorithme. C'est bien plus avancé comme activité de recherche, on a une idée plus claire de comment on ferait ce changement dans la racine et on peut faire des essais dans un environnement de test et non pas dans un environnement qui soit actif. Nous proposons que ce travail continue mais en tant qu'activité séparée, peut-être dans le département du bureau de la technologie de l'ICANN, ce qui aurait été pratique pour le roulement que l'on a déjà complété au moment où on a commencé nos travaux.

Comme je le disais, nous avons élaboré et rédigé un document qui présente l'approche et qui fait maintenant l'objet d'une consultation publique. Il est disponible à travers le site web de l'ICANN. Nous avons reçu des commentaires hier lors de la réunion que nous avions

organisée. À partir de ces commentaires, nous avons remis la date butoir à la fin janvier pour que vous ayez un peu plus de temps pour faire des commentaires. Et une fois que cette période de consultation publique aura été conclue, nous vous inviterons à participer avec nous pour évaluer tous ces commentaires et pour les mettre en œuvre d'une manière pratique. Donc nous espérons pouvoir mettre en œuvre et publier un calendrier qui comprenne des dates vers la fin de cette année.

En sommes, il nous semble que les roulements de la KSK de 2010 et de 2017 ont été considérés réussis. Nous espérons pouvoir reprendre ce succès et le répéter dans l'avenir, mais d'y rajouter plus de prévisibilité et un calendrier ordinaire à ces roulements. Il me semble que les roulements annuels seraient trop complexes comme je l'ai dit tout à l'heure, mais nous espérons pouvoir publier les KSK auparavant pour donner davantage de temps pour le roulement de la clé. Si vous ne l'appréciez pas, c'est très bien mais on voudrait avoir vos commentaires toutefois. On cherche toujours à avoir des commentaires positifs, constructifs. Si cette approche vous semble inconvenable, faites-nous savoir quelle serait une meilleure approche. Nous essayerons de peaufiner l'approche que nous avons pour avoir une approche qui améliore ce que nous faisons à l'heure actuelle. Donc une fois que la période de consultation publique sera finie, nous publierons les commentaires et leur analyse.

Ah oui, j'ai ajouté ici une autre diapositive sur un autre sujet mais il me semblait que c'était à vous qu'il fallait que je parle de tout cela. Nous fêterons bientôt le dixième anniversaire des opérations de la KSK et

les bénévoles de la communauté, que l'on appelle les représentants de la communauté de confiance, travaillent avec nous depuis 10 ans. On sait que vous êtes tous intéressés par de nouveaux défis, donc on a conçu un nouveau plan pour commencer à remplacer ces représentants de confiance de la communauté qui servent depuis quelques années. C'est devenu un processus constant. Toutes les personnes intéressées peuvent envoyer des déclarations qui sont préservées. Et dès qu'on a de nouvelles disponibilités, on vérifie les SOI, les déclarations d'intérêt, que l'on classe en fonction des différents critères comme la diversité géographique, la diversité des genres, l'appartenance aux différentes communautés, etc.

Pour notre processus, nous avons un peu modifié la procédure. Nous avons maintenant 10 personnes qui ont été sélectionnées pour remplacer les membres actuels de notre TCR mais pour les TCR actifs, nous allons donc faire de nouvelles nominations d'ici quelques mois pour l'année 2020. Donc ce groupe de personnes qui sont disponibles va être utilisé et il faudra retrouver d'autres bénévoles. Si vous êtes intéressé à participer à nos TCR, on cherche toujours d'autres volontaires qui souhaitent y participer. Donc si cela vous intéresse, faites-le-nous savoir et envoyez des candidatures. Voilà.

Si vous avez des questions, je serai ravi d'y répondre.

DAN YORK : Merci Kim. Vous êtes le seul à avoir fait une présentation qui parle de destruction tout le temps et de détruire. J'imagine que personne ne voudrait passer huit heures dans une petite salle dans un centre de

données à parler de destruction. C'est vrai qu'on ne veut pas prolonger la cérémonie sans doute.

Vous disiez que le processus et les commentaires opérationnels de janvier ou février, la fin de la période consultation, seront intégrés. Quand est-ce que vous commencerez le processus si les commentaires sont repris ? Parce que je sais que c'est un travail qui prend deux ou trois ans pour arriver à la prépublication du document.

KIM DAVIES : Je dirais – et c'est un justement individuel, c'est mon opinion personnelle – étant donné qu'on a déjà bien commencé à travailler et que la période est déjà commencée, on ne suivra pas le même calendrier de trois ans suivant le premier roulement. Mais peut-être que dans les prochains trimestres, on sera en mesure de publier cela. Donc peut-être que la prochaine KSK pourrait être générée en 2020.

DAN YORK : Merci.

Dmitry.

DMITRY BURKOV : Merci. J'ai des commentaires à vous faire, Kim. Ce n'est rien de neuf mais je voulais le répéter en public.

Avant de commencer à travailler sur une nouvelle initiative, est-ce que l'on ne pourrait pas vérifier si la récupération fonctionne dans tous les

cas ? Parce que nous avons discuté de la récupération mais on ne savait pas quelle était la situation avec les smart cards. Donc avant de commencer à parler de cycle de vie, de modification au processus, je pense que l'on devrait d'abord réviser toute la procédure.

Du point de vue de la génération de la KSK et de la cryptographie, je sais que cela ne prend pas énormément de temps. Dans la pratique, on a pu le faire en peu de temps auparavant. Vous proposez maintenant une nouvelle idée qui est de prendre des cycles de quatre ans pour remplacer à chaque fois la KSK, ce qui, il me semble, n'a aucun sens. Mais le cycle de vie des smart cards avant était de 10 ans. Et en général, ce sont des choses qui n'intéressent personne que de raccourcir ce cycle de vie.

Et par rapport aux HSM, je pense qu'on les remplace étant donné de la durée de vie de la batterie. Je ne comprends pas pourquoi on passerait de 10 ans à quatre ans, à trois ans. Cela devrait être quelque chose de plus raisonnable. Par exemple, un cycle de vie de la KSK d'un an serait trop court ; il n'est pas nécessaire. Il y a des avis plus extrêmes qui disent que l'on pourrait générer de nouvelles KSK à chaque cérémonie sans avoir besoin de plus d'installations. Cela dépend de nous, c'est une décision à prendre. C'est juste qu'il faudrait voir ce qui est le plus raisonnable.

Dans le domaine de la récupération, pour revenir à ce que je disais, avant de commencer un remplacement ou une transition, il faudrait supprimer la clé précédente si nécessaire. Merci.

KIM DAVIES : Vous avez soulevé un bon nombre de questions.

Le cycle de vie est de cinq ans, c'est ce que nous visons à atteindre en ce moment. Mais la situation particulière que nous avons avec la gestion des HSM est que le HSM n'est jamais connecté au système électrique, au réseau, sauf toutes les six moins pendant une heure et demie. Donc la durée de vie de la batterie est importante parce que c'est de quoi nous dépendons. On est conservateurs du fait de dire qu'on va le faire toutes les cinq années parce qu'on en a quatre sur deux installations, c'est-à-dire qu'on remplace une HSM toutes les cinq cérémonies ou chaque 1.25 années. C'est vrai qu'on ne remplace pas les HSM à chaque cérémonie mais l'idée serait d'avoir des cycles de vie de cinq comme je le dis.

Par rapport aux smart cards, nous nous y penchons à partir de recherches récentes. C'est une activité que nous sommes en train de réaliser en parallèle. Mon commentaire à ce sujet visait à transmettre l'idée que nous avons d'autres évènements opérationnels qui prennent du temps et qui ne nous permettent pas de nous consacrer à des cérémonies de signature à chaque fois.

Mais nous avons une approche de planification et nous devons faire attention aux besoins de ces activités opérationnelles. Et il nous semble que tout cela doit se faire suivant un ordre, qu'il y ait des témoins présents, les TCR. Et les gens ne peuvent pas faire attention constamment, donc il faut mettre à profit le temps qu'ils nous consacrent.

DMITRY BURKOV : J'étais surpris par cette dernière idée de générer tout type de cartes de smart cards. Cela pourrait poser un problème organisationnel. J'apprécie vos idées autrement.

KIM DAVIES : Oui, donc on explore en fait les idées avec les TCR. On n'a pas décidé d'une approche. On essaie de savoir ce qu'ils en pensent d'abord. Merci.

DAN YORK : Y a-t-il d'autres questions ? On est un tout petit peu en retard mais on a le temps pour les questions si vous voulez.

JACQUES LATOUR : Est-ce qu'on pourrait revenir en arrière ? Ici, on a une dernière destruction et en parallèle, on a la création de la nouvelle clé. Avez-vous considéré la possibilité de faire A le trimestre suivant après avoir fait le H de la période précédente pour qu'il n'y ait pas de superposition et pour que le travail soit séquentiel ?

KIM DAVIES : Oui, ce serait possible. On essayait d'avoir un équilibre raisonnable où il n'y aurait pas trop de superposition. On pourrait bien sûr le prolonger encore plus. Soyez conscients qu'on essaie de faire la concurrence à cette idée de roulement annuel. Je sais que ce n'est pas ce que préféraient beaucoup de personnes mais c'est un point à discuter. On croyait qu'il faudrait que l'on ait une fréquence plus

équilibrée mais on pourrait bien sûr le prolonger pendant quelques trimestres de plus.

JACQUES LATOUR : Oui. Peut-être que les séances devraient être plus courtes et que les observations seraient de tout avoir branché à ce moment-là.

KIM DAVIES : Ce n'est pas trop pratique mais on verra, on en parlera.

DAN YORK : On a plus de temps. On a décidé de respecter la pause-café de 15:00 à 15:15. On s'est que Yoshiro ne peut pas parler aussi vite et ce serait intéressant de lui donner plus de temps donc si vous avez d'autres questions à poser, sentez-vous libre de les poser tout de suite.

JACQUES LATOUR : Avez-vous vraiment besoin d'avoir une année ou pourrait-on avoir une année et deux ou trois trimestres pour améliorer les délais du processus ? Parce que la durée n'est pas le principal. Le plus important est d'avoir une période ordinaire de deux ans ou trois ans. Mais si c'est plus simple pour l'IANA et pour les autres bénévoles de travailler au processus de cette manière et de ne pas avoir une séance super longue et super ennuyeuse, c'est un facteur à considérer.

KIM DAVIES : Du point de vue opérationnel, il n'est pas nécessaire que nous respections ces durées d'une quantité X d'années. Cependant, on l'a évalué du point de vue des rapports publics et de la sensibilisation et étant donné qu'on essaie de se borner à des trimestres, étant que ce sont des méthodes que nous avons utilisées qui semblent bien fonctionner, c'est mieux de le faire le même jour chaque année, par exemple le 11 octobre. Si on disait : « C'est le 11 octobre. », c'est plus simple de communiquer ce message et que les gens s'en souviennent. Si on change du 11 avril au 11 juillet d'une année à l'autre, c'est plus difficile de communiquer.

J'ai cependant une sauvegarde à faire ici et c'est le fait que nous essayons toutefois de transmettre l'idée que ce sont des dates cibles. S'il y avait une anomalie opérationnelle qui nous exigeait de faire une pause, on n'hésiterait pas. Bien sûr, le principal est la stabilité de la racine, son intégrité. Donc si on devrait remettre nos mesures d'un trimestre, de deux trimestres ou de trois trimestres, on le ferait. Donc ces dates, dans la pratique, pourraient être remises comme dans le cas du dernier roulement.

Mais ceci étant, il est utile d'avoir un calendrier prévisible sachant que cela se fera tous les 11 octobre tous les trois ans. C'est plus facile de communiquer comme cela.

DAN YORK : Et les administrateurs de DNS sauront quand partir en vacances, ce qui est important.

Y a-t-il d'autres questions ? Est-ce que quelqu'un va se présenter comme candidat pour le groupe des TCR, les représentants de confiance de la communauté ? Il nous faut des candidats.

ORATEUR NON-IDENTIFIÉ : Ce n'est pas pour me porter volontaire mais je me demandais si les cérémonies se font toujours aux États-Unis étant donné qu'il faut les faire là où il y a le personnel. Mais peut-être qu'on pourrait considérer d'autres alternatives.

Je pensais à la difficulté de faire des mises à jour de logiciels ou autres dans le monde réel. Peut-être qu'on en est déjà à la période minimum de sécurité qui nous permet de faire ces roulements et de faire attendre les autres. Donc c'est pour cela qu'il me semble plus convenable de ne pas changer à des cycles de vie d'un an.

KIM DAVIES : Par rapport à la question de l'emplacement des cérémonies, on avait une nécessité historique de placer les installations aux États-Unis suivant notre contrat avec l'IANA. Ce n'est plus le cas. On pourrait reconfigurer l'emplacement. Cela aurait un coût cependant et on aime bien avoir les commentaires de tout le monde là-dessus. Mais oui, étant donné la configuration actuelle, ce serait possible. Ce n'était pas possible auparavant.

DAN YORK : J'ai Warren et Sergei.

WARREN KUMARI : Warren de Google.

J'allais proposer d'avoir des établissements de gestion ailleurs, mais vous venez d'en parler.

DAN YORK : Sergei ?

SERGEI : J'ai un commentaire sur la procédure des TCR.

J'ai présenté une candidature mais je voudrais avoir le feedback de votre part. Je ne sais pas si ma candidature est toujours valable ou pas parce que je n'étais pas retenu comme TCR.

KIM DAVIES : Si votre candidature a été envoyée après 2017, c'est là qu'on a lancé le nouveau processus, elle devrait toujours l'être. Le but est d'envoyer des rappels annuels et il me semble que c'est ce qu'on a fait l'année dernière. Vous me le direz si ce n'est pas le cas. Et on avait lancé un appel à bénévoles en 2009. Au départ, on avait sélectionné les premiers TCR. Il n'y a pas eu d'autres appels jusqu'en 2017. Et en 2017, nous avons commencé avec ce processus permanent sur le site web que nous avons lancé et on reçoit des candidatures constamment.

Autrement, on envoie un rappel annuel aux bénévoles comme je le disais pour leur faire savoir que leur déclaration d'intérêt est toujours

dans nos archives, pour savoir si les personnes sont toujours intéressées, si leurs circonstances ont changé, si les personnes veulent toujours être dans ce groupe de candidats ou pas.

Donc si vous avez envoyé une candidature, si vous n'avez pas eu de réponse, il se pourrait qu'il y ait un problème mais je pourrai vérifier individuellement si votre candidature est toujours valable et enregistrée. Merci.

RUSS MUNDY : Moi, je voudrais remercier Kim personnellement d'avoir fait cette présentation ici à l'atelier parce que c'était la bonne occasion de présenter ce sujet. Je sais que vous l'avez abordé à d'autres séances mais étant donné l'intérêt de votre travail, on voulait vous donner autant de temps que possible puisque vous étiez là. Et je voudrais reconnaître que l'ICANN, la PTI et Kim ont présenté leurs travaux en temps et en heure. On vous en remercie.

DAN YORK : Ceci étant, nous allons faire la pause. Merci Kim d'être venu. Je vous encourage vivement à télécharger la présentation, à consulter le document, à y faire des commentaires puisque c'est ce qu'il faut à Kim et à son équipe pour bien comprendre votre avis, même si c'est pour dire : « C'est très bien, je suis d'accord. » C'est très utile pour Kim de recevoir ce type de message. C'est ce qui lui faut. Donc merci.

On part à la pause. On reprend à 15:15 et c'est Jaap qui va nous parler des nouvelles aventures dans le domaine de la RPKI. Désolé, non,

plutôt Jaap ne sera pas le premier. Ce sera Yoshiro qui présentera d'abord et qui va devoir nous quitter tout de suite à la fin de sa présentation. Donc Yoshiro, Jaap et puis moi.

[FIN DE LA TRANSCRIPTION]