SAN JUAN – Atelier de DNSSEC - Partie 3
Mercredi 14 mars 2018 – 13h30 à 15h00 AST
ICANN61 | San Juan, Porto Rico

JACQUES LATOUR : C'est l'interrogation. Vous devriez l'avoir, on l'a distribuée. Si vous ne l'avez pas, j'ai ici quelques feuilles. S'il vous faut encore une feuille, dites-le moi. On peut mettre le nom de Warren aussi.

ORATEUR NON-IDENTIFIÉ : Je vais compléter trois interrogations pour ainsi gagner le prix.

JACQUES LATOUR : Très bien. Vous pouvez créer vos propres règles. Il y a six bonnes réponses par question, six points par bonne réponse, 6,5 points par bonne question. Il y a 8,5 questions. Nous avons quelques heures pour répondre à cette interrogation. Donc un point par réponse, une réponse par question, maximum de 10 points. Et nous allons démarrer maintenant.

Première question – il y a une réponse par question. Vous ne pouvez pas mettre A, B, C, D ; il y a juste une réponse à chaque question. Vous n'aurez pas de point. Si vous voulez, vous pouvez mettre plusieurs réponses mais à ce moment-là, vous aurez zéro point.

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

Première question. Quel est le ccTLD qui a le plus récemment signé le DNSSEC ? A) Guinée-Bissau ; B) les îles Åland ; C) Bhutan ; D) ou l'Italie. Donc quel est le ccTLD qui a le plus récemment signé le DNSSEC ? Une seule réponse.

Deuxième question. En quelle année Porto Rico et Brésil ont pour la première fois signé leur TLD ? A) 2007 ; B) 2009 ; C) 2011 ; D) 2013 ; voilà les quatre possibilités.

Troisième question. Conformément aux statistiques d'APNIC, quel est le pays qui a le déploiement le plus important par habitant ? Quel est le pays qui a les taux les plus importants de déploiement de DNSSEC ? A) La Suède ; B) Kiribati ; C) Les Pays-Bas ; D) Groenland. Très bien, j'avais mal lu, excusez-moi.

Quatrième question. Conformément au RFC 4509, comment les résolveurs validant gèrent la présence de SHA1 et SHA256 dans un ensemble d'enregistrements de ressources DS ? La mise en œuvre doit ignorer les enregistrements DS ou les enregistrement DS SHA1 ou SHA256 ou doivent être compatibles avec les deux types d'enregistrement DS. Voilà les quatre possibilités. Nous en avions parlé à un moment donné par rapport à cela.

Cinquième question. En quelle année a été tenue la première cérémonie de signature KSK pour la zone racine à Culpeper, Virginie, États-Unis ? On ne sait pas. A) 2004 ; B) 2007 ; C) 2010 ; D) 2012.

Question six. Que représente le H dans le paquet logiciel SoftHSM ? A) Homogénéisé ; B) Heuristique ; C) Durci (Harden en anglais) ; D) Hardware.

Question numéro sept. Quel est le TLD qui a le plus grand nombre d'enregistrements DS enregistrés depuis la signature de la racine ? A) .se ; B) .nl ; C) .us ; D) .bank. La source, ce sont les diapositives de Roy. On a pris ces informations d'une diapositive de DNS-OARC.

Question huit. Lesquels parmi ces termes liés au DNSSEC n'est pas un acronyme ? A) DANE ; B) ENAM ; C) [DKIEM] ; D) DNS. Jake m'a aidé avec cette interrogation. Il a l'habitude de cela, donc c'est une question intéressante. Une seule réponse possible.

Question numéro neuf. Quel pourcentage de tous les TLD de la racine sont signés ? A) 97-100 % ; B) 94-96 % ; C) 90-94 % ; D) 86-89 % ; E) 81-85 %.

Dernière question. Lequel des TLD suivants ne se trouve pas dans la zone racine ? A) .aaa ; B) .abd ; C) .aco ; D) .aeg ; E) .ant. Je n'ai pas eu besoin de faire défiler plusieurs pages pour trouver ces exemples. Très bien.

Voilà, c'est le moment de corriger. S'il vous plaît, mettez votre nom sur la feuille, passez la feuille à votre voisin, nous allons corriger. Et j'ai toujours raison ; je suis la source qui fait autorité.

Première question : Bhutan, 2 décembre 2017 ; c'est le plus récent ccTLD signé. Donc la réponse correcte, c'est C).

Deuxième question : 2007, Porto Rico. Donc la réponse correcte, c'était la réponse A). J'espère ne pas m'être trompé. Quand est-ce que vous avez signé pour la première fois le TLD ? C'est le moment où ils ont signé pour la première fois. Si nous voyons, les statistiques, elles proviennent de Verisign.

Troisième question : alors la réponse correcte, c'est .gl, le Groenland, 76,98 %.

Question quatre : donc pour cette question, cela vient de l'atelier DNSSEC. La réponse correcte, c'est B, ce qui rend un roulement de la KSK non valide.

Question numéro cinq : la réponse correcte est la réponse C), 2010. L'idée, c'était de répondre correctement aux questions pour pouvoir avoir le billet pour manger. Mais bon, ce n'est plus le cas.

Alors pour la question six : la réponse correcte, c'est la réponse D), matériel, c'est-à-dire hardware en anglais.

La question numéro sept : le .us, c'est celui qui a le plus grand nombre d'enregistrement DS, c'est-à-dire que la réponse correcte est la réponse D). La réponse est sur les diapositives de Roy. Je vous assure qu'elle se trouve là. Donc la réponse

correcte, c'est la réponse D). Vous pouvez envoyer un courriel à Roy si vous avez des doutes. J'ai toujours raison, je vous l'ai dit. C'est la quantité d'enregistrements DS dans la racine. La question était la suivante : quel est le TLD qui a le plus grand nombre d'enregistrements DS depuis que la racine a été signée ?

Alors il y a deux KSK avec quatre DS de différents types par clé. Il faut savoir que celui qui pose les questions a toujours raison. Très bien, exactement.

E-N-U-M, c'est comme cela qu'on le dit, non ? DANE, NUM, [], DNS. Et la réponse correcte pour la question numéro 8, c'est DNS.

Question suivante : pourcentage 90-94 %.

Et ensuite question dix, la réponse correcte, c'est la dernière possibilité, .ant.

Très bien. Nous corrigeons maintenant. Qui ont eu cinq points ou plus ? Six ou plus ? Une seule personne ? Sept ? Huit ? Neuf ? C'est tout ? Alors vous êtes le grand gagnant.

RUSS MUNDY : Très bien, merci tout le monde. Nous nous amusons toujours avec cette interrogation. Mais maintenant, nous allons devoir

nous dépêcher un petit peu parce que le quiz était prévu pour avant le déjeuner.

Maintenant, je vais passer la parole à Viktor Dukhovni, qui va faire sa présentation. Allez-y, Viktor. Vous avez un micro. Vous pouvez vous lever et prendre le micro si vous voulez. Très bien.

VIKTOR DUKHOVNI : Je vais le tenir, d'accord. Je m'appelle Viktor Dukhovni. Je travaille dans le domaine de la sécurité et de la messagerie électronique depuis un certain temps. J'ai écrit quelques RFC concernant la sécurité dans cet espace.

Je vais vous parler, d'un côté le contexte, je vais vous donner un peu de contexte. Ensuite, je vais parler de DANE. Si vous ne savez pas ce que c'est, je vais vous expliquer brièvement. Je vais vous parler de ce qu'il faut faire même si vous ne mettez pas en place DANE. Mais si vous avez une zone qui est signée DNSSEC, vous pouvez recevoir des courriels des gens qui ont mis en place DANE. Et donc nous allons voir ce qui peut se passer dans ce cas. Nous allons parler de comment mettre en place DANE de manière fiable parce qu'il y a des gens qui veulent le mettre en place mais ne savent pas comment le faire de manière correcte. Donc je vais vous expliquer un petit peu comment mettre en place cela. Et ensuite, nous allons parler d'une enquête que nous avons mise en place qui fait un suivi de l'adoption de DANE

pour voir quelles ont été les difficultés, le cas échéant, lors de la mise en œuvre de ce type de solution.

Ensuite, on a une annexe. J'ai beaucoup de matériel en cas où on n'aurait pas suffisamment de temps d'aborder toute cette question. Il y a donc énormément de diapositives. J'ai une cinquantaine de diapositives. Je sais que je ne vais pas pouvoir vous les présenter toutes, donc dans l'annexe, vous avez le reste de la documentation.

Parlons donc de la sécurité des courriels. Nous avons donc l'expéditeur qui peut utiliser l'authentification TLS qui envoie un message à un destinataire à travers un serveur de messagerie. Et le destinataire peut lire ce message à travers une authentification TLS pour savoir que l'expéditeur est le bon expéditeur.

Donc nous avons le MTA, c'est-à-dire le transfert de courriels qui permet cet échange entre l'expéditeur et le destinataire. Nous avons donc une authentification avec un chiffrement complet.

Et donc je vais vous décrire en détail ce qui se passe dans cette deuxième étape entre l'expéditeur et le destinataire. C'est l'espace où j'ai mis qu'il y a un miracle qui se produit. Très bien.

Que se passe-t-il entre les organisations quand on échange des courriels ? Nous avons quelque chose qui s'appelle STARTTLS ou

Opportunistic STARTTLS. Ce sont des serveurs de messagerie où l'on veut déterminer si le destinataire est compatible avec un chiffrement des données qui sont dans les courriels. Avec cette technologie, qui est très utile, elle permet de faire en sorte qu'aucune interférence ne puisse endommager ou ne pas permettre cette communication.

Mais cette technologie est vulnérable à des attaques actives. Vous pouvez lire des documents qui montrent que cela arrive de temps en temps. Et l'attaquant actif qui veut interférer peut détourner le BGP et donc retarder le courriel pendant quelques heures ou bien il peut empoisonner le cache du DNS ou bien il peut également affecter le STARTTLS et l'expéditeur reçoit un message comme quoi le destinataire n'est pas capable de recevoir son courriel.

Malgré tout cela, la solution STARTTLS a eu beaucoup de succès. Vous le voyez dans ce graphique, vous voyez comment l'évolution de l'adoption de cette solution a progressée au cours des dernières années. Je me souviens, il n'y a pas longtemps, il y avait 5 ou 10 % de taux d'adoption. Mais maintenant, à droite, vous voyez que 90 % des courriels qui passent par Gmail sont chiffrés à l'aide de STARTTLS. Il y a un lien au bas de la page sur lequel vous pouvez cliquer pour plus d'informations.

J'aimerais donc vous parler du SMTP et pour voir comment on peut résister aux attaques actives de type empoisonnement de cache, etc. Comment faire ? Nous sommes dans un écosystème où il y a beaucoup d'attaques qui sont opportunistes et c'est pour cela qu'il nous faut un signal qui nous dise que l'expéditeur est sécurisé. Et ce signal doit être véhiculé à travers un mécanisme qui, dans ce cas, peut être le DNSSEC.

Un message à retenir, c'est que beaucoup de gens veulent dire que certains SMTP utilisent DNSSEC, mais ce n'est pas comme http. Ce sont deux systèmes différents. Vous pouvez en savoir davantage si vous cliquez sur le lien. Mais la première différence, c'est la direction. Le courriel peut déterminer quelle est la direction alors que http ne le fait pas. Et il faut faire confiance au contenu du prochain enregistrement.

Et l'autre point, c'est que, à mon avis au moins, le web ICP, les autorités de certification sont trop nombreuse pour pouvoir construire un système de vérification. Quand il y a une exception avec http, on peut cliquer dessus et vous pouvez dire : « Je veux voir cette page quand même. » alors qu'avec le courriel, on ne peut pas dire : « Je veux voir ce message quand même. » Et donc on doit faire confiance à ce système.

Alors donc voilà que DANE arrive et DANE est tout à fait adapté au SMTP. Donc DANE, c'est donc l'authentification basée sur le

DNS des entités nommées, traduit en français. Donc dans le SMTP, la définition de la RFC 76 que nous avons mise en place, il est indiqué que l'on peut recevoir des courriels de manière sécurisée en publiant un enregistrement dans la zone signée par le DNSSEC.

Donc l'enregistrement que l'on publie commence par un chiffre de port, le 25. Ensuite, il y a une étiquette de protocole, on utilise le TCP et ensuite, il y a l'hôte qui est nommée avec sécurité. Et il y a des paramètres qui indiquent comment sécuriser le trafic.

La présence de cet enregistrement TLSA pour les courriels tel qu'il est définit par la RFC dit que je ferai absolument à chaque fois le STARTTLS, sinon, cela veut dire qu'il y a une attaque ou une erreur opérationnelle dans ma zone, par exemple j'ai oublié d'activer STARTTLS même si j'avais promis de le faire. Donc c'est important.

Le signal passe par le DNSSEC. Donc en fait, c'est résistant au déclassement. Étant donné que le DNSSEC authentifie qu'il y a un déni d'existence, le résolveur validant ne va pas identifier l'attaquant. Il va voir un échec et va passer à la suite.

Donc nous avons un contrat pour faire le STARTTLS. Mais au-delà de cela, nous avons également un contrat non seulement pour faire le STARTTLS mais pour avoir également une chaîne de

certificats d'authentification qui correspondent à ces enregistrements. Donc voilà ce à quoi la clé SHA256 correspond.

DANE authentifie les contrôles de manière à ne pas avoir des CA externes chiffrés. Il y en a auxquels on fait confiance, d'autres non. Donc le service est autonome dans le DNS, à la fois pour la publication des enregistrements et pour l'authentification. Et il y a donc résistance au déclassement.

Ensuite, j'avais promis que je parlerais un petit peu de ce qu'il faut faire pour faire fonctionner le DANE. Les domaines commencent à le mettre en place. Comcast – je ne sais pas si le monsieur est toujours là –, ils font toujours validation de DANE outbound. Donc si vous recevez un courriel de Comcast, faites attention à cela. Ou alors web.d et ietf.org, même chose : ils utilisent l'authentification DANE pour l'expédition. En tout cas, ils le font pour les courriels qui arrivent.

Alors les expéditeurs DANE ne parleront pas à un hôte MX lorsqu'il y a un échec. Le TLSA peut prouver que l'enregistrement n'existe pas. La non-existence n'est pas un échec. Un échec, c'est des données mauvaises : de mauvaises signatures, un problème par rapport au paquet DNS ou des signatures qui ont expirées, etc. ou alors, pas de réponse. Si on est dans cette situation et surtout, si c'est quelque chose qui se

passe sur l'hôte MX, vous n'aurez pas de courriel. Et cela ne va faire que continuer au cours des années à venir.

Donc sans enregistrement TLSA, si vous n'avez pas le DANE, assurez-vous que le déni d'existence est livré de manière fiable. Et DANE est le premier protocole pour lequel ceci est important. Il y a d'autres choses qui entrent en compte qui s'appuient sur le DNSSEC, pour protéger les enregistrements qui sont là, pour s'assurer que ce qui est là est protégé. Mais là, on parle de ce qui n'est pas là.

Alors ce qui n'est pas surprenant, c'est qu'en 2013, quand j'ai commencé à travailler sur le DANE, il y avait beaucoup de serveurs de noms qui ne fonctionnaient pas bien avec cela parce qu'en fait, peu importait. Et maintenant que nous l'utilisons, la plupart des opérateurs utilisent le système. Mais il faut le savoir pour tester son propre système.

Alors la clé avec le DANE, c'est l'hygiène de votre DNSSEC. Donc tout ce que vous avez à l'écran, EDNS(0), fragments IP, bonnes réponses, no data, etc., tout ceci doit fonctionner sur votre domaine. Donc je ne vais pas tout lire dans toutes les diapositives. Ce qu'il retirer de tout cela, c'est de tester vos domaines pour vous assurer que tout fonctionne.

Donc la surveillance. Alors, autre chose, il y a un certain nombre de pare-feu, de boîtiers intermédiaires. Il faut donc protéger vos

serveurs de noms contre ce trafic hostile en bloquant les requêtes pour certains types d'enregistrement. Donc si vous avez par exemple une requête MX, ça va. Mais si par exemple le TLSA, CA, de nouveaux types, et bien il faut bloquer ces requêtes. Peut-être pas, en fait, parce que si vous bloquez, cela casse le DANE ; cela ne fonctionnera plus. Et puis en plus, il y a le problème des délivrances de certificat d'autorité. Ou alors, peut-être que cela bloquera votre roulement de KSK.

Donc ne déployez pas de pare-feu qui bloque les requêtes de DNS par type d'enregistrement. C'est une mauvaise idée, cela n'aurait jamais dû exister. Mais si vous avez un pare-feu de ce type, et bien ne le mettez jamais en route.

Alors je vous donne des exemples avec Digg de tests, de requêtes que vous pouvez utiliser. Et donc la réponse, c'est « no data MX domain ». Donc en principe, il ne devrait pas y avoir d'expiration.

Alors voilà la liste de contrôle DNSSEC. Je ne vais pas rentrer dans le détail là-dessus. J'ai mis différents points avec des points en plus sur l'hygiène du NSEC3. Ce n'est pas directement lié au DANE, mais c'est quand même quelque chose qui est important que j'ai inclus dans le questionnaire. Vous pouvez lire les liens et comprendre un petit peu ce qui se passe en matière d'hygiène DNSSEC.

Alors un petit diagramme avec DNSViz avec les envois de courriels. Donc techtrack.gov, à chaque fois, lorsqu'on a signé leur zone, on avait toujours un numéro de série plus élevé après le SOA. Donc le SOA ne valide pas et cela ne marche jamais. Donc si vous écrivez un code, vous pouvez faire un inversement et en fait, je me rappelle qu'il y avait une différence [inintelligible]. Et si je change d'un seul point, et bien cela signait. Alors attention, surtout pas. Donc faites attention parce que s'ils avaient, en fait, fait la surveillance, ils s'en seraient rendus compte. Alors voilà pour l'hygiène DNSSEC. Donc faites-le même si vous n'utilisez pas le DANE.

Alors il y a d'autres diapositives avec des exemples de mauvaise hygiène DNSSEC, vous verrez.

Alors adoption de DANE. Alors imaginons que vous êtes très enthousiaste par rapport au DANE, vous souhaitez absolument l'adopter. Alors la première chose, c'est qu'il faut déjà avoir le DNSSEC ; il faut signer vos zones. Une fois que vous avez signé vos zones – et c'est là que cela se complique –, la gestion du DNSSEC, en fait, c'est difficile. Vous verrez que le DANE n'est pas compliqué. Je vais vous convaincre.

Alors ce qui est compliqué – et je vais vous montrer comment le faire correctement – c'est de coordonner vos enregistrements TLSA et votre chaîne de certificat. Parce que DANE, à la base,

nécessite que vous changiez, lorsque vous faites la rotation de vos clés, sur deux endroits. Premièrement, le déploiement de vos certificats de vos clés privées et également, mise à jour de vos enregistrements TLSA. Et ces changements, cela peut paraître compliqué mais vous allez voir, cela va être simple ; je vais vous expliquer.

Alors première chose, on va parler du DANE de sortie. Imaginez que vous n'êtes pas prêt à signer votre zone, que vous n'avez pas bien compris de manière opérationnelle, vous n'avez pas convaincu votre équipe. Mais vous pouvez quand même activer le DANE pour les courriels que vous envoyez. Pour cela, il vous faut juste un résolveur validant le DNSSEC. En principe, c'est celui qui se trouve sur les serveurs de courriels. Parce que ce sont des machines qui fonctionnent bien, ce ne sont pas des téléphones ni des ordinateurs portables, donc ils peuvent avoir un résolveur local qui améliore la performance et qui vous permet d'exploiter ceci pour la validation. Beaucoup de MTA qui mettent en place le DANE qui ne font pas la validation par eux-mêmes. Ils s'appuient simplement sur les résolveurs locaux pour leur dire si oui ou non les enregistrements sont validés. Donc il faut qu'il y ait un chemin sécurisé, et donc c'est beaucoup plus simple si vous faites cela sur la même machine.

Donc les MTA, vous pouvez utiliser postfix XM. Cloudmark également qui propose des solutions aux FSI qui sont un petit

peu plus importantes que les petites MTA telle que postfix XM. Et il y en a d'autres. Il y en a d'autres qui vont arriver. Je sais qu'il y a des fournisseurs qui y travaillent.

Une fois que cela est fait, vous allez regarder les documents, vous mettez cela en route et en principe, cela fonctionne. Exactement comme Comcast et leur ancre de confiance négative, de temps à autre, il faut faire des ancres négatives de DANE, pour ainsi dire, des domaines à exclure parce qu'ils posent problème.

Parfois, il y a des gens qui se proposent pour entretenir certaines parties des noms de domaine. Alors n'hésitez pas à nous donner des informations s'il y a des problèmes de validation de noms de domaine. En principe, il n'y en a pas beaucoup mais bon, on peut avoir une liste d'exceptions à entretenir.

Alors la focalisation de cette présentation, c'est surtout le DANE à l'arrivée, donc les courriels qui arrivent. Alors la première chose à faire, c'est que votre MTA doit être compatible avec le STARTTLS. Donc assurez-vous que votre MTA est compatible avec STARTTLS.

Ensuite, vos enregistrements MX doivent être signés DNSSEC. Si vous avez un problème de sécurité, l'homme du milieu va rediriger votre courriel où il le souhaite et vous n'aurez pas de

sécurité de vos courriels, à moins que votre propre domaine soit signé.

Et ensuite, c'est encore plus intéressant parce qu'une fois que votre enregistrement MX est signé, si votre courriel est hébergé chez un fournisseur qui est autre que vous-même et qui s'occupe de votre serveur courriel, à ce moment-là, vous n'avez plus rien à faire. C'est à lui d'implémenter tout le reste du DANE. Les TLSA sont chez cet hébergeur, cet hôte MX.

Donc si vous gérez beaucoup de domaines, et bien vous n'avez qu'à signer vos domaines et la gestion des courriels, tout ce qui est relatif à la sécurité, est fait par votre fournisseur externe. Par contre, si c'est vous qui gérez vos courriels, vous êtes fournisseur et donc vous agissez de cette manière comme si vous étiez un fournisseur.

Alors le fournisseur publie deux types d'enregistrement TLSA. La certification en définit 24, dont 22 qui sont mauvais. Donc il y en a deux qui sont dignes d'être publiés. Premièrement, le 311 ; c'est un certificat qui s'appelle le DANE EE. Donc en fait, c'est le serveur « end entity », entité finale. Avec publication de la clé publique, vous dites : « Oui, mon serveur aura une clé publique précise. » L'alternative, c'est de dire : « Alors, je ne suis pas sûr que est le certificat que mon serveur aura, mais j'ai une ancre de confiance donc je vais publier le SHA256 hash, la clé publique

pour celui qui émettra mon certificat. Et vous pouvez aussi publier les deux.

Donc l'enregistrement TLSA, c'est donc 311 ou 211 ou alors, si vous ne m'écoutez pas, vous faites autre chose et vous vous trompez. Alors le reste des enregistrements, c'est la valeur « hash ». Donc c'est là que vous dites quelle est votre clé publique, le reste de l'enregistrement. Donc vous regardez le bas de la diapositive, OC72, ça commence par cela et ensuite, on termine par D3D6. Peut-être que cela a changé, je ne le sais pas. La dernière fois, quand j'ai vu, c'était cela.

Alors ensuite, comment gère-t-on les enregistrements TLSA ? Ce qu'il faut faire, c'est que les enregistrements TLSA soient dans le DNS avant que la chaîne de certificat soit déployée. Donc en fait, il y a beaucoup de cache dans le TLSA entre le résolveur et les serveurs. Et aussi, entre les serveurs faisant autorité, il y a cache avec les serveurs esclaves et la zone maître.

Et il y a en fait un gros retard entre le moment où vous faites votre modification, votre mise à jour, et le moment où les clients commencent à voir ceci par rapport à ce que vous aviez avant. Et donc l'enregistrement TLSA qui dit : « J'ai tel certificat. » doit être en place pendant un certain temps pour que le certificat soit activé. Et au moment de l'activation, les clients verront ce certification, ils regarderont l'enregistrement TLSA, ils verront

donc quelque chose de relativement récent et ils diront : « Ah, c'est bon, le certificat est bon. »

Alors heureusement, nous n'avons pas de problème de synchronisation. C'est impossible étant donné le cache DNS. Nous pouvons publier plusieurs enregistrements TLSA, certains fonctionnent maintenant, certains fonctionneront à l'avenir. Et en fait, on n'a pas besoin d'avoir une correspondance exacte de tous les TLSA ; il suffit uniquement d'une seule correspondance de TLSA. Donc on publie les clés très à l'avance, on s'assure qu'au moins un des enregistrements TLSA correspond soit à la clé actuelle, soit à la clé qui va bientôt être actuelle.

Alors il y a deux choses. Je recommande la première. Vous publiez deux enregistrements TLSA qui, tous les deux, correspondent à la clé publique : un la clé actuelle et l'autre, la clé suivante qui arrivera lorsque vous roulerez votre certificat. L'autre modèle que je recommande, c'est de publier deux clés : une pour votre serveur et l'autre pour le CA émis, alors actuel et avenir, donc une clé maintenant et une clé à l'avenir.

Alors que fait-on pour ne pas perdre la tête dans tout cela ? Donc la rotation des clés, elle se fait à peu près à tous les 90 jours. Mais il n'est pas bon de devoir passer par différentes étapes dans l'ordre trois à quatre fois pendant les 90 jours, se souvenir

de tout ce qu'il faut faire, etc., attendre et passer à la suite. Non. Il faut avoir un seul cycle de modifications en 90 jours.

Pour simplifier, vous générez la prochaine clé le jour même où vous déployez la clé actuelle. Donc admettons qu'on est au jour zéro, j'ai déployé la clé actuelle mais j'ai également généré la clé que je vais utiliser dans 90 jours. Donc ma clé privée, je la garde hors ligne mais tant que je peux avoir la valeur de la clé publique, et bien je peux déployer à la fois la chaîne de nouveau certificat et publier l'enregistrement de TLSA avec la clé que j'aurai dans 90 jours.

Donc sur la diapositive, vous voyez deux enregistrements de TLSA avec la clé actuelle que j'ai mise en route et ensuite, la clé suivante. Après, au bout de plusieurs semaines, mois, années – et d'ailleurs, je vous recommande de le faire souvent parce que c'est plus pratique de débugger plutôt que de faire cela tous les trois à cinq ans parce que là, vous ne saurez pas si vous faites une erreur.

Donc lorsque le moment est venu de faire la maintenance, vous obtenez un certificat de la clé pré-générée et c'est facile. Vous savez, vous signez un CSR, c'est facile à faire. Vous obtenez un nouveau certificat CA. Mais avant même de penser à obtenir un certificat et de le déployer, assurez-vous que l'enregistrement TLSA correspond à la clé qui est en place. En principe, ce devrait

être bon depuis longtemps. Et cette vérification vous permettra de ne pas avoir de problème. Vous ne déploierez jamais de certificat sans enregistrement TLSA déjà là depuis longtemps. Une fois que vous l'aurez fait, vous déployez votre certificat et vous revenez à la première étape pour générer la clé suivante. Et avec ce type de processus, vous vous assurez de ne pas être sous-pression à la dernière minute parce que vous avez déjà fait le travail. Donc cela fonctionne très bien et cela fonctionne même avec le chiffrement. Donc voilà, c'était le premier modèle.

Deuxième modèle, au lieu d'avoir la clé actuelle pour le serveur et la clé suivante, vous avez la clé actuelle et la clé actuelle pour votre CA. Donc selon ce modèle on publie les deux. Et s'il y en a un qui vérifie, c'est bon, cela suffit. Et quand le moment est venu de faire le roulement, tant que le CA reste le même, et bien vous pouvez utiliser une nouvelle clé qui ne correspond pas nécessairement au 311. Cela continuera de fonctionner parce que vous êtes avec le même CA. Et ensuite, vous vous assurez que l'enregistrement 211 correspond. Une fois que tout fonctionne, vous pouvez donc passer à l'enregistrement 311 après avoir déployé le certificat.

Ce modèle, en fait, vous permet, si vous êtes toujours un petit peu en retard, si vous déployez les choses à la dernière minute, de mettre à jour l'enregistrement 311. Par contre, si à un moment ou à un autre, votre CA décide d'utiliser un nouveau

certificat, une nouvelle clé publique, et bien à ce moment-là uniquement, vous vous assurez d'avoir obtenu un nouveau CA de la nouvelle clé publique, un certificat avec la même clé que celle que vous avez utilisée avant. Donc vous entretenez cette continuité. Donc le 211 changera mais le 311 sera le même. Donc en fait, vous sautez de l'un à l'autre. Donc vous en gardez un et vous changiez l'autre. Tant que vous avez une certaine discipline dans tout ceci, le processus est relativement simple.

Bien sûr, tout processus que vous faites régulièrement est sujet à l'erreur humaine. Si vous lisez différents enregistrements, si par exemple vous êtes fournisseur de services, il faut vraiment qu'il y ait quelqu'un qui automatise le système, il ne faut pas que ce soit fait manuellement. Malheureusement, je ne peux pas vous dire comme déployer le certificat parce que vous savez, le stockage, le déploiement, dépend des cas. Et différents serveurs faisant autorité ont différents mécanismes d'intégrations des données. Et donc je parlerai peut-être des scriptes à un moment ou à un autre mais pour l'instant, l'automatisation, c'est un petit peu quelque chose qui dépend des différents sites pour l'instant.

Si vous déployez les enregistrements TLSA et le DANE, il faut que vous ayez des coordonnées qui fonctionnent dans le WHOIS, SOA, postmasters. De temps à autre, les gens pourront vous envoyer des courriels et vous contacteront par rapport à cela. Et

de temps à autre, j'ai du mal pour trouver les bonnes coordonnées pour les personnes.

Surveillance. Comment surveiller le DANE. Je le fais actuellement mais je ne peux pas surveiller les systèmes au niveau mondial. Donc c'est à vous de surveiller votre propre DANE et vous assurer qu'il fonctionne correctement.

Voilà une liste des meilleures pratiques pour DANE. Ne pas utiliser STARTTLS en même temps... Voyez toutes les meilleures pratiques.

Comment déployer DANE ? Il y a des logiciels, Postfix, Exim, Cloudmark. Si vous le faites pour vous, je recommande mailinabox.email. Ils vous donnent tout un kit que vous pouvez utiliser pour intégrer toutes les fonctionnalités. Vous pouvez déléguer. Il y a tous les exemples qu'il vous faut et tous les détails y sont inclus, antivirus, etc. C'est un excellent logiciel. Si vous êtes un développeur, vous pouvez utiliser OpenSSL pour utiliser également les bibliothèques que vérification. Si vous utilisez GnuTLS, vous pouvez le faire, mais il y a certaines mises en garde donc je ne le recommande pas forcément. Contactez-moi si vous voulez développer quelque chose qui utiliser GnuTLS. Et si vous êtes responsable de la maintenance ou que vous allez écrire des logiciels lié à DANE, également, contactez-moi.

Voilà une liste d'outils DANE. Vous avez les sites, vous pouvez tester votre propre domaine. Il y a une liste d'utilisateurs où l'on publie des statistiques mensuelles. Vous voyez, donc vous pouvez cliquer sur ces liens. Vous avez différentes informations. Il y a un validateur que vous pouvez utiliser pour tester votre propre DANE ou bien vous pouvez le faire vous-même avec un scripte partagé. J'en ai un exemple à vous donner si cela vous intéresse.

J'ai deux minutes pour vous parler de mon enquête. J'ai lancé une enquête qui couvre certains domaines qui utilisent le DANE ; 5,2 millions de domaines sont signés DNSSEC actuellement, 178 000 domaines ont DANE SMTP. Voyez donc les pourcentages de gens qui peuvent avoir des problèmes et ce pourcentage est assez faible. Je n'ai pas encore réussi à parler avec eux, mais vous voyez ici la croissance dans l'adoption de DANE au fil du temps. Nous avons beaucoup d'organisations qui adoptent cette solution. Et c'est une croissance qui se poursuit de manière soutenue.

Voilà quelques domaines. Comcast figure sur cette liste. Vous voyez qu'il y a toute une liste de domaines qui ont adopté DANE, .org, etc. Bien sûr, il y en a plus mais voilà ceux qui l'utilisent de manière permanente.

Ici, vous voyez des fournisseurs qui hébergent des domaines qui appliquent DANE. Mais l'hôte du courriel ne déploie pas forcément DANE. Vous voyez, ces fournisseurs, si vous faites partie de ces fournisseurs, vous pouvez avoir une influence pour encourager l'utilisation de DANE. Vous voyez qu'il y en a un grand nombre qui sont signés déjà DNSSEC. Il y a une grande population de domaines qui se retrouvent dans ce cas de figure.

Google passe de google.com à googlemail.com. Et faire le DNSSEC pour googlemail.com devrait être assez simple. Et donc je suis optimiste et je pense que si on a de plus en plus de domaines qui sont hébergés sous googlemail.com, nous pourrons voir des progrès positifs.

Très bien. Et ici, j'aurai besoin de votre aide. J'aimerais pouvoir surveiller plus de ccTLD qui travaillent avec des fichiers de zone partagés. J'aimerais avoir plus d'informations là-dessus. J'aimerais également que les gens puissent apporter une solution aux problèmes liés au déni d'existence.

Essayez de mettre en route DANE outbound, y compris si votre domaine n'est pas signé parce qu'autrement, ce problème apparaît très vite et j'aimerais bien notifier du problème. S'il vous plaît, mettez en route DNSSEC et DANE si vous hébergez des serveurs MX. Et bien sûr, j'aimerais parler aux gens de GoDaddy qui hébergent énormément de domaines. Il y a très

peu de ces domaines qui sont signés et ce serait génial si GoDaddy pouvait signer pour tous les domaines qu'il héberge.

Annexe, je ne vais pas en parler.

Est-ce qu'il y a des questions ou je n'ai pas le temps pour les questions ?

RUSS MUNDY : Désolé Viktor. Merci beaucoup de cette présentation. Je pense que peut-être que les gens pourront vous poser des questions dans les couloirs s'ils vous retrouvent. Merci beaucoup. On n'a pas de temps pour des questions.

Warren, est-ce que vous pouvez nous rejoindre ? Cathy a les diapositives. Très bien.

Maintenant, nous aurons le panel le plus enthousiaste de la journée si vous voulez, le plus intéressant de la journée. Je suis sûr que tous les gens de la salle sont au courant des plans de roulement de la KSK qui avaient été mis en place et qui ont été reportés. Il y a tout un ensemble d'activités en cours à ce stade. Matt va nous faire une présentation par rapport à cela. Et ensuite, nous allons avoir une discussion avec les gens qui sont autour de la table, Joe, Warren, Jacques. Donc Matt, vous avez la parole.

MATT LARSON : Merci Russ. Bonjour. C'est la même diapositive que je vais présenter dans quelques heures dans la salle principale. Nous avons une présentation par rapport à cela. Je vais passer ce sujet en revue un peu rapidement parce que vous êtes au courant de la plupart de ces questions. Je vais donc être assez bref. Si vous pensez qu'il y a des éléments qui manquent, n'hésitez pas à me le dire ou à m'envoyer un courriel. Je vais faire un récapitulatif de où nous en sommes.

En septembre de l'année dernière, nous avons reporté le roulement de la KSK après avoir analysé les rapports de l'ancre de confiance à partir du RFC 8145. Et après cette analyse du le département OCTO de l'ICANN, nous avons identifié différents pourcentages en fonction des données. Mais on a identifié qu'il y avait beaucoup de serveurs qui n'avaient pas encore la nouvelle clé. Nous ne savions pas ce qu'il fallait anticiper, mais on trouvait que les pourcentages étaient assez élevés et nous ne savions pas pourquoi on avait obtenu ces valeurs de pourcentage et nous voulions investiguer.

Donc nous avons lancé des enquêtes. Il y a une personne dans cette salle qui a fait partie de ces enquêtes. Nous avons essayé de contacter 500 résolveurs qui avaient donc l'ancienne clé en septembre 2017. On n'a pas été surpris de la difficulté que cela

représentait de pouvoir contacter ces opérateurs basés sur IP. Nous avons pu contacter seulement 20 % de ces serveurs. Et parmi ceux-ci, nous avons vu que 60 % avaient des adresses avec des IP dynamiques et 25 %, c'était des résolveurs qui transmettaient des requêtes venant d'autres résolveurs.

Maintenant, nous aurions voulu trouver des causes pour pouvoir relayer les messages appropriés. Mais ce n'est pas ce que nous avons découvert. Alors nous avons décidé de parler à la communauté et de demander à la communauté des orientations par rapport aux étapes à suivre. Cela s'est passé en janvier. En décembre, on a annoncé le report et en janvier, on a demandé l'avis de la communauté par rapport aux étapes à suivre.

On était d'accord sur le fait qu'on n'avait pas moyen de mesurer les chiffres de manière exacte. Ce que l'équipe qui avait conçu le RFC il y a quelques années nous a conseillé, c'est de continuer à essayer de mesurer parce que finalement, les utilisateurs pourraient être affectés. Et toutes ces discussions nous ont amenés à la conclusion de savoir que ce serait difficile de mesurer avec exactitude en ce moment. Alors par consensus, il a été dit que l'ICANN devrait rouler la clé KSK.

En février 2018, on a publié un projet préliminaire – j'insiste, c'était un projet préliminaire – pour que le roulement de la clé ait lieu le 11 octobre 2018. Il n'y avait pas des critères de mesure

explicites découlant de cette discussion avec la communauté, mais nous allons publier des données concernant le RFC 8145 de manière périodique pour voir comment cela évolue.

Il y a eu une période de commentaires publics ouverte. On a encore le temps de faire des commentaires, elle va fermer le 2 avril 2018. Et j'encourage tout le monde à y participer car la façon dont nous allons procéder dépend des résultats de la consultation publique.

Voilà un récapitulatif pour savoir ou nous sommes. En mi-avril, nous allons publier le rapport du personnel sur la consultation publique. Si on regarde la date d'octobre, nous allons procéder comme l'indiquait la diapositive que je vous ai montrée.

Nous allons avoir un atelier en septembre où le Conseil d'Administration va demander au SSAC et au RSSAC de commenter le plan. Nous allons reprendre cette question au Panama et j'espère que nous allons pouvoir obtenir des réactions du RSSAC et du SSAC pour savoir si nous allons poursuivre avec la décision du Conseil d'Administration. Il y a des ateliers du Conseil d'Administration à chaque réunion de l'ICANN. Donc il y aura cet atelier du Conseil d'Administration en septembre et on va demander au Conseil d'Administration d'approuver une résolution pour autoriser ICANN org à rouler la clé.

Maintenant, je vais passer aux données. Nous avons petit à petit ajouté des données du RFC 8145 que nous obtenons de différents serveurs. Cette diapositive vous montre les derniers développements. Nous avons des données venant de 12, je crois, serveurs ; il y en a un qui ne participe pas. Et nous obtenons des statistiques à partir de DNSCAP ; on fait marcher DNSCAP toutes les 60 secondes à travers une requête DNS et nous obtenons ces informations que nous collectons.

Voilà le schéma ici dans ce graphique qui est un peu difficile à lire peut-être. Vous voyez la ligne rouge et verte, c'est le nombre d'adresses IP, unique source dont nous obtenons des rapports. Et la ligne verte est le nombre total de sources. Vous voyez que nous avons 50 000 sources par jour et vous voyez donc que le résultat, c'est la ligne noire qui nous donne le pourcentage. Vous voyez qu'on est à hauteur de 20 %, ce qui représente une amélioration par rapport aux données que nous avions obtenues au départ. Mais à un moment donné, il faut arrêter de faire des diapositives et commencer à faire des présentations aux réunions de l'ICANN et c'est ce que nous sommes en train de faire.

Voilà un petit peu d'informations. Nous sommes sûrs que les gens ont appliqué la mise à jour parce qu'il y avait des problèmes de sécurité. Il n'y a pas eu de drop-off après 30 jours parce qu'on voit encore qu'il y a des serveurs qui ont l'ancienne

clé après 30 jours. Je pense qu'on est face à des erreurs qui ne fonctionnent pas suffisamment longtemps pour pouvoir obtenir ces informations.

Vous voyez ici des données qui viennent de différents serveurs racine, à l'exception du serveur J ; nous n'obtenons pas de données du serveur J. Ici, nous avons les IP uniques qui sont ajoutées par jour. Voilà combien d'IP uniques que nous n'avons pas vues auparavant qui s'ajoutent au jour le jour. Nous voyons de plus en plus ce type de nouvelles adresses IP qui s'ajoutent. On peut imaginer que cela va nous amener à une situation plus stable. Que ce soit un conteneur ou non, on peut imaginer qu'on peut avoir tout type d'adresse IP qui peut nous expliquer pourquoi nous obtenons ce nombre d'adresses IP uniques par jour.

Ici, vous voyez les sources uniques au fil du temps. La ligne verte montre les sources uniques au fil du temps qui ont rapporté le RFC. Et si vous suivez vers la droite, il y a le nombre d'adresses uniques depuis que nous avons commencé à collecter des informations. Ces IP ont donc rapporté des informations à partir du RFC. Et ce pourcentage est encore pire.

Vous voyez donc les adresses uniques toutes les 24 secondes, le cumul au fil du temps. Et vous voyez qu'il n'y a pas beaucoup de

différences entre le nombre de sources que nous avons eues dans notre rapport.

Je vais dire cela autrement. Il y a peu d'évidences d'une mise à jour qui soit mise en place vers la nouvelle clé. Vous pouvez voir ces graphiques qui sont publiés à toutes les semaines, si vous cliquez sur le lien, vous allez voir.

Et c'est ma dernière diapositive, je peux publier la liste actuelle ; j'ai l'autorisation de l'ICANN pour le faire. Ce serait similaire à ce que vous voyez sur l'écran. Vous voyez, il y a différentes fréquences et le nombre de sources que nous recevons, le pays, etc. Donc il y a la possibilité pour nous de contacter certaines de ces sources. Nous avons un peu de temps avant de lancer le roulement.

Très bien. Je vais m'arrêter là pour que l'on puisse avoir suffisamment de temps d'échanger ou de débattre.

RUSS MUNDY : Merci beaucoup, merci Matt pour cette présentation. Il y a d'autres membres dans ce panel. Nous voulons avoir d'autres perspectives. Jacques Latour va nous en parler du point de vue des TLD.

JACQUES LATOUR : Les TLD dans notre pays sont une source d'inquiétude. J'ai suivi de près cette question et comme j'ai dit pendant mon commentaire, c'est qu'il est virtuellement impossible de mesurer cela. Il est virtuellement impossible de tracer une ligne sans qu'il y ait des dommages collatéraux. Si nous voulons vraiment maintenir cette confiance perçue vis-à-vis de la racine, il faut le faire de manière prudente parce que s'il y a une panne, les gens vont pouvoir le résoudre facilement. Il ne va pas se passer des mois ou des semaines pour que l'on puisse résoudre cela. La façon de résoudre est assez facile.

Mais à mon avis, plus on retardera cela, plus on passera du temps à analyser ce processus, plus l'impact sera grand. Tous les processus pour créer cela sont impeccables, cérémonie de signature, etc. Donc si on reporte davantage cela, finalement, cela va aller à l'encontre de la confiance que les gens ont dans le système.

Nous devrions rouler la clé l'année prochaine. Cela devrait être roulé tous les ans. Et donc si un jour il nous faire un roulement de clé d'urgence, il n'y aura pas de problème, il n'y aura pas de risque.

Ensuite, on peut utiliser DANE dans les grandes entreprises et c'est le CA central, tout cela dépend de la clé que nous voulons construire. Alors je pense qu'il faut le faire et faire avec, et

éventuellement dire : « Voilà la façon de résoudre le problème. » s'il y en a un. Si quelqu'un va dans le DNS, il faut qu'il puisse trouver aussi la solution, et c'est ce qu'il faut faire. Mais si l'on attend davantage, cela n'aura pas des conséquences positives.

RUSS MUNDY : Merci Jacques.

Alors maintenant, Joe. On va avoir la perspective plus large d'un grand FSI.

JOE CROWE : Je suis d'accord par rapport à cette question, on pourrait faire cela tous les ans parce que dans une grande entreprise, on pourrait avoir des problèmes. Nous ne voulons pas éteindre la validation DNSSEC. Et lorsque le premier roulement de clé a été fait, on a validé, on l'a testé pendant des mois pour s'assurer qu'on était conforme au 5011. Peut-être qu'on n'utilise pas le 5011 et qu'on se repose surtout sur le résolveur mais s'il y avait eu un problème, on aurait été là.

Donc si on a l'automatisation avec un roulement tous les ans et si le processus s'améliore au fil du temps, et bien cela veut dire qu'il y a moins de charges de travail sur les opérateurs. Mais la clé de la réussite, à mon avis, dans tout ceci, c'est de tester et de

continuer de tester et aussi de s'assurer que tout est à jour. En tout cas, c'est ce que je suggère.

RUSS MUNDY : Merci Joe.

Et maintenant, on va écouter Warren du point de vue d'un grand résolveur public, que nous connaissons tous. Warren.

WARREN KUMARI : Oui, bonjour. Je représente Google. Je n'ai pas énormément de choses à ajouter là-dessus. Mais il est clair que nous avons un logiciel custom. Nous n'utilisons pas le RFC 5011 parce que c'est très complexe. C'est bien pour les systèmes automatisés mais nous, ce que nous utilisons, c'est en fait une équipe nombreuse. Lorsqu'il y a publication, on vérifie, on l'importe manuellement dans un cluster canari et ensuite, on fait le roulement de clé manuellement.

Il y a un certain nombre d'entre nous qui avons discuté – pas à Google mais ici – du RFC 5011 et du roulement de clé et à savoir si c'était adapté. Peut-être qu'il y aurait une meilleure solution, je ne sais pas. Mais je ne vais pas ajouter de commentaires, j'ai simplement des questions pour Matt mais ce sera pour tout à l'heure quand on passera à la partie questions et réponses.

RUSS MUNDY : Merci Warren. Joe, Jacques également, merci, Matt aussi. Et maintenant, c'est justement le moment de poser vos questions. Et puisque Warren a le micro et qu'il a une question, je vais lui passer la parole. N'hésitez pas à lever la main si vous avez une question.

WARREN KUMARI : On va retourner en arrière, s'il vous plaît, sur les diapositives. Alors je ne sais pas si je comprends. Peut-être que j'ai mal compris mais donc l'idée de base, c'était qu'il y avait une mise à niveau de l'unbound. Mais je ne vois pas pourquoi vous avez toutes ces sources uniques. Vous êtes passés du RFC 8145 qui n'était pas fait et qui maintenant est fait ?

PETER KOCH : Je suis désolé d'être derrière vous, mais j'ai quelques questions. Tout d'abord, j'ai une remarque pour Matt parce qu'il y a des rumeurs cette semaine comme quoi... Je voudrais savoir ce qui pourrait se passer si le roulement était repoussé. Est-ce que vous pourriez clarifier ? Si on reportait encore le roulement de clé, est-ce que l'internet s'arrêterait ? J'espère que non.

MATT LARSON : Je ne pense pas que retarder le roulement arrêterait l'internet. Il n'y a rien qui s'arrêtera.

PETER KOCH : Je voulais juste clarifier parce qu'il y a des personnes qui ont l'impression que le roulement était urgent, qu'il fallait absolument qu'il se passe. J'aimerais que ce soit enregistré et que ce soit clair là-dessus.

MATT LARSON : Il est tout à fait possible que les commentaires de la communauté insistent pour qu'on arrête le processus jusqu'à ce qu'il y ait davantage de développement, qu'on revoir le plan à ce moment-là et qu'on repousse encore. C'est tout à fait possible.

WARREN KUMARI : Je crois que le gros souci, c'est que lorsque la clé a été signée au début, on s'est dit que le roulement sera au bout de cinq ans. Et puis pour diverses raisons, la transition, NTIA, etc., on a dû reporter ceci.

Donc le risque principal, c'est en fait la perte de confiance dans le roulement de clé avec le temps. Et donc je crois que la question à se poser, c'est de savoir est-ce que c'est plus risqué pour nous de rouler et peut-être de voir certaines interruption,

ou alors de ne pas rouler et puis les gens vont commencer à se dire : « Ça commence à sentir mauvais. » ? Et donc c'est pour cela que la période de consultation publique est ouverte. Et donc il faut absolument que les gens fassent des commentaires. Encouragez-les, c'est important.

JOE ABLEY : Alors quelques commentaires que j'ai entendus. Il ne faut pas faire d'erreur sur cette équation du risque. Est-ce qu'on roule la clé parce que c'est risqué ? Attention parce que de ne pas la rouler, c'est également risqué. Dans tout système, la possibilité de remplacer une clé va de paire avec les précautions en matière de sécurité physique ; la sécurité physique n'est jamais parfaite. Ce n'est pas noir et blanc, il faut toujours évaluer ; il y a toujours des zones grises. Donc l'équilibre des risques avec ce manque d'expérience par rapport au roulement de la clé, qui est une clé importante, je crois que c'est un risque assez mineur. Je pense qu'il y aura peut-être de brèves interruptions sur des réseaux mineurs mais après, il y aura réparation assez rapidement.

Donc je crois que le risque de ne pas rouler la clé, c'est qu'on ne saura pas faire. Et si on est forcés de le faire, cela va vraiment être la pagaille.

WARREN KUMARI : Oui, je suis tout à fait d'accord avec Joe mais quand même, s'il faut rouler la clé en situation d'urgence, le processus est totalement différent de celui qui a été décrit. Si on est pressés, c'est peut-être parce qu'on a manqué de confiance dans la clé. Dans ce cas-là, on ne peut pas utiliser le 5011 parce qu'on ne peut pas faire confiance au 5011.

Donc à la base, l'espoir, c'était de publier le DURZ et ensuite, de rouler la clé pour tester et ensuite, tous les deux ans passer à une autre test de la clé. Mais pour diverses raisons, on n'a pas pu le faire. Donc oui, effectivement, le premier roulement, cela va être compliqué. Et le pauvre Peter est responsable de tout cela.

MATT LARSON : Par rapport aux partenaires de gestion qui s'en sont occupés en 2010, l'intention n'a jamais été de rouler comme vous venez de le décrire. Il y a des gens dans la communauté qui ont poussé pour qu'on fasse différents roulements, mais cela n'a jamais été le cas au début. Le DPS a dit que la pratique dit pour le KSK au bout de cinq ans, mais pas cinq ans et après, six ans et sept ans.

ORATEUR NON-IDENTIFIÉ : Matt, est-ce que vous pouvez passer à la liste des AS ? Donc en haut, 41 462 sources, 55836. Donc le nombre de visibilité à ce niveau-là de validation DNSSEC, c'est pratiquement zéro. Donc

qu'est-ce que cela veut dire en fait ? Ce qui nous arrive du RFC 8145 est vraiment tordu. Et nous ne comprenons pas tout. En septembre de l'année dernière, on s'est dit : « Bon, on ne comprend pas. » Mais d'une certaine manière, ce n'est pas l'appétit pour le risque qui a changé. La confiance dans le signal RFC 8145 s'érode. Et cela, ce sont des données qui ne représentent pas les résolveurs validants. Et si vous ne validez pas, et bien peu importe le roulement de clé. Les résolveurs validants qui regardent les publicités Google voient ceci. Dans mon cas, c'est ce que j'utilise.

ORATEUR NON-IDENTIFIÉ : Mais vous avez dit que cela reflète l'environnement large. Et s'il y a un ensemble de validations qui ne voit pas, c'est d'autant plus étrange et inexplicable. Donc d'une certaine manière, ce que je vous discussion, ce n'est pas que notre appétit pour le risque a changé mais que notre confiance dans le signal RFC 8145 commence à s'éroder de plus en plus. Et cela fait sept ans qu'on travaille à ce roulement de clé. On pourrait passer encore sept ans là-dessus mais de toute évidence, je ne vois vraiment pas pourquoi. Parce qu'à un moment ou à un autre, on va avoir un évènement qui provoquera le roulement, ce sera le premier roulement, on n'aura pas prévu pour ce genre de situation et on va avoir d'énormes problèmes. Moi, je vous encourage vraiment – et c'est un feedback que je vous fais – de faire le roulement tel

que vous l'avez prévu. Et je vous encourage aussi – parce que cela, c'est la conversation suivante – de le faire de manière régulière. Et s'il n'y a pas de régularité qui a été mise en place, je pense que 12 mois, c'est peut-être bien. Et tout cas, je vous encourage vivement à rouler, à rouler cette année et à continuer de le faire chaque année en octobre.

PETER KOCH : Question suivante. La première question, c'était les autres qui étaient perdus. Là, c'est moi qui suis perdu. Les gens disent qu'il faut qu'il y ait des règles régulières et il y a un des avantages, c'est donc que cela aiderait d'avoir un mécanisme en place pour le roulement de clé au cas où on ait besoin d'un roulement en urgence.

Mais si je comprends bien, le 5011 est incompatible avec le roulement en urgence. Je vois que vous hochez de la tête, personne ne vous entend.

ORATEUR NON-IDENTIFIÉ : Je crois que nous sommes tous d'accord. Warren et moi, on a commencé à réfléchir à cela par rapport au 5011 et il faut faire quelque chose.

PETER KOCH : Pour les roulements réguliers il faut une autre explication ?

ORATEUR NON-IDENTIFIÉ : Il faut remplacer le 5011.

PETER KOCH : Mais ce sont deux questions différentes. S'il faut en parler aux opérateurs de résolveurs qui ne sont pas dans la salle et qui ne passent pas toute la journée à y travailler, quel est l'objectif du roulement régulier ? Parce que pour se préparer en cas d'urgence... en fait, ce n'est pas ce qui motive le travail.

MATT LARSON : Alors un petit déni de responsabilité, je ne fais pas partie de la PTI, je fais partie du bureau technologie.

Alors à long terme, tous, on pourra s'aventurer et dire qu'à l'ICANN, on a un autre système, on n'est pas obligé de compter sur la méthodologie actuelle avec le calendrier de roulement régulier. Moi, j'aimerais avoir des clés de standby dans l'apex. Les clés actuelles, tout ce qu'on peut faire pour générer une autre clé avec l'infrastructure qu'on a actuellement veut dire qu'il y aura partage avec la clé actuelle. Donc n'importe quel scénario, s'il y a compromission, on compromet les autres clés. Donc il faut trouver d'autres clés dans l'ensemble de clés pour

pouvoir – ce sera un petit peu le luxe – rouler sans problème quand on veut.

Alors le 5011 a des problèmes en termes de taille de l'ensemble de clés apex. Donc je crois qu'il y a plusieurs choses à faire. Il y a le protocole et puis il y a l'opérationnel. Mais je crois qu'il y a moyen d'avoir des roulements réguliers, d'avoir également un plan en cas d'urgence et de faciliter le travail.

FEDERICO NEVES : Federico Neves de nic.br. Très bien, Matt. Merci pour cette présentation.

Je suis d'accord avec vous en dehors du fait que j'ai déjà fait un commentaire sur l'enregistrement public. Donc si je vais dans le sens de ce que vous avez dit, l'idée d'avoir des clés de rechange publiques, il faut qu'on pense à un roulement d'algorithmes parce qu'on a des clés de rechange et l'algorithme actuel, avec la taille des clés qu'on utilise actuellement, fait qu'il faut y réfléchir, utiliser la technologie actuelle avec ces clés publiques plus petites.

WARREN KUMARI : Alors j'aimerais répondre à la question de Peter. Il y a deux types de roulement de clé en urgence. Il y a le roulement de clé où

quelqu'un publie accidentellement la clé sur le New York Times. Alors là, panique générale et là, le 5011 ne fonctionne pas.

Il y a un autre roulement de clé en urgence où il devient de plus en plus clair que ce que vous utilisez n'est pas aussi solide que vous ne le pensiez. Certaines personnes vont dire : « Oui, c'est ce qui se passe pour le SHA1, par exemple. » Vous les roulez, donc peut-être je ne sais pas, quelques semaines, quelques mois. Donc suivant votre niveau d'urgence, le 5011 peut marcher ou non.

Ensuite, commentaire suivant. On a parlé d'un autre système pour les roulements de clés, donc s'éloigner du RFC 5011. Pour cela, on pourrait avoir des clés en stand by qui ne seraient pas publiées à l'apex. On pourrait publier des clés en plus comme enregistrement, mais sans signer en fait quoi que ce soit, donc pas dans l'ensemble de clés DNSSEC. Mais ce serait en fait un enregistrement en plus. Vous dites : « J'ai sept clés, voici la liste. Allez voir les deux noms qui pointent vers la clé publique. » Comme cela, on pourrait faire un roulement. Mais de toute façon, il faudrait faire ce roulement.

BENEDICT ADDIS : Bonjour, Matt. Je suis très heureux d'être ici, de vous avoir écouté.

Alors un petit rappel. Les serveurs shadow peuvent notifier, peuvent informer ces opérateurs de réseau – je voulais juste le rappeler – s'ils souhaitent recevoir des alertes par rapport à ce type de problème, même si ces alertes savent que le résolveur fait quelque chose de bizarre plutôt que de dire qu'ils ont la clé 2010 et qu'ils sont prêts à aider. Mais il semblerait que 30 à 50 % des ASN souhaitent recevoir ceci.

MATT LARSON : Merci, c'est une très bonne idée. Je sais qu'on a échangé des courriels avec les serveurs shadow.

Alors je n'ai pas mis ceci sur la diapositive mais autre tactique, c'est d'aller dans l'autre sens, de trouver ceux qui en font beaucoup – et nous avons de bonne données d'APNIC là-dessus – et de commencer par le haut et de vérifier que les personnes qui ont beaucoup d'observateurs soient prêtes et qui ne font pas le DNSSEC de manière à cocher et à se dire : « Bon, on ne sait pas qui n'est pas prêt mais on sait qui est prêt. » Et ceux qui sont prêts, c'est un pourcentage que l'on peut utiliser. Donc si vous voulez bien nous aider avec cela, c'est bien.

RUSS MUNDY : Je pense que nous n'avons pratiquement plus de temps, à moins qu'il n'y ait une dernière question, vraiment, qui vous brûle les lèvres. Allez-y.

ORATEUR NON-IDENTIFIÉ : Je suis boursier ICANN et j'ai quelques questions de base. Quel est le rôle des anciennes clés dans le roulement ? Est-ce qu'elles servent à valider les anciennes clés ? Et si c'est le cas, qu'est-ce qui se passe s'il y en a une qui est compromise ? Et si c'est le cas encore une fois, quelle est l'atténuation des risques ? Quel est le plan ?

WARREN KUMARI : Alors le protocole actuel, donc le RFC 5011, c'est que donc l'ancienne clé signe la nouvelle clé. Donc si vous faites confiance à l'ancienne clé, vous pouvez faire confiance à la nouvelle clé. Et après, vous dites, vous pouvez oublier l'ancienne clé. Donc l'ancienne clé, vous ne lui faites plus confiance après. Mais si l'ancienne clé est compromise ou si vous perdez foi en cette clé, vous ne pouvez plus l'utiliser.

Donc il y a un autre processus – et je ne suis pas sûr si c'est quelque chose qui est très connu, très public – c'est donc de savoir s'il y a compromission et s'il y a des preuves de cette compromission de l'ancienne clé. Il peut y avoir peut-être une

séance d'urgence pour générer de nouvelles KSK, etc., mais la distribution de cette clé, la publication de cette clé, comment savoir si on peut faire confiance, cela, si c'est signé par un CA, je ne sais pas si c'est une bonne réponse en fait.

Donc il faut qu'il y ait une bonne documentation, un processus de tests pour savoir si la clé a effectivement été compromise, donc pour savoir ce que l'on fait.

RUSS MUNDY : Ceci étant, je pense que nous allons maintenant clore la séance et quitter la salle. Mais je souhaitais vraiment remercier Matt, Larson, Joe Crowe, Jacques Latour et Warren pour leur participation à ce panel. Et en particulier, nous devons remercier Kathy Schnitt qui a organisé cette séance toute seule. En principe, il y a toujours deux autres personnes mais vous avez fait un excellent travail, Kathy. Donc merci pour cette organisation excellente. Voilà.

Notre programme sera réorganisé à l'ICANN62. Dans un mois ou deux, nous enverrons des requêtes pour des présentations. Donc n'hésitez pas à réfléchir à vos idées pour la suite. Et j'espère qu'on se retrouvera donc dans quelques mois au prochain atelier. Merci.

[FIN DE LA TRANSCRIPTION]