COPENHAGUE – Atelier sur les DNSSEC - 1e partie
Mercredi 15 mars 2017 – 09h00 à 10h30 CET
ICANN58 | Copenhague, Danemark

INTERVENANT NON IDENTIFIÉ : […] logistiques importantes. Et donc, je vous demande de m'écouter. Surtout si vous voulez manger à midi. Alors, à vos tables, vous devez avoir un petit billet, sinon, dites-moi. À moi ou à Kathy. Et il y a une petite carte derrière, si vous souhaitez la suivre. En tout cas, moi j'en ai besoin. Donc, ne me demandez pas où aller.

Quoi qu'il en soit, donc, on mange de l'autre côté du couloir, dans le coin. Par ailleurs, il y a une pause optionnelle, de 10 h 30 à 11 heures. Nous allons donc, lors de cette pause, en fait, continuer de travailler, parce que nous avons beaucoup de choses à faire. Mais vous pouvez tout à fait vous lever, aller prendre du café, de l'eau, etc. si vous voulez donc faire une pause à ce moment-là.

Je vais maintenant passer la parole à Dan York qui va donc nous aider à commencer notre travail.

DAN YORK : Bonjour. Comment ça va, tout le monde ? Allez. Bonjour. Voilà. Attendez ! La matinée est belle. Alors ils sont en train d'essayer de me trouver dans la caméra. Non. De l'autre côté. Voilà. Je vais laisser de ce côté. Regardez, la caméra me suit. C'est magnifique.

Non. Non. Non. Elle remonte. Elle redescend. Ah ! Salut, les gens à distance. Je sais qu'il y a des gens qui vont nous rejoindre à distance. Alors bonjour à tous. Nous avons beaucoup de choses à faire aujourd'hui. Comme Julie l'a dit, nous allons travailler donc pendant la pause.

Alors, est-ce que Matt Larson est là ? Non. C'est lui qui sera la victime de la pause. Donc si vous voulez vous lever, vous pouvez–

Est-ce que vous connaissez le roulement de la KSK ? Matt en a parlé hier, mais je pense qu'il aura peut-être des nouveautés, des choses nouvelles à vous apprendre. En tout cas, il y a un certain nombre de personnes qui sont là. Combien d'entre vous êtes nouveaux à cet atelier DNSSEC ? Il y en a quelques-uns. Très bien. Bienvenue.

Non. Vous, vous ne comptez pas.

Alors, voyons où nous en sommes. Cette séance vous est présentée par un comité de programme. Combien il y en a qui

sont dans la salle de ce comité ? Donc vous pouvez, en fait, accusé ces personnes-là si vous n'êtes pas contents. Sinon, si vous êtes intéressés , il y aura un autre atelier DNSSEC abrégé, en fait, lors de la séance de Johannesburg. Donc ce sera un petit peu une journée technique comme la dernière fois.

Donc si vous voulez montrer vos recherches à la communauté, si vous voulez que la communauté sache un petit peu ce que vous avez fait, et bien, il y aura un appel à proposition après notre séance d'aujourd'hui. Et sinon, et il y aura un autre également à Abu Dhabi, en novembre. Ou octobre, je ne sais pas exactement.

Donc voilà les personnes avec lesquelles nous allons travailler. Nous voulons également remercier ces trois sociétés : je vois Jim d'Afilias qui est là, Jacques de [CIRA], et Christian de SIDN. Donc on les remercie. C'est grâce à eux qu'on pourra manger ici et qu'on pourra continuer notre travail. Et je cherche un quatrième sponsor pour les prochains ateliers donc n'hésitez pas à venir me voir si cela vous intéresse. Ça ne coûte pas cher et vous pouvez nous aider en plus. Donc c'est génial.

Alors, ça, c'est une photo d'hier soir– Irwin, le voici, qui nous a donc accueillis du Danemark. On l'applaudit. C'est dommage, parce que cette photo nous l'avons prise à la fin. La majorité des gens était partie. On s'est dit ah zut ! Il nous faut une photo pour les transparents. Donc voilà. En fait, on était plutôt 30

personnes, mais il y en a pas mal qui était partis quand on a pris la photo.

On a une excellente discussion. Donc c'était très très bien. Merci Irwin de nous avoir accueillis. Et puis, pour Johannesburg, nous aurons besoin d'un sponsor. Même chose pour Abu Dhabi donc si cela vous intéresse, n'hésitez pas à nous le dire. C'est très intéressant de passer du temps ensemble à chaque fois.

Alors, voilà les activités qui sont soutenues par le SSAC ainsi que par l'Internet Society Deploy 360 Program. Donc voilà les deux entités. Alors, ça ne marche pas. Nous avons un problème technique. Ça y est. C'est bon. Alors voilà notre programme. Vous avez une copie en principe. Vous devez l'avoir. Donc vous avez–

Nous avons un panel sur ce qui se passe avec le DNSSEC en Europe. Je vous donnerai une petite mise à jour du point de vue de l'IETF. Si vous n'avez pas suivi ce qui s'est passé, nous avons ensuite Matt qui nous parlera du roulement de clé. Ensuite, nous avons un panel qui parlera de ce que nous faisons avec la validation des FSI en termes de roulement de clé. Donc que font les FSI pour se préparer.

Il y a également pour Paul Wouters qui nous fera une démonstration, donc, sur la sécurisation des e-mails. Paul et ensuite Vittorio qui nous parlera des échanges ouverts, et

Roland, également, qui nous parlera du déploiement ECDSA. Ah ! Vous allez changer de place. D'accord. Vous êtes assis ici. Donc Roland, ECDSA. Et également, la personne qui est là-bas, je ne sais pas si vous connaissez donc l'ECDSA, mais on en parlera.

Ensuite, Wes. Wes avait d'autres réunions. Je ne sais pas s'il est là. Mais il parlera ; il nous fera un questionnaire sur le DNSSEC. Et [Mario] me disait, faut-il leur donner la réponse tout de suite à ce questionnaire. En fait, vous êtes tous invités à participer à cette activité qui sera très sympathique. Avec Wes.

Et ensuite, autre démonstration. Je ne sais pas ce que c'est. Mais c'est encore une fois une question de sécurisation et de chiffrement des e-mails. Ah ! Voici Paul. Donc voyons ce que nous faisons ensuite.

Alors, c'est vous qui allez pousser– qui allez appuyer sur le bouton, c'est ça ? Ça y est, ça marche. Merci. Il y a quelque chose qui s'est passé.

Alors, tout d'abord, les statistiques de déploiement. Je ne sais pas si vous avez vu le rapport sur le déploiement du DNSSEC. C'est un excellent rapport qui a été fait par un certain nombre de personnes qui sont présentes dans cette salle sur les statistiques, à savoir où en sommes-nous en matière de déploiement du DNSSEC. Donc je vais vous montrer un tout petit peu un aperçu général, mais je vous encourage à regarder ce

rapport, à le passer en revue. Parce qu'il vous explique un petit peu où nous en sommes actuellement en matière de déploiement.

À l'Internet Society, il y aura une mise à jour qui sera faite en 2017, avant Abu Dhabi, pour vous dire un petit peu où nous en sommes, quels sont les taux de croissance, etc.

Il faut peut-être que je me rapproche pour que ça fonctionne. Alors. Où en sommes-nous ? Donc voilà un petit peu le tableau de validation DNSSEC de Jeff Houston. Donc en fait, la situation est stable. Nous sommes 14 % - 15 % environ, au niveau mondial. Ça change suivant différentes régions. Regardez donc pour le monde, les différents chiffres que nous avons. Vous voyez un petit peu ce qui se passe. Alors, ce qui est important pour bien lire ce graphique, si vous regardez la première colonne, c'est le pourcentage de validation que Jeff voit, qui se passent dans ces régions. Et ici, Google PDNS. C'est donc le pourcentage de personne qui utilise le DNS public de Google.

Donc dans certains pays, le pourcentage est élevé. Cela veut donc dire que les FSI globaux font une validation Google. Mais dans des pays, comme vous voyez là, par exemple, en Europe de l'Ouest, on ne voit que 7 % d'utilisation du PDNS Google. Donc en fait, les FSI font eux-mêmes la validation au niveau local. Et

ça, c'est bien. C'est une bonne chose. Nous souhaitons que ceci soit localisé. Donc voilà ce qu'on a, au niveau mondial.

Et en ce qui concerne l'Europe, attendez. On revient en arrière. Voilà. Donc les îles Féroé, je ne sais plus où c'est d'ailleurs. Il faudra m'aider. C'est vers l'Islande, me semble-t-il. Nous ? On continue vers le nord, c'est ça ?

On a perdu en foot contre eux. C'est ça qui est important. Donc ils sont en haut des statistiques de Jeff Houston. Ils sont à 90 % de toutes les requêtes DNSSEC qui sortent des îles. Donc c'est leurs statistiques. Le Danemark est là. Très bien. Et encore une fois, la statistique et passe pour l'utilisation du PDNS de Google. Ça veut dire que les FSI dans cette région font beaucoup de validations. C'est bien.

Donc voilà pour la validation. On passe à la signature.

Rick ? C'est son graphique, donc si vous le voyez, vous pourrez le remercier pour son rapport. Alors je viens de me rendre compte que j'ai des interprètes. Je crois que je parle trop vite, en fait. Elles me disent oui. Ça y est. Je vais ralentir.

Ce rapport vous donne le nombre de domaines qui ont été signés. Et bien sûr que l'augmentation c'est avec tous les nouveaux gTLD qui ont été signés. Alors, passons maintenant à

la suivante. Là, vous avez le nombre de numéros qui ont été signés. Donc par rapport à la statistique de Rick. Donc le SIDN.

Alors, à chaque fois que je cherche quelqu'un, la personne a changé de place. Christian était avec Jacques, là. Qu'est-ce qui se passe ? Tous les Hollandais sont là. Alors le .nl a le chiffre le plus important de domaine que l'on voit : 2 500 000. Donc, ensuite le Brésil, et vous voyez le reste. Le .se, le .cz. André ? Il est là ? Il n'a pas changé de place.

Alors, ces chiffres, vous pouvez les obtenir du site de Rick. Alors si vous voulez obtenir ceci, tel que vous l'avez à l'écran, vous allez à droite. Signe total. Vous cliquez dessus et vous cliquez encore une fois, et à ce moment vous aurez toutes les informations organisées de cette manière.

Si vous regardez le graphique et vous voyez que votre pays n'est pas représenté, à ce moment-là, envoyez un e-mail à Rick et il travaillera avec vous pour l'incorporer. Rick souhaite justement ajouter des statistiques qui montrent les résultats.

Ensuite, ça, c'est pour les nouveaux gTLD. Donc on aime bien vous fournir cette statistique pour que vous sachiez un petit peu où nous en sommes, en termes de DNSSEC, pour les nouveaux gTLD. Le chiffre du haut, donc, c'est OVH. C'est un fournisseur qui signe ses domaines, qui vraiment se préoccupe de la sécurité. Donc voilà.

Ensuite alors je vais parler de nos cartes. Et les cartes que nous faisons, pour ceux qui ne sont pas au courant, nous permettent de diviser en différents domaines. Donc est-ce que c'est expérimental ? Est-ce que c'est annoncé ? Parce que c'est déployé d'une manière ou d'une autre ? Voilà à quoi ressemble le monde maintenant en matière de ccTLD. Donc de manière générale, ça ne va pas trop mal à part l'Afrique. Mais la plupart des régions du monde, en fait, signent.

Donc bien sûr il y a l'Afrique, avec du Sud et certaines parties de l'Asie qui doivent s'améliorer un petit peu.

Ensuite, voilà à quoi ressemble l'Afrique maintenant. Alors, la bonne nouvelle, c'est que depuis la dernière réunion, on a obtenu l'Afrique du Sud. Est-ce qu'il y a des gens de l'Afrique du Sud ici ? Non ? Donc ils travaillent déjà depuis un certain temps pour en arriver à signer. Donc depuis décembre, c'est bon.

Nous avons également des ateliers qui ont lieu. Je sais que Rick Lamb va partir dans un certain nombre de ces pays pour travailler avec les ccTLDs du lieu pour signer. Ensuite, en Asie-Pacifique, il y a eu des personnes qui ont signé récemment : le Hong Kong et le Vietnam qui ont signé en décembre, et Samoa, qui a signé en janvier.

Ensuite, l'Europe. L'Europe est similaire à ce qu'on avait avant. Ensuite, l'Amérique latine continue d'avancer. Façon à la suivante. Et Amérique du Nord, même chose. On reste stable.

Donc ces cartes sont disponibles. Vous pouvez les recevoir tous les lundis si vous vous inscrivez. Ensuite, alors, j'ai déjà parlé de ça. On passe.

Alors nous avons un projet sur l'historique du DNSSEC. Donc j'ai toujours besoin de personnes qui puissent apporter leur contribution, donc n'hésitez pas.

Voilà. C'est tout ce que j'avais à dire pour ce matin. Y a-t-il des questions ? Des commentaires ? Oui. Allez-y Monsieur.

[MARK] : Mark [inaudible], Global Village. J'ai vu une statistique sur le .eg, mais je ne sais pas si c'est la bonne statistique. Eg donc l'Égypte.

En fait, j'aimerais bien savoir ce que ça veut dire. Parce qu'en fait, nous sommes le bureau d'enregistrement .eg mais ils ne permettent à l'accès à l'API pour nous. Et donc je me demandais comment fonctionnait le DNSSEC dans ces circonstances.

Je crois qu'ils utilisent [Coca] ? Mais ils n'ont pas d'accès à ce système. Ça passe par nos contacts au registre eg.

DAN YORK : Vous posez une excellente question. En fait, la carte suit où est signé le ccTLD, mais elle n'indique pas nécessairement où les gens peuvent travailler avec le bureau d'enregistrement pour télécharger. Donc c'est une distinction intéressante.

Retournons à la carte Afrique. Vous en êtes au stade opérationnel ? C'était de quelle couleur ?

Alors, c'est vert clair. Ça veut dire que le DS a été signé, a été mis dans la racine. On ne le met pas en vert foncé. Donc stade opérationnel tant qu'on n'a pas vérifié que vous pouvez télécharger des enregistrements DS.

MARK : Donc c'est une question d'accès pour les bureaux d'enregistrement.

DAN YORK : Oui. Alors si vous voyez un pays en vert clair, et si vous savez que vous pouvez télécharger des enregistrements DS, dites le moi. Parce que le passage DS racine, donc stade opérationnel, ça, il faut enfin entrer en contact avec les gens pour savoir si ça fonctionne en fait.

Donc l'Égypte n'est pas passée à l'autre couleur parce qu'on ne le savait pas. Du point de vue opérationnel, on sait quand il y a DS et racine, mais c'est tout.

Très bien. Je vais passer au panel régional suivant. C'est ça ? C'est comme ça qu'on fonctionne ? Alors pour ceux qui sont nouveaux, qui viennent d'arriver, c'est une séance assez informelle. On aime les questions. N'hésitez pas. Vous pouvez utiliser le micro qui est là et poser vos questions. On ne vous mordra pas ; enfin, j'espère.

Je suis modérateur pour ceci. Bon. Je vais m'asseoir parce que je ne vais pas rester debout pendant toute la journée.

Alors, là, ce qu'on organise, c'est des ateliers DNSSEC. On aime en fait rassembler différentes personnes qui s'occupent de différentes choses dans le DNSSEC.

Et donc, on a un panéliste qui est là avec nous. Et donc je vais commencer par donner la parole à Andre pour qu'il puisse nous dire ce qui se passe en république tchèque.

ANDRE : Merci beaucoup. République tchèque. Andre au micro. Je suis du .cz, alors une petite mise à jour sur ce qui se passe dans la République tchèque.

Je crois qu'on a déjà dit, nous avons plus de la moitié des domaines enregistrés qui sont signés. Donc ce chiffre change beaucoup. Il faut en fait forcer les opérateurs et les bureaux d'enregistrement à signer. Et il y a également hébergement sur les serveurs DNS. Donc ça, ça va. Mais le plus compliqué, c'est la deuxième partie du domaine. Donc c'est compliqué. On essaie d'obtenir des sites de haut profil, comme les journaux, les banques. On essaie de leur expliquer pourquoi c'est important, pourquoi ils doivent le faire. Nous sommes donc en phase de croissance, mais je pense que la croissance va ralentir.

Par ailleurs, nous essayons de convaincre les gens dans le pays pour qu'ils adoptent le DNSSEC. Donc on arrive à impliquer tout ce qui est le .gov, la stratégie .gov. Il y a également la stratégie sur la cybersécurité. Donc l'idée c'est de convaincre le gouvernement à signer les domaines. Et le nombre de domaines gouvernementaux signé est assez élevé.

Par ailleurs, validation DNSSEC. Pour certaines institutions publiques, cela fait maintenant partie des normes. Actuellement, on peut dire que le DNSSEC, c'est pratiquement obligatoire dans le pays. En tout cas, c'est hautement recommandé.

Autre activité intéressante qui est liée avec le point d'échange local, nic CZ. Il y a un groupe de FSI qui ont des normes de

sécurité plus élevées. Donc ces FSI au centre d'échange, en fait, sécurise les informations. Et donc, pour pouvoir rejoindre le groupe, il y a un certain nombre de prérequis. Et le DNSSEC, la signature de domaine, est justement une des conditions sine qua non. Donc en fait, c'est vraiment devenu obligatoire dans le pays.

Alors, en termes de validation, selon les analyses de Jeff Houston, nous sommes pratiquement à 50 % des résolveurs. Le chiffre change. Il a déjà changé depuis la diapositive. Mais encore une fois, nous essayons de communiquer aux différents FSI. Nous communiquons par le point d'échange local. Donc nous essayons en fait d'éduquer les FSI. Nous essayons de les convaincre, en fait, de mettre en place la validation. Les opérateurs mobiles, en majorité, valident. Donc c'est une bonne chose. Donc nous produisons beaucoup de logiciels libres. Donc nous avons un serveur. Il y a des opérateurs donc de TLD.

Pour vous dire ce qui va se passer cette année, on voudrait ajouter un soutien pour les algorithmes EDDSA. Cela dépend du nouveau TLS, donc la mise en œuvre.

Également, nous souhaiterions ajouter un soutien au roulement de KSK. Actuellement, nous avons le roulement de clé qui n'est pas encore soutenu.

Alors deuxième partie, donc résolveur de [nœuds]. Donc premièrement, la mise en place du RFC 7706. Donc baisse du temps d'accès au serveur racine en utilisant One on Loopback.

Autrement, le RFC 8020 avec utilisation de cache validité agressive. Donc cela veut dire que si vous avez un domaine, cela veut dire que tout est en dessus du [note] et non existant. Avec utilisation donc agressive de cache validée, cela permet d'améliorer les choses. Et enfin, nous avons mis en place le DNS sur le TLS. Donc si on a- En fait je peux utiliser le TLS pour communiquer avec le résolveur. Donc voilà, donc ça, c'est pour cette année.

Ensuite, nous nous préparons pour le [ESDS]. Il y a environ 30 000 domaines qui sont actuellement signés par l'ECSA. On aimerait signer le .cz également. On aimerait avoir un roulement d'algorithmes, un deuxième par rapport à ce qui a été fait il y a quatre ans.

Donc on est en train de préparer la communauté. On communique avec les FSI. Comme je l'ai dit, pendant les points d'échange, nous avons des conférences régulièrement. Le problème c'est la mise en application dans un pays, et donc on essaie de dire– d'attendre poliment en fait. Ce serait quand même bien que l'IANA arrête de retarder le processus.

Par ailleurs, le [widget] IPv6. La connexion doit soutenir l'IPv6. Et du point de vue fonctionnel, il faudrait voir si cela permet de valider les deux, donc RSA et ECDSA.

Donc si votre résolveur de DNS valide mais ne supporte pas ou n'est pas compatible avec l'ECDSA, donc le bouton n'est pas vert, en fait. Il reste rouge. Donc le résolve heure est compatible avec l'un d'entre eux, mais pas l'ECDSA.

Donc voilà ce qu'il faut faire pour en fait permettre de passer à une nouvelle situation. Je crois que c'est tout. Merci.

DAN YORK : Merci Andre. J'ai deux questions. Est-ce que vous pouvez clarifier la question de l'algorithme 13 ?

ANDRE : Oui. Ça ne fonctionne pas.

DAN YORK : Alors, il faut arranger ça. Vous avez donc mesuré la certification numérique. Est-ce que cela est en cours de développement ou c'est déjà fait ?

ANDRE : C'est une stratégie numérique qui a quatre ans à peu près. Donc cela fait partie du plan.

DAN YORK : Très bien. Est-ce que vous avez des questions pour André ? Oui, s'il vous plaît.

KIM DAVIES : Bonjour. Puisqu'on parle de l'IANA, je voulais dire que nous travaillons pour l'ECDSA et l'EDDSA. Et ce que nous voulons faire, c'est mettre en place, faire une mise en œuvre plus mature, pouvoir le mettre en place dans nos systèmes. J'aimerais vous parler plus en détail de ce que nous faisons, mais c'est un travail qui est en cours.

ANDRE : Est-ce que vous savez quand est-ce que cela sera mis en place ? J'ai compris que c'est quelque chose de très important, qu'il faut le faire avec de la bonne qualité, mais ça doit se faire assez vite.

KIM DAVIES : Je n'ai pas de date à vous donner. Je vais vous faire une présentation par rapport à cela le moment venu, mais pour le moment je n'ai pas de date à vous donner.

DAN YORK : Merci beaucoup. Est-ce que vous voulez vous présenter, Monsieur ?

KIM DAVIES : Kim Davies. Je travaille à l'IANA.

DAN YORK : Merci beaucoup. C'est bien d'avoir les gens pertinents quand on pose les questions. Très bien. Ensuite, nous avons Peter Koch qui va nous parler de DENIC et .de.

PETER KOCH : Merci beaucoup. Je tiens à remercier le Comité du programme de m'avoir habité. Je vais vous parler un petit peu de ce qui se passe avec le DNSSEC en Allemagne et pour le domaine .de, en particulier.

Alors, pour vous donner un petit peu de contexte historique, nous avons commencé le déploiement complet du DNSSEC pour .de en mai 2011. Nous fonctionnons avec l'enregistrement des registres DNS key. Nous recevons les enregistrements DNS key qui, à peu près comme le font nos collègues tchèques, nous avons jusqu'à cinq clés. En général, les gens ont une ou deux clés. Et donc, il faut valider au moment de l'enregistrement.

Ça veut dire que nous appliquons donc des validations au moment de l'enregistrement. Cela est en ligne avec notre vérification non-DNSSEC. Vérification. Donc nous vérifions que la chaîne pour l'enregistrement DS soit validée au moins par une des clés qui sont présentées. Et nous générons l'enregistrement DS pour tous. Parce que ça ne se justifie pas de supporter l'algorithme 1 pour tous les enregistrements DS.

Ensuite, nous nous basons sur un document que nous avons écrit il y a quelques années qui expliquent comment faire les changements d'opérateurs sans passer par des problèmes d'insécurité. Demande de sécurité. Cela est soutenu par notre système de registre parce que nous ne sommes pas basés EPP.

Si vous êtes intéressés par les détails, n'hésitez pas à me contacter après la séance.

Nous avons été témoins de quelques-uns de ces changements, et nous avons des informations là-dessus.

En ce qui concerne les bureaux d'enregistrement, il n'y a pas d'accréditation. Et nous ne demandons pas au bureau d'enregistrement de soutenir le DNSSEC. Ils le font.

En général, nous opérons dans le domaine complet des objets, avec toutes les informations DNSSEC qui existent là-bas. Et donc si les bureaux d'enregistrement n'ont pas mis en œuvre le

DNSSEC, ils ne vont pas nous fournir les informations concernant le DNSSEC.

Diapo suivante, s'il vous plaît.

Vous voyez ici les chiffres. Et puisqu'on parle tellement des domaines signés, c'est ce que nous avons. Cela correspond à 2011. On commence en 2011 et on voit deux couleurs. D'un côté, le bleu clair correspond au nombre de zones et de domaines signés ou de délégations signées. Nous avons jusqu'à 64 000 jusqu'à l'heure actuelle.

Il y a une croissance assez soutenue. Si vous regardez la partie droite de ce graphique, vous voyez que la croissance s'accélère pendant les cinq derniers mois. Nous n'avons pas une explication pour cela. On constate que cette croissance a lieu et l'on voit qu'il y a des bureaux d'enregistrement. Le nombre des bureaux d'enregistrement qui participe à cela augmente.

Mi 2015, nous avons eu une journée DNSSEC à l'institut d'informations de sécurité [inaudible] et, à ce moment-là, il y a eu des bureaux d'enregistrement qui se sont sentis encourager pour signer leur domaine. C'est une partie de l'explication peut-être.

Et un élément important, c'est les barres qui figurent en rouge qui correspondent au nombre de domaines qui sont signés,

quand on trouve du matériel de clé dans la zone mais qui n'a pas encore été enregistré chez nous. Cela est plutôt naturel puisque quand on signe un portefeuille de domaine, il y a donc une série de tests qui se mettent en place. Mais donc une partie de cela a duré pendant des mois. Donc on a parlé avec les bureaux d'enregistrement. Il y a parfois des revendeurs qui font du DNSSEC pour une raison ou pour une autre et qui attendent encore pour se mettre en contact avec le bureau d'enregistrement.

Et donc nous sommes en cours d'encourager ces gens à travailler sur ce matériel de clé et essayer de voir si les gens ont des difficultés au niveau technique et qu'ils n'arrivent pas à communiquer.

Diapo suivante, s'il vous plaît.

DAN YORK : On dirait qu'il y a 20 000 noms de domaine auxquels vous faites référence ?

PETER KOCH : Oui. 20 000 noms de domaine qui restent.

Donc quelles sont les dernières activités ? En 2016, nous avons changé notre HSM pour le KSK et le ZSK. Nous avons utilisé ce

qui, à l'époque, était assez pas cher, mais que nous ne supportons plus. Et nous avons migré. Nous avons choisi le Luna Safe Net. Et nous avons migré de carte PCI à notre système qui implique un roulement KSK. Et nous avons fait cela en août 2016. Excusez-moi ?

Oui. Tout le reste, on a gardé au niveau de la taille des clés. J'ai parlé du nombre d'enregistrements. Il y a une spécificité. Nous avons une fonction qui nous permet d'avoir des données d'autorité, jusqu'à cinq enregistrements par domaine. Beaucoup de gens utilisent cela. Et cela est utilisé par cette fonctionnalité.

Nous avons donc 230 000 domaines dans cette zone d'autorité, qui sont signés accidentellement, pour ainsi dire. Mais donc les délégations correspondent à 64 000 en ce moment.

La plupart de cela est fait par les bureaux d'enregistrement, par les opérateurs de DNS dans les bureaux d'enregistrement. On voit des groupes de centaines, des milliers de domaines qui sont signés dans les infrastructures qui sont gérées par les bureaux d'enregistrement. Parfois le client final le sait, parfois il ne le sait pas. Mais nous avons un grand bureau d'enregistrement qui a commencé à migrer vers le DNSSEC. Donc on s'attend à ce que les chiffres augmentent de manière encore plus importante.

Le marché est poussé par les bureaux d'enregistrement et par les opérateurs de registres. Et je pense qu'avec une seule clé, ça pourrait être plus facile.

En ce qui concerne les algorithmes, la plupart utilise RSA. Vous voyez dans le cercle, nous voyons ici 5 % l'algorithme 13. Il y a au moins un autre bureau d'enregistrement qui tombe dans cette catégorie où il signe les domaines à l'aide de l'algorithme curve 13. Ensuite on voit d'autres, un petit nombre de domaines qui utilisent l'algorithme 14. Ensuite, on voit un autre groupe qui utilise donc l'algorithme 5, 10.

Nous supportons encore Ghost. Celui-ci, c'est un domaine de test pour nous. Et il y a aussi d'autres tests qui ont été mis en place.

Comme Kim me l'a dit, puisqu'on a la validation, il faut donc voir quel est l'algorithme utilisé dans nos logiciels de validation. L'algorithme 15 et 16 ont été normalisés, même s'il n'y a pas de mise en œuvre, de notre côté au moins. Mais l'ED 25519 sera– on verra prochainement le ED 25519.

Maintenant, du bas vers le haut. En 2013, nous avons eu 300 bureaux d'enregistrement et au moins un domaine qui étaient signés et enregistrés. Nous sommes dans les 300 bureaux d'enregistrement qui adopté DNSSEC. Et quand je dis au moins un nom de domaine sous gestion, vous le voyez ici. Vous voyez

donc comment les chiffres évoluent. Il y a 16 900. Et à droite, vous voyez d'autres bureaux d'enregistrement qui ont un seul domaine sous gestion, qui est signé DNSSEC.

Il y a quelques bureaux d'enregistrements qui ont contribué à la plupart des chiffres que vous voyez ici. Et donc vous voyez quelle est la distribution des noms de domaine, qui est tout à fait en ligne avec ce que j'ai expliqué avant. À savoir qu'il y a un nombre croissant de bureaux d'enregistrement qui adopte la validation DNSSEC.

Diapo suivante. Très bien. C'est tout ce que je voulais dire. Y a-t-il des questions ?

DAN YORK : Est-ce qu'il y a des questions pour Peter ? Non, il faut lui poser des questions. Il faut parler allemand peut-être ?

INTERVENANT NON IDENTIFIÉ : Une question. Vous avez parlé de l'ECDSA qui était supporté par un bureau d'enregistrement. Est-ce que c'est au niveau régional ?

PETER KOCH : Honnêtement, je ne sais pas.

INTERVENANT NON IDENTIFIÉ : Très bien. Nous en reparlerons après.

PETER KOCH : Je peux vérifier. Mais oui, je devrais dire que la plupart des bureaux d'enregistrements qui ont adopté DNSSEC sont des bureaux d'enregistrement allemand. Donc nous croyons qu'une partie de cette croissance est un effet collatéral d'une initiative SDIN qui a encouragé ces bureaux d'enregistrement.

Merci beaucoup.

INTERVENANT NON IDENTIFIÉ : Dernière question.

Si vous aviez EPP, est-ce que vous pensez qu'il y aurait plus d'enregistrement ?

PETER KOCH : Vous voulez dire plus de 16 millions de domaines ? Non. Nous ne croyons pas ça, mais peut-être que ce n'était pas ça votre question.

Non. Ce n'est pas qu'on n'ait pas exprimé de l'intérêt par rapport à cela, côté titulaire aux côtés bureaux d'enregistrement. Il n'y a rien sur lequel nous pourrions exercer une influence.

DAN YORK : Merci beaucoup, Peter.

Maintenant, nous allons donc appeler un local, un pays local. Donc on va parler du Danemark. En anglais, s'il vous plaît.

ERWIN LANSING : Bonjour à tous. Bienvenue au Danemark.

Nous avons commencé à appliquer DNSSEC en 2010, après la signature de la racine. Nous avons vu des progrès. Il y a une liste qui est assez longue.

Je dois remercier Jack de cette idée. Et nous avons permis à nos bureaux d'enregistrement de venir directement nous contacter. Et au lieu de leur permettre de copier-coller de longs condensats, de longs hashs, nous avons importé des clés DNSSEC. Donc nous pouvons chercher cela dans nos serveurs, chercher les clés et leur donner ces clés, et leur dire quelle est la clé que vous voulez. Et donc il y a moins de possibilités d'erreurs, etc.

Diapo suivante, s'il vous plaît.

Quand nous avons lancé notre portail, nous avons donc changé les conditions de service. Nous avons tous les noms qui doivent être enregistrés avec nous. Donc nous sommes au courant de toutes les informations par rapport à cela. Ensuite, nous avons

changé les conditions de service. Et donc, les bureaux d'enregistrement permettent aux opérateurs de registres de gérer les clés par défaut. Et les opérateurs donc, par défaut, peuvent donc gérer les clés au nom des bureaux d'enregistrement.

Nous avons mis en place une journée technologique auprès des médias. C'était une activité vraiment très intéressante. Il a donc de grands titres au niveau des médias ; nous avons attiré l'attention des médias.

Nous avons ajouté de nouveaux algorithmes. Nous avons donc l'algorithme 13 et 14, et nous envisageons l'algorithme 15 et 16.

Ensuite, en ce qui concerne l'EPP, la mise en œuvre était assez faible. Nous avons enregistré un nouveau domaine. Nous avons donc prolongé la publication d'EPP jusqu'au mois d'août. Et maintenant, donc la fonctionnalité permet que l'on puisse ajouter et éliminer le DNS key.

Nous avons donc un atelier tous les deux ans sur le DNSSEC. C'est un atelier d'une journée complète, technique, avec des activités sur place pour signer des zones et pouvoir obtenir des résultats à la fin de la journée.

Les statistiques. Nous aimons tous ces statistiques. Cela est différent de vos statistiques, Peter, parce qu'ici on voit qu'il y a

certains qui utilisent l'algorithme 13. Nous travaillons avec eux et on va voir comment ça évolue.

Mais la raison pour laquelle on voit le graphique comme on le voit, c'est parce que toute la mise en œuvre technique a impliqué donc des discussions avec les bureaux d'enregistrement pour qu'ils signent leur zone. Et vous voyez qu'il y a eu beaucoup de domaines qui ont été signés récemment. Et ces bureaux d'enregistrement utilisent l'algorithme 13.

Maintenant, nous sommes un peu plus hauts que 5 % de noms de domaine signé. Et il faut des encouragements. C'est ce dont on a besoin. La plupart des bureaux d'enregistrement sont un peu gâtés. Ils veulent de l'argent. Et donc, nous essayons d'encourager donc l'utilisation du DNS est en leur disant que c'est bon pour les clients et que cela est bénéfique en dernière instance pour eux-mêmes.

Nous recommandons aux gens devoir donc les différents domaines utilisés. Nous avons trouvé des domaines qui sont signés, mais dont nous n'avons pas les clés. Je pense que c'est ma dernière diapo. Est-ce qu'il y a des questions ?

DAN YORK : Est-ce qu'il y a des questions pour Erwin ? Tout le monde adore Copenhague et personne ne veut mettre en colère les locaux, c'est ça ?

Allez-y, posez-lui des questions.

INTERVENANT NON IDENTIFIÉ : C'est très bien que vous nous permettez de télécharger les clés, et j'espère que d'autres vont suivre votre bon exemple.

DAN YORK : Très bien.

INTERVENANT NON IDENTIFIÉ : Question. Quelle est la vitesse à laquelle se poursuit la validation DNSSEC au niveau des FSI ?

ERWIN LANSING : Nous avons plusieurs FSI. Et les chiffres, c'est à peu près 50 %.

INTERVENANT NON IDENTIFIÉ : C'est très intéressant. Parce que la situation est différente aux Pays-Bas où nous avons un grand nombre de domaines signés, mais pas beaucoup de FSI qui valide le DNSSEC encore. C'est l'inverse. C'est intéressant d'écouter ça.

INTERVENANT NON IDENTIFIÉ : Est-ce que vous allez me corriger par rapport à cela ?

INTERVENANT NON IDENTIFIÉ : Non. Je ne suis pas un FSI.

DAN YORK : Très bien. Pour ceux qui les écoutent à distance, c'était un échange entre les gens qui se trouvent aux deux extrémités de la table. En Anglais. Question. Pour ce qui est des FSI aux Pays-Bas, qu'ils vont valider ?

CHRISTIAN : Il y a des rumeurs selon lesquelles le FSI le plus grand commencera à valider DNSSEC. Si c'est le cas, ça sera une bonne nouvelle, car il pourra donc entraîner les autres FSI à suivre son exemple.

DAN YORK : Très bien. Oui.

ERWIN LANSING : Une remarque. Nous n'avons plus de T-shirt, mais nous avons beaucoup de T-shirt sur l'algorithme 13, si vous en voulez.

DAN YORK : Si vous voulez donc des T-shirts de femme, il ne nous reste que des T-shirts de femmes. Donc si vous voulez des T-shirts de femme avec l'algorithme 13, vous pourrez en avoir. Il faut juste demander à Peter.

ERWIN LANSING : Il nous reste certain T-shirt avec certains thèmes.

DAN YORK : Donc si vous voulez, vous aurez aussi une écharpe DNS.

JACQUES : Non. Malheureusement, nous n'avons plus d'écharpes.

DAN YORK : Bon. Nous pouvons passer à un autre pays qui va nous parler. C'est Alex qui va nous parler du DNSSEC en Autriche.

ALEXANDER MAYRHOFER : Merci. Si vous regardez ses diapos, vous allez voir qu'elles n'ont pas changé beaucoup depuis la dernière fois, qui était en 2014. Ce qui montre, je dois admettre– je vais le dire de manière positive. On encourage donc le DNSSEC, mais je vais vous donner un peu plus de détails.

Dans quel domaine nous fournissons des services DNSSEC. Bien sûr, au niveau des ccTLD, .at ; ensuite, nous avons la production DNSSEC depuis février 2012. Nous utilisons open DNSSEC pour cela et nous proposons à nos bureaux d'enregistrement de télécharger les enregistrements DS avec l'extension EPP. Nous travaillons aussi avec un produit qui s'appelle Registry in a box. C'est un registre qui peut être utilisé pour neuf nouveaux gTLD.

Comme vous le savez peut-être, le DNSSEC est obligatoire pour les nouveaux gTLD. Nous avons open DNSSEC pour ses TLD aussi et nous permettons donc que le téléchargement des enregistrements DS. Nous travaillons également avec beaucoup d'Anycast pour beaucoup de clients. C'est quelque chose que nous recommandons. Et nous offrons ce qu'on appelle le Bump in the wire, signature Bump in the wire (BINW). C'est ce que notre département d'ingénieur a décidé de proposer et de faire. C'est gratuit. C'est inclus dans le service. Et certains registres ont signé cela parce qu'ils étaient trop paresseux pour mettre en œuvre la signature eux-mêmes. Donc ils ont adopté cette option.

Voilà un récapitulatif du calendrier. Nous avons mis en place le test, la plate-forme de test. Ensuite, nous avons eu le DS dans la racine, et nous avons donc commencé EPP quelques semaines après.

Les statistiques en ce qui concerne les bureaux d'enregistrement. En mars 2017, nous avons 405 bureaux d'enregistrement. Nous en avons perdu quelque 100 parce qu'il y a des frais minimums pour les bureaux d'enregistrement. Ce qui est assez spécifique par rapport à nous, c'est que nous demandons à nos bureaux d'enregistrement d'indiquer s'il valide ou non DNSSEC.

Et ce qui se passe actuellement, c'est qu'on pourrait parler pendant des heures, mais quand on voit un transfert vers un bureau d'enregistrement qui n'a pas de validation DNSSEC, nous enlevons donc l'enregistrement DS de cette zone-là. C'est une décision de politiques que nous avons pris en 2012, et nous devrons peut-être revisiter sa décision.

La bonne nouvelle, c'est que nous avons 405 bureaux d'enregistrement. 20 de plus ont décidé d'adopter DNSSEC. Et 43 de ces 405 bureaux d'enregistrement ont au moins un domaine validé DNSSEC.

Diapo suivante, s'il vous plaît. Alors. Comme je l'ai dit, nous ne donnons pas au bureau d'enregistrement des encouragements financiers. Nous avons très peu de noms de domaines signés, mais si vous voyez les chiffres de 2014, les choses ont un petit peu changé. Maintenant, on voit un petit peu la ligne de temps, et on voit qu'il y a une croissance par rapport aux domaines

signés DNSSEC. Et cela correspond un petit peu à ce qui se passe en Allemagne. Ce qui a du sens, parce qu'une grande partie de nos bureaux d'enregistrement sont basés en Allemagne. Donc on voit donc le nombre de domaines signés DNSSEC qui a augmenté de 50 % parce qu'il y a eu un bureau d'enregistrement qui adopter DNSSEC.

Nous voyons de manière très intéressante que les chiffres à la fin de la charte, vous voyez bon que les chiffres sont assez stables. Concerne les bureaux d'enregistrement, vous voyez que le DNSSEC est dominé par un petit nombre de bureaux d'enregistrement de grande taille, qui ont au moins une personne qui encourage l'utilisation du DNSSEC.

Diapo suivante.

Qu'est-ce que nous avons fait récemment ? Nous avons éliminé [inaudible], les enregistrements DS [inaudible] de la racine. Nous avons mis en place quelques roulements de clé KSK et nous avons mis en place les algorithmes 13, 14 sur EPP.

Ce que nous envisageons de faire, c'est une soirée DNSSEC, par exemple, pour essayer d'établir une collaboration autour donc du roulement de la clé KSK.

Dernière ? Très bien. Merci beaucoup. Merci de votre temps.

DAN YORK : Merci beaucoup de ce point de vue De ce qui se passe en Autriche. Y a-t-il des questions pour Alexander ?

INTERVENANT NON IDENTIFIÉ : Quand exactement avez-vous activé le 13/14 ?

ALEXANDER MAYRHOFER : Je crois qu'il y a quelques semaines. Je ne suis pas sûr. Il faudrait que je vérifie.

DAN YORK : Y a-t-il d'autres questions ? Des questions pour tout le panel peut-être ? Moi j'en ai une, sinon. Mais allez-y. Je préférerais que vous commenciez. Fils, vous n'avez pas de questions ? Non ? Quelqu'un d'autre ?

Alors, ma question, en fait, c'était si on réfléchit à toutes les présentations qu'on a entendu. En fait, j'ai une question d'ordre général. À votre avis, que peut-on faire pour que davantage de bureaux d'enregistrement soient encouragés à signer ? Qu'est-ce que vous pouvez nous dire ? Dans votre espace, quel est votre point de vue par rapport à ce que vous avez pu expérimenter ?

INTERVENANT NON IDENTIFIÉ : Au Danemark, ce qu'on a vu par rapport à tout ce qui a été fait l'année dernière, c'est qu'il faut aller parler au bureau d'enregistrement, parler des obstacles techniques pour l'EPP. Il y a un autre service qui s'appelle le DSU, donc DS upload, avec une chaîne qu'on poste et on dit voilà, c'est ma clé. Terminé.

Si je veux l'EPP, c'est parfois très simple. Ça peut être un API très simple, mais ça peut être autre chose. Ça peut être une question de politique. Donc il faut parler au bureau d'enregistrement, identifier quels sont les obstacles techniques et ensuite donc essayer de les encourager à le faire.

Donc en fait, leur faciliter les choses.

INTERVENANT NON IDENTIFIÉ : Ce qui est marrant, c'est que lorsque je parle aux bureaux d'enregistrement, très souvent, ce n'est pas une décision technique. Dans certains cas, ce qui se passe, c'est qu'ils sont informés par le marketing qu'il y a d'autres concurrents qui, en fait, ont une coche, une autre coche qui s'appelle le DNSSEC. Donc c'est le marketing qui va voir les ingénieurs et qui dit, "Vous savez on n'a pas ça, nous". Et l'ingénieur leur dira d'accord.

Et en fait, ils viennent nous parler pour que l'on utilise le Bump in the wire, par exemple. Donc parfois c'est difficile de les

convaincre. C'est en fait une charge administrative pour eux. Ça fait déjà longtemps qu'on n'en parle. Les Danois ne sont pas forcément faciles à convaincre. Dans la plupart des cas, c'est en fait quelque chose qui vient du marketing. C'est intéressant quand même.

DAN YORK : Ah. Les gens du marketing. Toujours il pose problème.

PETER KOCH : Oui. Je suis d'accord avec Alex. Cette croissance organique, c'est intéressant pour moi. C'est ce qu'on voit pour le .de, aussi. Il y a également la tentation d'agir de manière rétroactive et d'assigner, en fait, d'encourager financièrement les gens. Surtout quand les bureaux vous le demandent. Mais à mon avis, ce n'est pas quelque chose qui sera appuyé par notre modèle de gouvernance, etc.

Mais en plus, ce qu'il faut savoir, c'est que c'est un peu une punition. C'est un des avantages. Et puis il faut savoir que ce n'est pas seulement une question technique, étant donné qu'on a déjà 20 000 domaines signés. Et d'ailleurs, je n'ai pas dit tout à l'heure, j'ai oublié, qu'il y a des centaines de domaines qui sont avec un bureau d'enregistrement qui a déjà des milliers de domaines qui ont été signés. Donc très souvent, c'est un sujet de

communication. Donc une question de neutralité entre les revendeurs et les clients. Donc je crois qu'effectivement, communiquer c'est utile. Il faut motiver les gens à aller s'adresser à leurs clients spécifiques, et cela prend du temps.

La patience est utile. C'est regrettable, mais il faut le dire.

DAN YORK : Merci Peter. Autre personne ?

INTERVENANT NON IDENTIFIÉ : J'ai une question pour Peter, surtout. On a fait la remarque comme quoi les Danois ont une certaine attitude. Mais il y a eu un document dans lequel, dans le contexte des e-mails, il faudrait considérer le système pour les agences gouvernementales allemandes. Est-ce que vous avez vu une standardisation au niveau de vos nombres ? Parce que je sais qu'aux Pays-Bas, le fait que le gouvernement ait décidé d'utiliser le DNSSEC, ça veut dire que ça a un impact, en fait. Est-ce que c'est la même chose pour les Danois ? Est-ce que vous êtes d'accord ? Qu'est-ce que vous en pensez ?

PETER KOCH : je ne pense pas qu'il y ait de listes similaires. Elle existe pour des secteurs très réglementés du marché. Il y a différentes

exigences. Mais en fait, cela n'aurait un impact que sur un petit nombre d'entités. Ce que l'on ne voit pas ici, c'est l'importance du domaine. Si par exemple c'est un domaine d'un grand journal ou si c'est le domaine d'un grand fournisseur XYZ, etc. donc c'est complètement différent de nos petits domaines privés par exemple. Donc il faut toujours ajuster la mesure par rapport à la réussite ou par rapport à une apparence de succès.

Mais donc, dans notre cas, les 16 millions de noms de domaine doivent être signés pour que l'Internet soit sécurisé. Il y a des domaines qui sont résolus très fréquemment, et d'autres qui peut-être ne voient qu'une ou deux requêtes de résolution par jour. Et donc, encore un autre mot-clé, je n'ai pas mentionné ceci tout à l'heure non plus parce que ça faisait partie du rapport qui avait été mentionné par Dan. Mais le BSI, l'institut sur la sécurité, a une recommandation qui soutient le DANE. Et donc cela couvrirait leur service d'e-mail.

Et donc, par le passé, nous en avons parlé. Et donc c'est très intéressant de déployer le DANE parce qu'on n'a pas d'impact sur les clients. On peut le faire de manière séparée. Et donc cela n'aurait pas d'impact sur le nombre.

Nous avons également que le gouvernement fédéral a signé ces domaines. Nous avons également un grand fournisseur

d'Internet cable qui expose ses clients à ces validations. Et bien sûr il y a Google. Mais tout ceci est contenu dans le rapport.

Donc il y a une croissance, mais elles ne se reflètent pas nécessairement dans le nombre de domaines signés.

DAN YORK : C'est intéressant que la croissance fasse partie des e-mails du BSI et d'autres. Je crois que cela alimente le fait dont on a parlé. Si l'on regarde dans l'ordre du jour, nous allons parler de la sécurisation des e-mails. Une question là-bas ?

INTERVENANT NON IDENTIFIÉ : Je m'appelle [inaudible]. Je travaille pour une compagnie de sécurité en Allemagne et je fais partie d'un comité de consultation sur la sécurisation.

Première question pour Peter et pour Alex. Si vous regardez les chiffres, vous pouvez voir les Hollandais et tout ce qu'ils ont fait. Mais combien de bureaux d'enregistrement allemands utilisent le DNSSEC ? Est-ce que vous pensez que c'est uniquement l'influence des Hollandais, ou est-ce qu'on a réellement un nombre important de bureaux d'enregistrements allemands qui utilisent le DNSSEC ?

INTERVENANT NON IDENTIFIÉ : Je vais répondre donc en premier. Excusez-moi, je ne peux pas vous regarder et parler dans le micro en même temps. Donc j'avais 109 bureaux d'enregistrement qui était sur la diapositive, à droite avec un domaine, et à gauche les plus importants.

Je ne suis pas sûr, mais je crois que deux sur les cinq étaient des bureaux d'enregistrement allemands qui était arrivés après l'initiative SIDN.

Mais donc déjà les bases avaient été établies. La situation est un peu compliquée, en fait. Assigner des domaines au bureau d'enregistrement, c'est récent. Parce qu'en fait, on voit les bureaux d'enregistrement. Mais est-ce qu'on peut faire une investigation sur la base des opérateurs exacts. Donc c'est possible que ça soit un bureau d'enregistrement [Hollande]– opérateur de noms de domaine hollandais, pardon, qui passe par un bureau d'enregistrement allemand. Donc il y a utilisation du DNSSEC d'une manière générale. Mais il y a aussi revente du côté des noms de domaine et pas nécessairement d'appui de l'infrastructure. Donc ceci complique un petit peu la vision générale.

Et puis c'est également compliqué pour non de dire à l'utilisateur final, par exemple, écoutez ce bureau d'enregistrement soutient le DNSSEC. Qu'est-ce que ça veut dire

soutenir le DNSSEC ? En fait, le consommateur final doit faire le choix. Je ne sais pas si ça répond à votre question.

INTERVENANT NON IDENTIFIÉ : Du point de vue du consommateur final, pour nous nos consommateurs, ils ont tendance à utiliser la conformité DNSSEC. Pour eux, c'est la seule chose qui les intéresse. Donc si on est une banque, ils sont conformes à 100 % ; ils doivent avoir le DNSSEC.

Donc en Allemagne, nous n'avons pas de réglementation de sécurité sur le DNS. Donc en fait, nous n'avons pas d'obligation. C'est pour ça qu'en fait les gens l'utilisent peu.

ALEXANDER MAYRHOFER : La situation est assez similaire pour nous. Je ne sais pas exactement. Il faut que je vérifie [inaudible]. Mais je crois que sur les six plus grands bureaux d'enregistrement qui ont des enregistrements, je crois que pour la plupart, c'était des revendeurs allemands, de grands revendeurs allemands.

Je n'ai pas regardé le chiffre exact qui nous vient des Pays-Bas. Nous n'avons pas beaucoup en fait d'enregistrements de Hollande. En fait, il faudrait que je vérifie. Mais je dirais que la majorité des enregistrements DNS dans notre registre nous viennent des grands revendeurs automatisés allemands.

DAN YORK : Jacques, vous avez une question ?

JACQUES : Nous avons cinq minutes qui nous restent, n'est-ce pas ?

DAN YORK : Oui.

JACQUES : Non. Ce n'est pas lié à l'Europe, mais par rapport à DINE. Il y a eu un problème donc il y a quelques mois. C'était très triste n'est-ce pas pour le DNS sexe, pour les bureaux d'enregistrement. Parce qu'il y en a beaucoup qui ont fait des changements d'urgence pour ces domaines de vos profils. En fait, il y a eu un problème de cache pendant 24 heures. Et il y a eu un problème de transfert. Et donc ils ont essayé de nettoyer les enregistrements. Donc ça c'est peut-être un sujet pour une autre séance, mais il nous faut, pour les bureaux d'enregistrement– par exemple, au Canada, nous avons déjà du mal à convaincre les bureaux de faire le DNSSEC. Et donc lorsqu'on a un problème, eh bien il nous faut absolument trouver une solution.

DAN YORK : Donc vous avez en fait complètement changé de sujet de discussion. Oui. Je vous avais prévenus. Non. C'est un excellent sujet. Comment s'occuper de l'automatisation, des clés sécurisées. Il y a un certain nombre de propositions qui existent et qui [Inaudible] mise en œuvre.

ERWIN LANSING : C'est une des choses que nous avons faites il y a deux ans je crois. C'est qu'on a diminué le TTL pour arriver à une ou deux heures. C'est trop long certes, mais c'est quand même plus court qu'une journée entière.

DAN YORK : Je crois que c'est un excellent sujet si quelqu'un souhaite le proposer pour l'atelier DNSSEC pour l'ICANN 59 ou 60. Jacques, peut-être que vous souhaitez réfléchir à ça ? C'est effectivement un bon sujet de conversation, si ça vous intéresse.

Alors, on va applaudir nos intervenants de la région. Merci beaucoup. Alors je vais me mettre debout. Je vais parler de l'IETF. Et si vous souhaitez vous lever comme moi lorsque vous présentez, vous pouvez le faire. Ou alors, vous pouvez rester assis. C'est comme vous voulez.

JULIE HEDLUND : Je dois vous expliquer que cela ne marche que pour les PowerPoint. Donc vous, vous avez un PDF. Donc votre cliqueur ne marchera pas. Mais je vais vous aider.

DAN YORK : Ah merci. Alors j'aimerais remercier la personne qui a posé la question sur l'Égypte ce matin, parce qu'on m'a tout de suite corrigé ; le .eg n'est pas signé. Et enfin, quand on regarde dans la base de données on se rend compte– en fait, il faut que je vérifie le code de la carte. Je commençais à m'inquiéter parce qu'il semblerait que dans la base de données, le .eg n'est pas présent. Donc il y a un problème, là.

Donc si vous avez envie de vous occuper de tout ce codage, n'hésitez pas. J'aimerais bien savoir pourquoi l'EG n'est pas enregistré, pourtant il y avait une couleur sur l'EG.

Alors, les activités DNSSEC à l'IETF. Combien de personnes sont impliquées dans l'IETF d'une manière ou d'une autre ? Très bien. Un certain nombre de personnes. Alors, je vais rapidement parler de l'IETF. Alors pour ceux qui ne connaissaient pas bien, c'est le groupe de travail de génie Internet. C'est donc l'organisation qui crée les RFC, donc les appels à commentaires. C'est en fait les normes qui sont derrière l'Internet.

Donc il y a des groupes de travail qui existent, des WG. Il y en a plus de 100. Et il y a des chartes qui permettent de créer certaines normes. Oliver est là. Il fait partie– il est président d'un des groupes de travail qui existent. Il y a également des séances où les gens qui ont des intérêts communs se ressemblent pour en discuter. Et ce qui est intéressant, c'est que n'importe qui peut participer aux différents groupes de travail. Pouvez participer aux listes de diffusion. Etc. vous pouvez soumettre un document préliminaire sur l'Internet. Un draft, si vous le souhaitez.

Alors, voilà le processus. Il y a des personnes qui créent un document préliminaire sur tel ou tel sujet qui devrait être standardisé. Ensuite, il y a un processus de discussion du projet préliminaire. On débat. On approuve. On adopte, etc. Et on passe partout ce processus jusqu'à ce que ce document préliminaire sur l'Internet soit publié comme RFC. Ou alors, il peut être abandonné. Ou alors il peut devenir autre chose. Mais c'est en fait le processus d'ensemble que vous avez là, qui permet d'établir des normes.

Alors en matière de DNS, l'IETF travaille principalement par liste de diffusion, par e-mail. Donc c'est par ce biais que tout est approuvé, etc. Mais trois fois par an, on se retrouve dans différents endroits du monde de manière à ce que les gens puissent y accéder de manière plus ou moins facile.

Alors combien de personnes seront présentes au 98, à Chicago ? Donc je ne parle pas des Américains, mais je crois que beaucoup des personnes qui sont présentes dans la salle seront également à Chicago. Alors que se passe-t-il à Chicago ? Tous les ingénieurs impliqués dans différents sujets se retrouvent en personne. Et donc les sujets les plus complexes qui ne peuvent pas être résolus par e-mail sont débattus sur place.

Donc nous avons vu différent discussion là-dessus par rapport à ce qu'on devait faire. Par exemple, qu'est-ce qu'on va faire avec les noms de domaine à utilisation spéciale ? Voilà. Warren, qu'est-ce qu'on fait de ça ? Donc c'est un petit peu ce type de discussion passionnée que nous avons et que nous souhaitons faire avancer.

Donc il y a Chicago, il y a Prague et il y a Singapour pour cette année. Donc on se déplace régulièrement dans le monde. Alors qu'est-ce qui se passe au niveau de l'IETF ? C'est donc tout ce qui est lié à la sécurité. Les grands groupes de travail au niveau du DNS OP. Le groupe sur les opérations du DNS. Je ne sais pas si vous connaissez la personne qui s'occupe du RSSAC, etc. C'est une des coprésidentes de ce groupe. Donc elle fait aussi partie de l'ICANN.

Donc le DNSSEC en est à une étape où les normes ont été définies et maintenant il faut passer au déploiement du DNSSEC.

Donc il y a de nouvelles modifications, de nouveaux commentaires qu'il faut intégrer pour améliorer le système.

Donc récemment, le dernier RFC c'est sur la gestion de l'enregistrement DS, avec CDS et DNS key. Donc l'idée c'était d'obtenir un nouvel enregistrement DS.

Il y a un projet préliminaire sur les problèmes de cache et donc nous en sommes à la dernière étape de commentaires avant publication.

Il y a un certain nombre d'autres documents qui sont en cours d'élaboration. Si cela vous intéresse, si vous voulez savoir où en sont les normes, je vous conseille de suivre le DNS OP. Il y a d'autres activités qui ont lieu en dehors du DNSSEC, mais vous pouvez donc avoir des informations intéressantes.

Autre groupe, le groupe de travail DANE qui donc est présidé par Oliver et une autre personne, qui a été créé pour créer la norme DANE ainsi que d'autres normes. Ce groupe a bien avancé dans son travail et il en est à l'étape, en fait, de clôture des activités, de voir comment conclure son travail.

Allez-y, vous pouvez parler.

INTERVENANT NON IDENTIFIÉ : Notre document final est en attente de publication. Nous attendons de voir si oui ou non ils sont approuvés.

DAN YORK : Son coprésident le regarde en lui disant « Attends, ça ne va pas là ». Et ça fait partie du processus de l'IETF, en fait. Organiser un groupe, mettre au point une norme et ensuite clôture le groupe. Parce qu'une fois que la norme est publiée, il ne reste plus qu'à déployer, etc.

Autre groupe qui a été très actif récemment, c'est le groupe sur la vie privée et le DNS. Donc c'est la question de la confidentialité. Ici, nous parlons de l'intégrité. De nous assurer que les données qui sortent du DNS ce sont celles qui ont été intégrées dans le DNS. C'est ça, le DNSSEC. Mais ce groupe-là prend en compte la confidentialité. Donc lorsqu'on envoie une requête au résolveur local, est-ce que je suis sûre que celles-ci vont protéger ces données de manière à ce que personne sache exactement ce que vous faites et tout ce que vous– quels sont vos agissements sur Internet.

Donc c'est le DNS sur TLS. Donc chiffrage de la connexion entre le résolveur de votre système et le résolveur récursif local auquel vous vous adressez. Donc c'est là que se fait tout ce travail. Il y a deux RFC qui ont été publiés récemment. Comme vous le voyez, la 7858 et la 1894 sur DNS sur DTLS. Pardon. Donc c'est en

janvier je crois. Et il y a encore pas mal de travail dans ce groupe pour identifier les mécanismes pour arriver à fonctionner correctement. On n'en est à une discussion pour savoir comment faire pour passer du résolveur récursif au résolveur faisant autorité. Donc quel est le lien en matière de droit privé entre ces deux ?

Et je dois vous dire que c'est intéressant, parce que je parlais à des clients entreprise, lorsque je parle dans ce type de conférence, c'est que je parle du déploiement, ils voient ceci et ils se disent, attends, toutes les requêtes DNS de mon ordinateur à moi au résolveur vont être chiffrées. À ce moment-là comment je vais faire pour surveiller ce que je fais au sein d'entreprise pour empêcher mes employés de se rendre sur des sites pornographiques, etc. Donc ça, c'est une grosse nouvelle pour entreprise, qu'on allait standardiser ceci. Alors bien sûr qu'on peut étendre ceci au niveau d'une d'entreprise, mais ce type de chose est en cours de développement parce que bien sûr qu'il y a des problèmes de surveillance sur l'Internet.

Autre note importante, il y a un groupe qui s'appelle le groupe [Curdle]. Vous savez, dans l'IETF, on a toujours des noms très sympas pour les groupes de travail. Donc ça, c'est sur la courbe elliptique de cryptographie et comment mettre ceci en lien avec nos protocoles. Donc récemment, il y a eu une standardisation, un nouvel RFC sur le DDSA. Donc la courbe pour l'algorithme

lithographique. Donc ceci a été standardisé. C'est le RFC 8080. C'est l'algorithme 15, me semble-t-il. Ou 16 ? 15 et 16. Donc Andre [Surray] s'en est occupé. Il n'est plus là. Il n'est pas là. C'est en des auteurs de cet algorithme. C'était Andre ou quelqu'un d'autre peut-être. Je ne sais plus.

Donc nous avons un nouvel algorithme qui existe et il y a un certain nombre de personnes qui sont en train de voir comment le mettre en œuvre.

Donc voilà un petit peu ce qui se passe. Et donc avec l'IETF 98, donc dans deux semaines à Chicago, la partie DNS qui se passera, c'est donc le [inaudible] IETF 98. Donc on verra quelles sont les activités DNS en ce domaine. C'est quelque chose que nous faisons dans les IETF. Il y a donc des équipes qui font ceci. Je ne sais pas si, ben, vous y serez. C'est ça ?

Vous voulez nous expliquer un petit peu ce que vous faites ?

BEN : Donc le samedi et le dimanche, un certain nombre des membres de mon équipe qui travaille dans le DNS, mais il y a d'autres personnes également, d'autres équipes. Par exemple [Andrew Surray], d'autres développeurs d'IFC, qui vont organiser deux tables. Nous avons un certain nombre de projets sur lesquels nous souhaitons travailler. Parfois il y a des chevauchements en

fait du travail de différentes équipes pour la mise en œuvre des RFC et des projets.

Et surtout pour les projets DNS, on se concentre souvent sur son propre projet et sur sa mise en œuvre, et finalement, on arrive à de nouvelles fonctionnalités qui sont mises en œuvre. L'idée c'est donc de redonner ceci à la communauté. Et donc l'intérêt de l'IETF c'est que les RFC sont mis en œuvre. Donc on a des mises en œuvre de référence. C'est très intéressant.

DAN YORK : Si vous êtes à Chicago, si vous connaissez des personnes de Chicago qui souhaite contribuer, n'hésitez pas. Vous pouvez vous rassembler dans une salle avec plein de gens qui adorent le DNS et qui vont travailler sur des codes pendant très longtemps. Oui. Vous êtes les bienvenus.

Le DNS OP se retrouvera au début de la semaine. Le lundi. Il n'y a pas encore de calendrier officiel. Je n'ai pas vu beaucoup de choses sur le DNSSEC par contre. Je crois que c'est surtout le RPZ qui est déjà source de beaucoup de débats. Mais sur le DNS OP, vous avez exactement ce qu'ils vont faire. Je n'ai pas l'impression qu'il parle beaucoup du DNSSEC. Non. C'est surtout DNS. Mais bon. Quand même des discussions intéressantes.

Paul, vous avez dit qu'il y aurait peut-être des choses sur l'IPSEC ? C'était surtout sur les e-mails, c'est ça ?

WARREN : Non. C'est connexions VPN, et la question de confiance pour activation sur votre dispositif. Donc résultat [split] DNS. Lorsqu'on se connecte à un VPN.

DAN YORK : Très bien. Alors on en parlera peut-être dans le groupe IPSEC. Et dans le domaine de la sécurité, il y aura un projet sur le NSEC 5 est la proposition qui a été avancée. Donc voilà.

WARREN : C'est également dans le cadre du DNS OP. Il y a le [inaudible] 256 plutôt que le [inaudible] 1. Nous allons donc en parler, parler de la mise en œuvre.

DAN YORK : Très bien. Donc voilà un petit peu ce qui va se passer. Voilà donc pour l'IETF. Y a-t-il des questions là-dessus ? Allez-y.

INTERVENANT NON IDENTIFIÉ : [Inaudible]. Il y a également le groupe de travail qui présente la version EPPS publique sur le transfert des clés. Et il y

a également le projet de Jacques sur le transfert de tout ce qui est relatif aux clés pour les registres et les bureaux d'enregistrement. Donc c'est également un autre groupe important pour le DNSSEC.

DAN YORK : ALAC, savez-vous si on va en parler à Chicago ?

JACQUES : Nous sommes présents dans l'emploi du temps pour tout ce qui est expérimental, me semble-t-il.

DAN YORK : Très bien. C'est bon à savoir. Le groupe des extensions des registres considère– alors, pour les personnes qui sont là à l'ICANN, pour les bureaux d'enregistrement et les registres, c'est également un autre groupe dont il faut surveiller le travail, je pense. Voilà.

Vous pouvez suivre, si vous vous rendez sur le site de l'IETF, vous pouvez suivre à distance pour voir ce qui se passe et vous pouvez également participer. Voilà. C'est tout. Maintenant, on va demander à Matt de nous parler de la racine KSK.

Vous voulez parler avec ce micro, Matt ? C'est possible. Vous pouvez l'aider avec ces diapositives ? Oui ? Il n'est pas obligé d'utiliser le cliqueur. Si ?

MATT : Bonjour. Si vous êtes venus à toutes les séances DNSSEC, vous allez voir que c'est la troisième fois à Copenhague que je vais parler sur le KSK. Je vais faire de mon mieux.

Alors je voudrais faire un point assez rapide, parce que probablement vous avez déjà entendu parler de tout cela, sur le KSK. Voilà le calendrier pour le roulement de la clé de signature de clé.

Nous donc générons la nouvelle clé au troisième trimestre 2016 dans nos installations en Californie. Ensuite on passera aux installations qui sont dans l'Ouest. Et nous considérons que toutes ces installations sont prêtes au niveau opérationnel.

En ce qui concerne le projet, nous sommes à l'étape où nous communiquons aux gens la nouvelle clé. J'ai montré dans d'autres présentations que cette clé n'est pas encore publiée sur le DNS. Cela aura lieu le 11 juillet. Mais nous sommes donc dans la phase où nous communiquons, notamment aux opérateurs, c'est notre public cible. Parce que les opérateurs doivent

absolument mettre à jour leurs ancres de confiance, où les choses tourneront mal.

J'apprécie énormément la possibilité de vous montrer ce qui se passe. Donc le jour J, c'est le 11 octobre 2017. Et c'est la date à laquelle tout le monde doit faire attention. Notamment si vous avez des infrastructures de validation DNS texte. Après cela, nous allons révoquer l'ancienne clé et, à terme, l'éliminer de nos installations.

Cela nous place dans une période entre la génération de la clé et le roulement lui-même. Est un élément important, c'est que tous ceux qui font donc le protocole automatique de mise à jour de l'ancre de confiance doivent être absolument au courant de ce qui se passe. Parce que si vous faites confiance à une clé et que vous voyez une nouvelle clé qui est signée par l'ancre de confiance, éventuellement, après 30 jours, vous allez faire confiance à une nouvelle clé. Et donc vous allez passer cette confiance d'une clé à une autre. Et il est important que vous vous reposiez sur le RFC 5011, vous devez donc tester vos logiciels. Parce que notre RFC 5011, dans ce RFC, il faut attendre 30 jours pour pouvoir tester les logiciels. Et c'est pour cela qu'il est important de pouvoir utiliser notre banc d'essai pour accélérer ces tests.

L'ICANN veut donc proposer un banc de test, une plate-forme de test, pour que les opérateurs puissent valider cela en temps réel afin de pouvoir mettre à jour automatiquement ces clés de manière correcte.

Nous nous annonçons donc cette plate-forme d'essai à la cérémonie inaugurale de l'ICANN 58. Nous avons donc créé cette plate-forme d'essai pour que les opérateurs qui valident le DNSSEC dans leur infrastructure puissent valider leur logiciel.

Nous savons qu'il est plus sûr de considérer que cela dans les serveurs de production pour s'assurer que le serveur joue un rôle de confiance correcte. Et donc si vous êtes capables de réussir à ces tests, ça veut dire que vous êtes en condition, à même de pouvoir mettre à jour vos systèmes.

Ce qui importe, c'est plutôt le paquetage les codes ; c'est ça qui nous intéresse surtout de tester. Et on sait que la plupart des gens qui respectent le RFC 5011 sont prêts pour pouvoir mettre en place ces tests. Ce n'est pas un test difficile. Il s'agit d'une liste de diffusion. Donc tous les samedis, tous les dimanches pardon, on commence un processus à tour de rôle qui va changer les zones. Donc la zone de cette semaine, c'est au mois de mars donc. Vous voyez donc à quoi ça ressemble ? C'est un design assez ordinaire. Donc, souscrire à ce test implique de souscrire à cette liste de diffusion pour les différentes zones et

vous obtenez des messages toutes les semaines qui vous disent ce qui se passe au niveau des tests et ceux à quoi vous devez vous attendre.

C'est quelque chose d'assez simple, d'assez direct. Et c'est pour que les opérateurs puissent valider de manière facile leur logiciel.

Voilà ce que je voulais vous dire. Vous avez tout ce qu'il y a un roulement de la clé KSK, que le processus avance bien. Je voulais vous rappeler la date du 11 octobre 2017. C'est le jour J. Et ensuite, je répondrai à vos questions si vous en avez.

DAN YORK : Est-ce qu'on a des questions pour Matt ? Si personne des questions, apparemment j'ai une question. À quelle heure cette clé apparaîtra dans la zone ?

MATT : C'est une bonne question que m'a posée hier. Est-ce que vous l'avez posée l'autre jour aussi ?

Nous n'avons pas encore annoncé à la communauté à quelle heure cette nouvelle clé sera signée pour la première fois. Nous allons le faire bien sûr. Vous allez avoir le moment exact où cette signature aura lieu.

INTERVENANT NON IDENTIFIÉ : Où nous allons acheter une bouteille de champagne bien sûr.

MATT : Ben oui.

INTERVENANT NON IDENTIFIÉ : J'ai essayé cette plate-forme d'essai, et il y a donc un guide. Est-ce qu'on pourrait inclure les non-résolveurs ?

MATT : Oui. Merci beaucoup. Merci beaucoup de me poser cette question. Oui, j'aimerais bien si vous pouvez m'envoyer un texte. Je pourrais mettre à jour cela immédiatement.

DAN YORK : D'autres questions ? Ça veut dire que vous êtes tous préparés ? Que vous avez déjà mis à jour vos encres de confiance ? Ah, on a une question. Très bien.

INTERVENANT NON IDENTIFIÉ : Par rapport à la plate-forme d'essai, je sais– est-ce que quand on signe, on peut obtenir directement les ancres de confiance ?

MATT : Excusez-moi. Pourriez-vous répéter ?

INTERVENANT NON IDENTIFIÉ : Le DNSSEC a des ancres de confiance nouvelle. Est-ce que cela fera partie des tests ?

MATT : Non. Nous avons décidé de ne pas utiliser cette partie de la machine parce que cela est spécifique à la zone racine. Nous avons pensé que cela ne faisait pas partie de ce que nous voulions faire. Nous ne voulions pas que l'on puisse télécharger l'ancre de confiance depuis la racine parce que cela concerne spécifiquement la clé de la racine, et c'est une ancre de confiance arbitraire.

DAN YORK : Est-ce qu'il y a d'autres questions ? Très bien. Matt, on va vous applaudir et vous remercier de votre présentation. Merci Matt.

Nous avons quelques minutes avant de passer à la présentation suivante. Je vais justement dire qu'il y a des boissons et il y a quelque chose à manger aussi, si vous avez fort et si vous avez soif. N'hésitez pas à aller vous servir un café ou à manger

quelque chose avant de commencer notre prochain panel. Mais garder la porte ouverte, s'il vous plaît. Bon. Ben.

[FIN DE LA TRANSCRIPTION]