BEIJING - Session de DNSSEC Pour Tout Le Monde le guide du débutant
Lundi, 08 Avril 2013 - 17:00 à 18:30
ICANN - Beijing, République populaire de Chine

JULIE HEDLUND: Est-ce que nous avons commencé à enregistrer, dans le bonjour tout le monde est bienvenu à ICANN 46 à Pékin en Chine, et vous êtes dans la session de DNSSEC pour tout le monde le guide du débutant, ceux qui ne sont pas approchés plus de nous venait reprocher aux portes de se remettre session ludique et vous allez mieux voir les mieux entendre si vous êtes plus près, je suis avec ICANN alors que nous avons de l'avant et le roi des informations sur l'écran surtout les présentateurs et je vais passer la parole à Dan York qui est la nôtre animateur.

DAN YORK: Combien d'entre vous peut écrire DNSSEC? Oui c'est bon il en a plusieurs d'entre vous vous êtes au bon endroit, c'est une science qui est un peu une introduction nous en parler de ce qui est le DNSSEC est ce que cela résout et comment cela marché fonctionne, pour ceux qui veulent plus de détails il y a une autre session qui sera mise en place mercredi et qui donnera beaucoup plus de détails cela, c'est un de DNSSEC qui aura lieu mercredi avec beaucoup plus de détails, aujourd'hui nous allons y parler sur ce qui est le DNSSEC et quels sont les problèmes que cela résout, voilà donc l'emploi du temps et l'ordre du jour pour cet après-midi, son partant nous avons beaucoup de présentateurs, et je vais présenter.

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.

Alors j'ai Warren Kumari qui est de Google et qui va être un de nos présentateurs, Russ Mundy de Sparta, Julie qui s'est déjà introduit, nous avons Norm Ritchie et acques Latou, nous avons aussi une autre personne qui va venir plus tard. Nous avons quelqu'un qui est là au milieu de vous et qui va jouer un rôle diabolique dans notre petite présentation.

Alors je vais donc, pourquoi vous n'avancez pas la diapo? Nous savons que DNSSEC a commencé avec ITF IL Y a plusieurs années, nous avons une petite histoire d'alternative dont nous avons parlé aujourd'hui. Nous allons commencer il y a 7000 ans, disant que le DNSSEC il a commencé quand nous avions Aguina, elle vivait dans une cave au bord du grand canyon et elle vivait ici, de l'autre côté du canyon il y avait Og, il vivait aussi dans une cave à une grotte de l'autre côté du pantalon. Voilà les deux qui sont là mais ils ne se parlent pas souvent et c'est difficile de passer à un côté à un autre d'un camion et c'est difficile pour accéder de l'autre côté, donc de temps en temps ils descendent et ils remontent de l'autre côté et les voies ils se disent mais comment on peut se communiquer, injurieux en vue une fumée qui se dégageait de leur feu en pourrait commencer à parler alors ils ont commencé de faire des signaux de fumée, et voilà commencer la réunion mais malheureusement quelqu'un d'autre est arrivé, une autre préhistorique s'appelle Kaminski qui a décidé que moi aussi je veux participer à la conversation et à laquelle a commencé les signaux de fumée, et bien ce que vous avez Aguina d'un autre côté du canyon et elle elles avaient une grande importation avec leurs propres signaux de fumée et il savait exactement comment ça marché, et puis cet autre homme préhistorique qui arrive est maintenant elle voit deux ensembles de

signaux de fumée et elle s'est dite et ce qui se passe est donc voilà il y avait un problème.

Un jour elle décide de descendre de sa falaise pour voir qu'est-ce qui se passe et voir quel était le signant qui arrivait de la part de Og et il s'en allait le voir tous les deux messages du village Diffy, et il se dit qu'il j'ai une idée je vais rentrer dans sa grotte est il a trouvé qu'il y avait un gros retard de sable bleu qui ne se voyait que dans la grotte de Og, perçant d'autres avaient un tel sabre le, donc ce qu'il a fait ce qu'il a mis du stade de dans le feu de Og, la fumée et devenait le maintenant un seul que c'était facile pour Aguina, le regarder de l'autre côté du canyon et elle savait que la fumée devenait de Og. C'étaient les messages qui venaient de Og, alors quand Kaminski a essayé de faire les signaux de fumée, cette fumée n'étaie pas bleu, donc Aguina s'était rendu compte que avec le bleu elle avait la bonne conversation, en fait à la fois se consacrant un résumé de DNSSEC et à la fin du compte c'est ce que DNSSEC fait, c'est que on s'assure que vous avez la bonne information pour que vous savez exactement que c'est le message correct que vous voulez obtenir. Maintenant je vais passer la parole à Warren pour qu'il vous explique comment ça marche vraiment de façon que comprend comment le DNSSEC fonctionne.

WARREN: Tout d'abord il faut comprendre comment le DNSSEC fonctionne, mais pas tout le monde est en premier sait qu'est ce que le DNS et qu'est-ce que cela fait, le DNS converti les noms et les mots comme www. quelque chose, ça commence à la racine du DNS et ensuite chaque niveau demande quelle est l'adresse IP, donc on voit le message au

prochain niveau et donc si vous cherchez www.bigbank.com on dit oui je voudrais l'adresse de big-bang.com, la racine dit non je ne l'ai pas, donc ce que je sais c'est que d'où le.com vient. Donc vous devez le demander à eux.com et ils vont vous donner la réponse… Mais la prochain chose à faire ce serait je connais cette adresse, dont vous pourriez peut-être la demander de la personne autour de bigbank.com, il dit je voudrais l'adresse IP de www.bigbank.com et le serveur de bigbank dit ah je connais ça, la réponse c'est si votre ordinateur peut connecter. En fait il y a quelqu'un au milieu et qui essaye d'attaquer d'autres conversations, je pense peut-être que leur réunion est plus intéressante que la nôtre, donc à la base pour résumer chaque niveau de DNS vous donne les références d'autres niveaux et chaque niveau vous délectait vers le prochain niveau. Excusez-nous nous avons un problème d'audio, dont il est démenti sans plus populaire comme par exemple www.google.com ou www.yahoo.com ou www. excusez-nous, toutes ces questions commencent… Il faut à la base sa garde l'information dans le cache et la prochaine fois que quelqu'un pose la question la réponse est déjà là, et bien sûrs se sont beaucoup d'observations absorbées très rapidement par d'autres personnes qui parlent sur la ligne et cela nous aide pas. Donc nous allons faire un petit sketch pour démontrer cela.

Nous avons une autre personne qui parle à travers l'ordure dont nous avons beaucoup de mal d'entendre les interventions alors nous sommes désolés.

JULIE HEDLUND: Nous avons des interférences ne peut nous devons nous en occuper en attendant nous allons faire une pause et nos acteurs vont pouvoir se déguiser, c'est difficile.

WARREN: Je pense que mon costume était prévu pour quelqu'un qui est un peu plus maigre que moi.

JULIE HEDLUND: Nous sommes toujours en cause, on n'entend que le problème serait résolu. Merci beaucoup nous allons donc continuer.

DAN YORK: OK, nous allons nous amuser un peu, c'est difficile de décrire le DNS est le DNSSEC et c'est assez technique et c'est un sujet assez technique, nous avons des experts qui se distinguaient ici et qui vont devenir des acteurs, nous avons fait un petit sketch en vous montrant les transactions DNSSEC et voilà donc le sketch 01et je suis utilisateur Joe et voilà ici mon ISP et nous avons la racine et le.com et bigbank.com et dans ce premier acte de cette pièce devait être utilisateur final et je vais faire mes affaires bancaires en ligne, je vais m'asseoir dans mon bureau et je vais payer quelque factures.

ACT 1

JOE: M. ISP 'aimerais aller à www.bigbank.com.

M. ISP: Merci mais je ne sais pas où le www.bigbank.com est, donc ce que je vais faire ce que je vais aller voir la racine (root) et je vais demander aussi.

ROOT: Merci de me demander mais je ne sais pas où c'est, est-ce que vous pourriez demander.com à 1.1.1.1.

M. ISP: Vous savez où est www.bigbank.com?

.COM: Non je ne sais pas mais demandai donc à bigbank.com il est à 2.2.2.2.

M. ISP: Merci Bigbank, je cherche www.bigbank.com.

BIGBANK: Oui je sais, www.bigbank.com je sais cela où il est avec 2.2.2.3.

M. ISP: Merci, je vais donc donner la réponse à l'utilisateur final M. Joe. Je vais lui dire 2.2.2.3.

JOE: merci M.ISP et maintenant je peux prendre mes affaires bancaires, et mon ordinateur sait que bigbank.com est à l'adresse 2.2.2.3, et je peux aller payer toutes mes factures.

(Applaudissements)

WARREN: Personne n'a crié encore dans la salle, c'est dommage mais peut-être la prochain pour. Donc vous vous demandez peut-être quelle était cette présentation. Aguina était donc l'utilisateur et Og est le serveur, et quand M. Kaminski arrive il envoie des signaux lui aussi. Aguina elle est confuse, donc le DNSSEC c'est ajouter la fumée bleu au DNS. Donc pourquoi c'est si nécessaire?

Quand le DNSSEC a été fait au départ il avait des problèmes, Internet était plus petit et c'était une sécurité, les gens connaissent d'autres personnes et ils envoyaient des messages ou des autres pays n'avaient pas les spam, il fallait donc se protéger contre les gens qui prétendent d'être quelqu'un d'autre. Le serveur de nous va cacher cette information, le DNSSEC résout cela à travers des signatures numériques, en fait quand vous demandez à un serveur de DNSSEC, la réponse ça devrait être le prochain serveur sur la chaîne ou la réponse elle-même, et puisque cette réponse est signée vous pouvait croire le nombre de serveurs de la racine, la clé de la racine et dans quelle est la clé de la racine et cela construit une chaîne de confiance. Donc quand la racine dit qu'elle ne sait pas où l'adresse et les, mais je sais où.com est. Et ainsi vous pouvez le croire que le monde des serveurs ou le serveur quand vous demandez où www.bigbank est …. Mais il va dire je sais où il est le nom de serveur de nom de bigbank.com, donc la chaîne ainsi se complète. Est-ce que par on peut passer cette diapo où on peut faire le sketch au lieu de la diapo?

Donc, c'est encore plus complexe que jusque la description du DNS et donc j'espère que le prochain sketch va nous aider à démontrer comment tout cela fonctionne.

ACT 2

DAN YORK: Le DNS se sera illustré SA était illustré dans le premier acte, de ce que warren présenté et comment le DNS fonctionne, le DNS était sécurisé et ce que l'on va démontrer c'est l'attaque et milieu, c'est pour ça que le bien-être a été développé faisant répéter ce que nous avons fait tout à l'heure, nous avons faire encore et je vais aller payer leurs factures encore faire la même chose.

JOE: J'ai des factures à payer je voudrais aller voir M. ISP pour aller voir www.bigbank.com.

M. ISP: Merci, je ne sais pas où c'est mais je vais demander à la racine (root).

ROOT: Merci de me demander mais je ne sais pas du tout à aller parler à.com.1.1.1.1

M. ISP: Oui alors je vais aller là-bas.

.COM: Vous savez où se trouve bigbank? Je ne sais pas, mais je sais que ça se trouve 2.2.2.2.

M. ISP: Bonjour, vous avez l'adresse de www.bigbank.com?

BIGBANK: Oui je l'ai l'adresse pour bigbank.com est à 6.6.6.6.

M. ISP: Merci Beaucoup, voilà M. Joe utilisateur d'après ses 6.6.6.6.

JOE: Merci M. ISP, au moins je peux aller faire payer mes factures à www.bigbank.com, j'espère que personne ne cherche dans mes poches.

DAN YORK: Donc c'était l'acte numéro de, vous voyez que le docteur diabolique est la neige était une réponse avant que bigbank puisse répondre lui-même, et c'est comme ça que cela marche. Maintenant comment on met en place le DNSSEC, une des choses que vous avez dû voir ce qu'il y a deux sortes de serveurs, les informations de publication et aussi les informations de lecture, M.ISP qui lit les informations et ce que l'on doit faire c'est de trouver une façon pour eux d'identifier la formation, donc j'ai ce qu'on appelle une chaîne de confiance et c'est ce que la signature DNSSEC représente. Alors voilà ma signature.

M. ISP: Bonjour madame la racine, je voudrais faire ce truc de DNSSEC avec vous. Voilà mon information est comme ça vous pouvait savoir que c'est vraiment moi.

ROOT: Je vous confirme et voilà votre étoile, je confirme que c'est vous.

M. ISP: Bonjour.com, j'ai signé ma zone je suis le DNSSEC et je suis capable entends que bigbank.com et voilà ma carte qui établit cela.

.COM: Je confirme l'information.

DAN YORK: Alors voilà ce qui s'est passé là-bas et ce qu'ils ont développé ce qu'on en appel la chaîne de confiance suite ils ont authentifié les uns les autres, il y aurait donc une signature numérique sera passé entre les uns les autres, donc maintenant avec tout le monde qui est signé et donc nous allons répéter l'attaque de la personne et de lampes au milieu ou de la personne.

JOE: M.ISP je voudrais aller à www.bigbank.com.

M. ISP: Parfait, je ne sais pas où c'est mais je vais demander à la racine, je sais aussi que cette télé-là qui valide et qui me dit que c'est vraiment la racine.

ROOT: Je ne sais pas où bigbank est, mais je vais vous dire que vous pouvez aller au serveur.com.1.1.1.1. Et voilà sa signature.

M. ISP: C'est très bon ça à l'air d'être correct. Je voudrais aller à www.bigbank.com vous savais où c'est?

.COM: En fait je ne sais pas, mais je sais où est bigbank.com et je peux signer cette réponse pour vous.

BIGBANK: Je voudrais m'apparaisse pour www.bigbank.com, ah oui l'adresse est à 6.6.6.6.

M. ISP: Ce n'est pas une bonne réponse, ce n'est pas d'idées partez d'ici dégagez.

BIGBANK: Je suis vraiment content que vous ayez posé la question, je suis www.bigbank.com... 2.2.2.3 essais déjà signé.

M. ISP: Oui et ça c'est bon merci. Voilà Joe l'utilisateur est l'adresse est 2.2.2.3 essais validé.

JOE: Merci M.ISP maintenant je peux payer mes factures et j'ai pas besoin de me faire en erreur.

WARREN: On a fait beaucoup d'entraînement quand vous voyez, maintenant je pense que je vais passer la parole à Russ pour un exemple de la mise en place de DNSSEC est bien un guide des options de déploiement.

RUSS MUNDY: C'était excitant de faire cela, comme vous voyez nous nous amusons beaucoup et j'espère que ça aide à expliquer les réactivités qui sont inclus dans le DNSSEC, et alors quand vous regardez vraiment de détails spécifiques il y a beaucoup de choses complexes qui doivent être prises en compte et qui prennent place, mais quand vous prenez du recul et vous dites que ce que je veux que je peux faire pour commencer à mettre en place le DNSSEC, la réponse dans tous les cas et cela dépend de ce que vous faites avec le DNS, si vous n'êtes pas un opérateur de DNS qui fait vraiment et qui prend un DNS entend que FOCUS de leur baisse nette et de leur point principal de leur business si vous êtes un opérateur de registre, si vous êtes un fournisseur de serveurs enregistrèrent, si vous opérez beaucoup de choses au niveau DNS il y a plusieurs endroits que vous pouvez choisir et pour commencer si vous

êtes une entreprise avec beaucoup d'activités, et un ensemble de choses qu'il faut faire mais peut-être un peu différent.

Ce que vous avez besoin de verser d'examiner ce que le DNSSEC fait maintenant et les choses que vous faites au niveau des DNS, et comment est-elle différente pièce nous avait besoin pour permettre à mettre en place le DNSSEC et ce que je veux découvrir aujourd'hui. Donc si vous êtes par exemple un registre avec un gros TLD et des opérations importantes de TLD, vous avez probablement UN XXX DNS professionnel est là aujourd'hui vous faites est probablement essentiels de vos activités DNS avec votre propre personnel, vous avez probablement des gens qui sont experts est bien qualifié, si vous être notre genre d'entreprise qui fait des choses importantes avec le DNS mais peut-être qu'il idée que localise un petit peu, en indécence un peu plus en fait par des fournisseurs externes qui font le DNS pour vous et que vous voulez travailler avec ses fournisseurs externes, peut-être ils peuvent pas faire le DNSSEC par ce que beaucoup d'entre eux commencent à travailler sur le processus n'est certainement pas encore commencé.

Si vous êtes une activité qui fait des choses sur le côté en externe, le DNS n'est pas vraiment le parti important de votre business mais c'est important parce que votre business mais ce n'est pas votre FOCUS le plus important, peut-être vous pourrez faire cela de côté ça ne prend pas et vous pouvez peut-être faire cela en externe. Dans quelque soit la manière dont vous trouverez aujourd'hui, la première étape c'est de voir ce que vous faites avec le DNS aujourd'hui, si vous êtes comme Jacques ici et que vous êtes un ISP, une des choses préférées est un exemple référé pour moi c'est un groupe qui par exemple a fait

beaucoup avec xxx, aux États-Unis c'est comme xxx fournisseur d'ISP très important et tous les noms de serveurs qui sont mis en place dans le DNSSEC aujourd'hui, dont il y a des choses qu'ils ont fait pour faire marcher le DNS et pour leurs clients qui sont un peu différent de ce que par exemple Verisign a fait qu'il opérateur des.com et des.net, et quand xxx a aussi signé et ont authentifié.org ce sont toutes les étapes et il faut vraiment voir ce que vous faites comment vous le faites, si vous êtes une entreprise je me rappelle plus et ma vision n'est plus aussi bonne, je vais regarder sur la diapo.

Par exemple HP c'est une grande entreprise et une grande compagnie, de beaucoup d'expertise de DNS font toutes leurs opérations de DNS en interne mais ils en font beaucoup, ils sont sous le.com et ils sont déjà en place et ils peuvent signer et authentifier leurs hommes et toutes les hommes qu'ils administrent sous leur chapeaute. Et peu importe la manière dont laquelle vous faites le DNS aujourd'hui c'est ce que j'essaie de vous illustrer maintenant ce que vous devez voir ce qui suit, quels sont les éléments successifs si vous êtes une entreprise, vous allez opérer ou fournir des services récursifs et des serveurs autoritaires des noms ISP pour votre propre zone. Donc vous pouvez voir comment authentifier par la nature de la zone et c'est la chose la plus efficace pour commencer si vous êtes opérateurs avec des services autoritaires de nom, vous signez la zone et vous n'inquiétez pas ainsi les gens font la validation de DNSSEC dont ceux-ci mais ceci c'est votre zone est accoutumez vous à faire fonctionner la partie DNS par ce que il y a des changements dans le DNS normale.

Les changements qui doivent se produire c'est ce que j'appelle xxx à gauche c'est ce que l'on appelle souvent la phase d'alimentation que

vous soyez une entreprise ou une ccTLD, toutes ces choses s'appliquent pour toutes les zones, et de l'autre côté seul endroit où on met les informations si vous êtes une entreprise tour a lieu au sein de votre organisation, mais si vous traitez vos connexions avec le registre en, par exemple HP interagir avec le registre Erquy utilise pour arriver à.com et ils doivent échanger des informations avec le registraire afin que l'information puisse être placée dans le haut sommet du triangle, et ses consommés et distribués à droite, il y a beaucoup de protagonistes qui interviennent. Maintenant ce qu'il faut faire c'est examiner les pièces DNS, savez-vous où vous obtenez vraiment DNS est-ce que vous savez qui offert les serveurs de noms DNS vous dans la planification de DNSSEC, est de déterminer l'origine de tous les pièces de DNS, la première étape la plus importante qu'il faut faire. Donc ce que vous voyez ici c'est notre manière d'illustrer ce que je viens de dire, les informations sont saisies et ça entre dans le serveur autoritaire et ça été requit est demandée par l'utilisateur M.Joe, ensuite cela peut être présenté simplement d'une manière complexe si vous regardez il y a deux rangées, il y a les serveurs de racine de noms, il y a 13 lettres et dans la prochaine phase ça vous donne une idée des résolutions de requête de consultation de nom, et cela peut se produire dans un diagramme effectué par les outils que nous offrant au xxx pour www.CNN.com et il y avait plus de 100 consultations, mais maintenant c'est plus de 100 et c'est 120 sur CNN.com.

Donc j'ai bien fait, je n'avais pas le xxx mais c'est ce que le CNN.com fait maintenant, et que vous faites une consultation, donc la donnaient des hommes et le suisse qui est le plus important est ce que nous voulons montrer, c'est l'adresse IP pour www.bigbank.com et ce n'est pas

6.6.6.6 et c'est vraiment2.2.2.3 et c'est vraiment ce qui est important et ce que fait DNS pour vous, il vous faire ni la basse cryptographie technique qu'un usager de DNS peut prendre, prendre cette décision pour résoudre cette requête. Donc vous voyez le triangle à nouveau la partie envers celles-là où le DNSSEC fonctionne, lorsque vous analysez la partie gauche c'est la saisie des informations et c'est l'approvisionnement si vous avez un usage d'un an, vous allez à un registre un et l'alimentation et la notification se fait à ce niveau-là, une fois qu'il est introduit dans un serveur et qu'il est signé, ce sont les informations circulantes des requêtes et des consultations, il faut faire attention du point de vue de l'alimentation mais le DNSSEC résolu l'authenticité de source et le défi, il y a l'intégrité des données pour savoir si c'est la bonne information dans le bon endroit et qui vient du bon endroit pour vos désinformations DNS.

Si vous faites DNSSEC de la même façon que vous faites le DNS, c'est la bonne manière de procéder est faite de ce que vous faites avec le DNS et n'essaie pas de jeter les opérations de DNS et de remplacer par quelque chose de nouveau, parce que vous allez ajouter de la complexité parce que vous devez vous assurer que les opérations DNS fonctionnent avant que le DNSSEC fonctionne, et si vous regardez et ici une autre illustration avec elle que xxx additionnel avec une approche directe cela montre les endroits additionnels, mettre des obstacles additionnels pour assurer l'authentification pour que le consommateur des données DNS sache que cela vient du bon endroit et ce n'ont pas été interceptés pendant que il filait au long du Cable.

Ce que vous cherchez à éteindre vos opérations DNS, il faut analyser ce genre de choses. Les pièces qui placent les informations dans le DNS et

les pièces qui tirent les informations en dehors des DNS, il y a davantage de thèmes dans cette diapo qu'il en faut vraiment, mais on peut tout lire mais je vais simplement passer à la prochaine diapositive. Si vos opérations ou les produits de logiciels et équipements sont fournis à différents personnes, vous êtes allés au vendeur ou le fournisseur de services qui font les activités qui se rapportent aux DNS, et si vous dites que je veux faire le DNSSEC est-ce que vous pouvez m'aider pour faire le DNSSEC, et si il ne peut pas vous était enfin dans le DNSSEC c'est là où on peut commencer à l'avoir, et si quelqu'un vous fournisse le DNS qu'il puisse vous fournir le DNSSEC et que vous soyez une grande entreprise ou un opérateur DNS professionnel, il faut vous assurer que vos fournisseurs des produits et des services vont l'accepter. Et si tout pour la présentation formelle, et on veut vraiment que vous posiez et commenter ce que vous avez vu même s'il y a des choses que vous pensez que c'est complètement stupide dit que nous et on va essayer de les expliquer mais on veut vraiment répondre à vos questions et nous sommes là vraiment pour répondre à vos questions, vous avez des gens avec des microphones.

AHMED: Ma question est la suivante, à quel point ça va ralentir le trafic de l'Internet et exclura une influence?

RUSS MUNDY: En fait pas du tout, vous avez l'air est consigné dans ce que vous faites les requêtes normales et les réponses sont légèrement plus grandes, mais c'est une très très petite quantité et il y a un petit traitement supplémentaire lorsque les gens mettent en place des seuils et des

références et ça c'est seulement pour le bien-être et le reste n'est pas affecté, donc c'est vraiment négligeable.

DAN YORK: Une chose, nous avons de bonnes études là-dessus et c'est sur l'impact des fournisseurs de serveurs autoritaires une analyse efficace a été effectuée Wright quelques années auparavant c'est disponible en ligne ont beaucoup de formules et de détail pour nous en individuels, vous pouvez vous saisir de ce rapport et je ne me rappelle pas de chiffres mais c'est accessible, saisissez vos noms et voyez ce que ça peut être faire pour vous dans votre service d'autoritaire, on n'en parle des détails de donner qui sont disponibles sur les xxx de validation, ce que vous avez entendu parler du type de DNS Google, par des données publiques non, mais ce sont des choses qui sont perdues facilement pendant qu'on fait la mesure. Il y a des groupes qui essaient de mesurer la validation, et il n'y a pas un impact éducatif selon eux.

LENDAL MCDONALD: Je suis du programme de boursiers, ce que c'est coûteux de mettre en œuvre un DNSSEC?

DAN YORK: Ça dépend de l'immense palais de votre zone, Jacques vient de passer en revue certains processus avec le CA on pourrait en parler mais ça dépend du niveau de la sécurité et de précaution que vous lui intégrez dans votre environnement, il y a beaucoup une large gamme de choses qui peuvent être faits, la signature des différentes pièces avec des sources ouvertes et de cours minimaux comptaient à autre échelle avec

description de pièces de verrouillage qui coûte très cher, donc ça peut vraiment varier et ça dépend de vos exigences en matière de sécurité, ou si vous avez un opérateur ou une entreprise. Cela définit ce que vous allez parler de zéro avec toutes les logiciels à sources ouvertes jusqu'à très coûteux, plusieurs ccTLD qui l'ont fait, il y a une manière de voir que vous m'opérez de manière stable et même les ccTLD qui sont des environnements un petit peu complexe avec un type et quelques jours, si vous êtes une organisation pour vos propres buts vous pouvez le faire presque gratuitement.

Et pour le point de vue du côté de l'organisation, beaucoup de noms de serveurs autoritaires du côté sur les sonneurs également, le code de la vue l'allumait le DNSSEC et il faut finir d'ajouter une ligne au fichier de configuration ou bien cochée une boîte, et laissons les chômeurs de validation et tout est déjà là surtout pour du côté de validation.

RUSS MUNDY: Une chose que j'aimerais ajouter en particulier pour cette question, c'est que quand j'avais dis dans la présentation c'est vraiment les données et le contenu de la zone qui est important, c'est vraiment ce que vous essayez de protéger. Donc vous devriez étendre les efforts qui sont raisonnablement équilibrés à la manière dont vous protégez les données dont la scène elle-même. Donc si vous avez un processus qu'il arrache pour que les gens prennent et retirent les noms dans votre zone, effectuer les changements qui n'ont pas beaucoup d'attention et c'est une vérification minimale pour ne pas dépenser beaucoup d'argent sur les DNSSEC parce que vous dépensez davantage d'argent sur la partie crypto que pour la protection du contenu.

LEON: J'ai deux questions, si on utilise les services de DNS public de Google est-ce que ça vous donne un certificat de garantie, et comment un couple de domaine puisse contribuer au DNSSEC?

WARREN: Du côté de Google, il a récemment fait le DNSSEC sur les solutionneurs Google mais c'est encore dans un lancement qui va se passer très lentement. Et c'est pour les gens qui ont demandé cela spécifiquement, et dont le futur bientôt et peut-être très bientôt nous planifions devancer cela pour tout le monde. Donc si vous vous demandez 8.8.8.8 cela voudra automatiquement une réponse DNSSEC.

S'il y a une zone spécialement à très large où il y a un problème DNSSEC où il y a eu une erreur accidentelle, comme xxx a mis une place une encre négative et ce qu'il appelle une encre négative pour vérifier si la validation n'est pas faite, est à Google nous faisons la même chose et si il est clair pour la raison à laquelle la zone ne fonctionne pas et à cause d'une erreur temporaire, où il y a une possibilité de recevoir une réponse même si ce n'est pas sécurisé par le DNSSEC.

DAN YORK: Je vais parler pour que les parties privées puissent faire les utilisateurs, vous savez qu'il y a deux facteurs qui entrent en cause, de 300 domaines génériques il y a xxx qui sont signés si vous faites parti des 100, votre demande peut être signée et c'est la bonne nouvelle est cela peut fonctionner, et si vous ne faites pas parti vous devez voir si votre registre va supporter le DNSSEC, et dans certains cas il s'agit de jusqu'à

xxx, et de dire voilà laisser utiliser le DNSSEC, non il y a des registres qui le font automatiquement comme.DR Le font beaucoup dans leur région et certains en Hollande et en République tchèque aussi.

Si vous utilisez un.com et un.net, vous devez utiliser un registre qui le fait déjà les lois afin qu'ils le font déjà et ICANN a une tache sur leur site qui donne une liste des registres à qui supporte le DNSSEC jusqu'à présent. Vous pouvez donc aller voir dans certains cas mots sur les personnes moi j'ai demandé à mon franc registre contagieux peux obtenir telle ou telle chose, il m'arrivait de bouger et d'aller vers un monde votre nom de domaine parce que je voulais qu'il y ait une authentification et j'ai dû faire aller bouger patiemment donnant sur un autre registre pour que cela puisse fonctionner, du côté du registre cela dépend comment vous voulez inclure dans le processus et je vous experts il y a des idées et j'en ai un sûrement l'ordinateur est ainsi ce qui s'appelle une trigger DNSSEC qui permet de valider et de sélectionner un valideur sur mon système. Par exemple le sketch que nous avons fait ici, c'est une des choses que je peux vous configurer, quand je vais marche ce logiciel dans mon système ça me demandera Google, vous pouvez soit signés votre domaine du côté signature ou du côté de validation et vous pouvez voir si votre ISP supporte le DNSSEC et si il ne le fait pas pouvait leur demander et vous pouvez installer le logiciel qui ne correspond, il y a de chrome et safari qui fournit des signaux de validation aussi.

JULIE HEDLUND: Nous avons une fille, il y a quelqu'un il y a M. Labat et il y a un autre monsieur ici et j'ai vu un autre doigt qui s'élevait là-bas, nous avons quatre personnes dans la file d'attente pour des questions.

DAN YORK: Si vous opérez votre propre nom, et que vous n'avez pas une chaîne et que vous pouvez toujours signer il y a personne. Vous pouvez le faire vous-même et vous pouvez intégrer à l'intérieur de vos processus que vous ayez une chaîne jusqu'à la racine ou pas, il y a un nombre de capacités de culpabilité DNSSEC trigger, c'est une très bonne. Mercredi vous entendait plus parler il ouvrirait le moteur de recherche que nous avons élire dans des outils aujourd'hui sur le marché pour faire une génération du DNSSEC, ici une fois que vous allez un peu essayer de les utiliser et donner du suivi au développement de ces xxx oh excusez-nous.

RUSS MUNDY: Je voulais juste dire que les formulaires que nous avons distribué dès URL, donc aller voir ça.

QUESTION: Je m'appelle (nom) je travaille au DNSSEC en Chine. J'ai deux questions, la première c'est à ce que vous avez des dates pour montrer combien ou des données qui montrent combien de serveurs où le taux de serveurs qui employaient le DNSSEC? Est la deuxième question c'est si le serveur DNS est contrôlé par une encre, à ce que le DNSSEC peut toujours être utilisé dans ces situations?

RUSS MUNDY: Donc pour répondre à votre première question, il y a de nombreux points de donner est la chose la plus simple ce serait de voir si le déploiement dans le ccTLD. Il y a une carte qui montre le déploiement du DNSSEC sur le site 360 qui montrera dans l'avenir combien de ccTLD ont été signé ou on identifie, il y a des comptes qui ont été faits autrement mais celui-là est certainement le plus visible est la meilleure manière d'illustrer la croissance jusqu'à présent. Voyons la zone ccTLD et ceux qui ont été signés, cela peut vous donner une idée de la croissance.

Donc si un hacker prend le contrôle d'un serveur de nom avec le DNSSEC, qu'est-ce qui peut être vraiment authentifié pour l'utilisateur final qui utilise la formation de DNS, si les données elles-mêmes et passent tous ces données viennent, mais d'où elle vient et la personne qui en est à l'origine du DNS, si il y a un serveur milieu qui pourra avoir des informations ou qui a la mauvaise information dans la cage, et qui envoie un sélectionneur de validation. Donc là il aura des questions et les données ne seront pas authentifiées et donc abandonnées, si le hacker a le contrôle de la machine qui fait l'authentification et la signature cela veut dire qui contrôle la machine, et donc la paix pourrait causer des dommages. Si ils vont du côté provisions de data xxx, donc les mauvaises données de data sont signées par le DNSSEC, et donc le sont les chômeurs de validation ne pourraient pas voir la différence parce que ce serait signé et donc la faiblesse et que du côté provisionnement du côté gauche du triangle, et donc voilà la carte.

DAN YORK: C'est une carte qui a été mise en place par une compagnie qui s'appelle Chinkura et cela vous montre l'adoption, enfin l'adoption du DNSSEC qui se passe du côté de cette opération ne nous cela était planifié, il y a beaucoup de d'autres cartes qui sont basées sur les régions, il y a des cartes qui sont animées aussi et qui montre les tendances, et mercredi si vous venez à la session de travail de DNSSEC que nous allons mettre en place, vous verrez qu'il y aura plus de détails et il y a des gens qui sont là et qu'ils sont là d'aller en ce moment et qui parleront des statistiques que nous avons, et donc ce sera une séance plus approfondie pour mercredi.

JULIE HEDLUND: Si vous ne voyez pas ce graphique et cet organigramme pour les gens qui ne sont pas dans la salle, nous vous recommandons d'aller voir la représentation pour le DNSSEC et la session de travail de DNSSEC mercredi par ce que cette carte que nous parlons maintenant n'est pas sur le serveur adobe connect sur lequel vous êtes à distance en ce moment, donc il y aura une parleront plus de cela dont la session de mercredi.

RUSS MUNDY: Prochaine question?

MOHAMED: Je m'appelle Mohamed et je suis du Bahreïn je voudrais vous remercier pour ce petit sketch, j'ai deux questions à propos du DNSSEC, quelles parties sont inclus dans les transactions de DNSSEC? Est-ce que ça va jusqu'_à l'utilisateur final ou enregistré un qui veut mettre en place un

DNSSEC? Au niveau d'utilisateur final à s'il y avait quelque chose de nouveau nous avons de conférence spéciale, par exemple sur mon ordinateur? Et la deuxième question c'est pourquoi il y a une signature entre la racine et les autres sous racine, par ce que je pense que c'est assez bien défini à l'origine, donc comment vous l'avez démontré tout à l'heure, ses racines sont déjà bien définies. Donc quand ISP va vers le.com, pourquoi est-ce que la racine doit signer la transaction alors c'est déjà bien défini.

RUSS MUNDY: Je veux répondre à la première question en premier, DNS par nature si vous vous rappelez de la diapo tout à l'heure et commence à partir d'un point, et ensuite il descend par étapes remontant vers la diapositive. C'est l'information sur la structure de la formation du contenu du DNS, chaque personne qui existe ou qui exigent des informations qui demandent un DNS, un sélectionneur de telle sorte il sait où commencer, et chaque collectionneur qui fait beaucoup de travail et beaucoup de recherche est ce qu'un appel de la recrûssions, il sait déjà où il est le serveur de nom et il n'a pas besoin de savoir d'autres choses, il y a une boîte simple pour la racine et il y a d'ailleurs beaucoup plus de machines et il y a beaucoup de machines qui veulent vous fournir cette réponse. Le DNSSEC par design il est fait pour être une partie un transit et c'est la raison pour laquelle la dissuasion de la signature a été faite.

L'équivalence de dire je sais où l'adresse IP du serveur de racine elle est, donc tout commence par la clé publiée pour la racine est elle descend vers le bas. Je dois donc en parallèle avec la structure du nom lui-même.

DAN YORK: Il y a une réponse plus simple, M. le méchant ici ils pourraient représenter des signatures et donc signées des hommes est présenté cette apparence mais si ce que l'on appelle l'achat de la confiance globale de la racine jusqu'au roi lorsque l'on regarde cela lorsque il regarde cela ils vérifient la signature pour qu'ils remontent jusqu'à la si la racine, de danser pour ça que vous avez besoin de cette chaîne pour que l'attaquant ne voudront pas quelque chose que lui il dit que c'est signé, mais non ce n'est pas la signature que vous êtes supposés utiliser.

WARREN: Je vais essayer de répondre cela autrement, j'aurai trois manières de y répondre. Les signatures numériques utilisent la cryptographie, vous avez une clé publique est une clé privée et tout ce qui est utilisé par la clé privée peut être décrypté avec la clé publique. La clé privée c'est comme la signature, lorsque vous allez à la racine la racine elle dit que je connais la réponse mais je ne sais pas où il est www.bigbank.com se trouve mais je sais où se trouve.com est passée la clé publique et voici ma signature qui dit que c'est correct.

MOHAMED: Pourquoi le serveur de racine dont parlent les adresses IP, et par des clés signé parce que les services. On sent bien défini?

WARREN: Il y a beaucoup de TLD différents donc ceux qui sont.com sont bien connus, mais lorsque le nouveau TLD ce n'est pas connu. Il y a des millions de résolusioneurs dans une seule zone racine, maintenant il y a 13 adresses en fait et ainsi des millions et des millions de sélectionneur ne doivent connaître une série d'adresses et ils n'ont pas besoin de

savoir 100 000 ou 1 millions, il y a plus de 1 millions de zones de bien au-delà de 1 millions de zones puisque les sélectionneurs ont dû savoir où se trouvait la racine, il y a rien qui vous empêche d'avoir d'autres clés que vous connaissez et vous n'avez pas besoin de valider, et si vous faites ou si vous avez une entreprise ou un pays et que vous voulez avoir tous les sélectionneurs de votre pays d'où veut ou de votre entreprise, avoir la partie des informations publiques en a pas besoin d'aller jusqu'à votre approvisionnement, vous pouvez l'être à partir de là mais plus agrandie et plus c'est compliqué. Donc si on garde cela et on garde ça petit dans la zone racine on apprend que c'est le meilleur pour Internet global, mais cela n'empêche pas ce que l'on appelle des ancrages de confiance pour des hommes et des régions plus petites.

DAN YORK: Vous pouvez répéter la première question?

MOHAMED: Je pose la question sur quelles parties sont impliquées dans la transaction DNSSEC, est-ce que ça va jusqu'à deux usager final?

RUSS MUNDY: La politique est toujours important, et c'est ICANN est donc on doit parler de politique et il y avait beaucoup de documents très tôt pendant les activités de DNSSEC, est bien besoin d'avoir une politique générale, la conclusion pour le design et technique de ITF on va vous dire comment faire toute la protection cryptographie, mais la déclaration pour savoir ce que doit être la politique par-dessus et pourtant là dessus va au-delà de la définition technique, il y a quelques mois et surtout

dans la zone racine des ccTLD qui ont émis des informations de politique et des affirmations de politique et notre signature de notre sens de veux dire cela, cela va être opéré de telle manière mais ce n'est pas une nécessité absolue de DNSSEC d'avoir la signature.

WARREN: La réponse est parfois un petit peu plus complexe en ce qui contient… Actuellement la machine des usagers finaux ne font pas grand-chose avec ses informations, la machine des usagers parfois finir par s'impliquer et la part de CS DNSSEC aura lieu dans votre machine, il y a des gens qui intègrent la résolution dont l'application est donc il y a des gens qui font la validation DNSSEC à l'intérieur des applications et d'autres voient comment il a jeté au système d'exploitation se, pour le moment donc ce sont les ISP qui font parti avec le temps ne se sera reléguée au système d'exploitation.

DAN YORK: Nous fonctionnons avec le DNSSEC, nous avons à peu près 4 % des registres très qui offrent du DNSSEC. DNSSEC est en place pour de bonnes raisons, je suis intéressé de voir quelle sorte et quels genres de choses ont été faits pour aider à éduquer la population générale pour qu'il y ait plus de demandes pour que le registre est le comprenne les besoins d'argumenter et mettre en place le DNSSEC.

DAN YORK: Je vais répondre à ça parce que c'est un programme avec lequel je travaille, nous essayons de faire cela et nous essayons d'amener plus de demandes. Donc durant l'année dernière ne vous avez raison il y a cette

facilitation de la poule et l'œuf, nous avons besoin de plus de demandes que nous avons ce problème depuis deux jours, on dit pourquoi je devrais valider, il n'y a pas de validation il n'y a pas de demande est l'autre côté les gens disent pourquoi je devrais cinémas en parce qu'il n'y a pas trop de sélectionneur en place, mais mes collègues ici m'ont beaucoup aidé pour cela et vous aussi êtes ailleurs, les Google le fait que il l'encourage les Google pense que c'est important, et si les gens pensent que les Google il pense que c'est important alors les gens vont penser que c'est important pour eux aussi, c'était une bonne étape et cela nous a beaucoup aider et j'ai vu que le trafic a augmenté depuis, depuis une chose que nous entendons et que nous entendrons nous avons parlé dans notre réunion de mercredi, on va entendre les gens qui utilisent et on va parler de Dane, cela fournit une autre couverture de responsabilité.

En fait vous voulez que les gens utilisent cela, et nous pouvons ajouter une autre couverture de confiance en utilisant le DNSSEC, et il faut donc amener plus de demandes et il faut donner plus de validation et au gens pourquoi ils doivent le faire, au-delà de cela nous laissons ici et d'autres beaucoup d'entre nous travail sur la manière pour amener plus de demandes et pour qu'il y ait plus d'intérêt au niveau exécutif et au niveau des ingénieurs pour qu'il y ait plus d'informations, et pour donner plus d'outils pour provoquer cette demande, c'est devenu plus impliqué et vous savez vous n'avez que à utiliser une puce en ligne et il y a des choses qui se passent pour que tout soit simplifié et pour que nous puissions faire passer le message et pour montrer que c'est important et pourquoi. Donc ça vient.

RUSS MUNDY: Je pense que c'est une très bonne question, nous devons continuer à nous poser ces questions et nous avons beaucoup de gens ici qui ont été et qu'ils étaient engagés pour essayer de générer une demande, et ont nettement c'est une raison ou laquelle nous avons démarré cette session, nous avons essayé d'essayer de les faire comprendre les gens. Donc voilà comme ça vous pouvait comprendre qu'on peut avoir la fumée bleue pour arriver à créer les messages, si nous continuons à travailler pour les gens et expliquer aux gens qui ne comprennent pas vraiment ce qui est le DNSSEC et comment cela fonctionne, je pense que cela aidera les gens à comprendre que cinq ans les activités et leurs activités sur Internet beaucoup plus sécurisé.

ORATEUR: Oui je voulais juste dire que la République tchèque a eu beaucoup de réussite avec un set mis en place, André est ici et ils pourraient vous en parler.

RUSS MUNDY: SIDN est ici et ils ont fait beaucoup de travail ces gens-là, les Suédois aussi ils ont fait beaucoup de travail là-dessus dans tous les endroits, si vous voyez ce qui se passe autour de moi les gens travaillent des deux côtés et surtout la République tchèque et la Suède et les Pays-Bas aussi, ils ont beaucoup travaillé et ils ont travaillé aussi sur l'augmentation des authentifications.

QUESTION: Bonjour, merci beaucoup. Je suis xxx de Fennec et en tant que registre xxx qu'il allait appliquer le DNSSEC dans l'avenir proche. Je voudrais que

vous puissiez nous donner des conseils pour qu'on fasse moins d'erreurs lors du déploiement du DNSSEC ou dont les premières étapes du déploiement de DNSSEC, peut-être dans le processus de déploiement de DNSSEC et ensuite du côté des opérations.

JACQUES LATOUR: Oui je pense que je peux répondre à votre question, ce dont vous parlez c'est la validation pour que vous soyez sûrs de ce que vous faites et que c'est à 100 % bons, et à.CA nous avons passé beaucoup de temps à développer des solutions autour de ce sujet et nous avons xxx avec les ccTLD qui ont sorti en premier, nous avons fait quelques erreurs ici et là, et nous avons défini une des spécifications assez avancées fonctionnelles de comment nous devrions mettre en place le DNSSEC pour nous assurer que cela soit adéquat. Aujourd'hui il y a beaucoup de technologies et de signature il y a bien d'autres alternatives, et à la fin ne sont venus avec une technologie double, une somme de signature avec un logiciel de ce DNSSEC et nous validons les informations qui en sort pour nous assurer que aucun des logiciels a fait une erreur.

Si vous validez avec de technologies, les chances que vous ayez le même bug deux fois sont vraiment faibles, cela est disponible en ligne vous pouvait aller voir et les représentations là-dessus et vous pouvez regarder l'architecture de notre solution, en fait vous devez passer beaucoup de temps pour vous assurer que vous signiez de bonnes manières et débarrassant et ensuite vous pouvez vérifier la validation et nous faisons 16 tests différents pour nous assurer que les signatures sont valides et qu'ils ne sont pas expirés, nous avons pris et passer six mois de suivi et nous avons trouvé des bugs dans les DNSSEC que

d'autres gens n'avaient pas de découvert, si vous voulez on peut en parler et c'est très important que vous passez du temps sur vos validation avant de commencer.

RUSS MUNDY: Une des choses que je voudrais suggérer que Jacques n'a pas mentionné, les machines que vous allez utiliser pour faire la validation de ce qui est produit par votre mécanisme de signature, vous devrez aussi faire des ans de tests contre le validateur qui ont des informations de façon intentionnelle, et de façon à ce que vous puissiez identifier cela. La première étape serait que votre valideur fonctionne bien et vous faites cela en lui envoyant des données qui sont mauvaises, vous savez que ces données sont mauvaises et il y a des outils pour faire cela, dans votre valideur vous savez qu'il va être opérationnel. Je pense que c'est le message que nous ne voulons faire passer est planifiée pour les problèmes contingents.

QUESTION: Je suis du Yemen, je mets en place des technologies et ce qui m'intéresse c'est de comprendre la détection des headers, disant qu'en le trafic, par ce que les headers sont en général simple au départ, je pense que ici il y a de la vulnérabilité pour le DNS et que vous avez pensé à crypter les headers et à maximiser le potentiel des abus. À côté de la certification que vous faites des gens, peut-être une courbe pour le DNS qui pourrait être introduit.

OLAF KOLKMAN: J'étais le président du groupe de travail lorsque le DNSSEC a été standardisé, et la confidentialité était spécifiquement une non exigence et on a décidé de ne pas travailler là-dessus parce que les données DNS étaient publiques est transmis pour l'éternité, et c'était une non exigence. Également les mécanismes de confidentialité et de la protection de la vie privée et le mécanisme également il offre des mesures de contrôle.

RUSS MUNDY: Il y a plusieurs manières d'assurer la connexion et le système local, donc on peut en parler hors ligne également.

DASHA VLADIMIR: Bonjour je suis de Russie, j'ai deux questions sur la mise en œuvre de.RU quels sont vos impressions sur le succès et sur la mise en œuvre? Je regarde le statut DNSSEC pour aujourd'hui et il montre que la Chine est en phase expérimentale, qu'est-ce que cela signifie et combien de temps ça va les prendre pour le mettre en œuvre? Vous pouvez comparer ces deux expériences?

RUSS MUNDY: Je ne connais pas l'historique de Chine, M. expérimental depuis longtemps parce qu'ils travaillent sur plusieurs choses et mercredis vous entendraient une opération sur leur plan et il y aura une diapositive et vous pouvez voir spécifiquement leur plan à venir, et vous pouvez parler à ce monsieur, et sur la carte elle-même il y a différentes dégradations des stages des différentes phases, beaucoup de la complexité est-il tant impliqué, enfin Jean-Jacques parlait du travail qu'ils ont fait là-dessus

est si difficile à comparer en raison de la dimension l'équipement et la vie politique et les procédures, on peut pas faire une comparaison facile là-dessus en raison de ce qui s'y trouve.

JACQUES LATOUR: Ca nous a pris un an pour signer.CA et notre xxx a pris 20 minutes pour signer zero.CA.

DAN YORK: Je ne connais pas les spécificités de.RU mais je sais que ça a été signé récemment.

RUSS MUNDY: Je connais bien la carte et la méthodologie de collection et de Colette, j'ai travaillé de près avec Chinkara sur ce projet, les données collectées c'est vraiment par des bénévoles, et je me demande dans quel état vous voulais investir vos efforts, il y a des paramètres descriptifs et si vous faites ceci alors vous êtes probablement là, la spécifité quant à la durée qu'elle prend à une étape particulière, elle relève totalement l'entreprise et en ce qui concerne la collecte d'informations, lorsque que vous pourrez passer la prochaine étape parfois les gens disent et parfois les gens nous disent pas, même si ça a la même couleur sur la carte sait des choses indépendantes et donc c'est difficile de faire une comparaison.

DAN YORK: A l'exception que sur cette carte une fois quand ils sont sur le vert c'est là que on peut valider, nous ne savons parce que les dossiers sont

publiés, on ne peut pas vous donner une meilleure réponse malheureusement.

QUESTION: Je suis de Palestine, je veux parler de la durée de signature est ce que ça peut être mesuré?

DAN YORK: La signature que vous posez comme question. À l'intérieur de chaque signature il y a une date d'expiration, Donc la durée de vie de, donc il y a un document qui a été publié récemment et qui a souligné les meilleures pratiques et cela varie, souvent les gens vont publier pour voir la différence et les différents qu'il est utilisé pour les donner deux hommes, c'est peut-être pour un mois ou trois mois et il y a une autre clé qu'on utilise pour signer qui peuvent durer un an et il y a un document n'en peuvent vous orienter vous verrait les recommandations spécifiques qui s'appellent les directives versions 022 opérations de DNSSEC. RFC 6781 voilà vous y retrouverez les recommandations.

NICHOLAS: Je m'appelle Nickolas et je suis dans le programme de boursiers et je suis curieux de savoir l'algorithme de description pour la poignée de main, où l'amalgame. Est-ce que c'est un algorithme discret ou une factorisation de zone?

DAN YORK: On peut encore une fois, il y a plusieurs algorithmes qui sont autorisés et nous avons défini 05, les cryptographies je ne peux pas les nommer

tous mais il y a plusieurs deux variations SHA, RSA, SHA1 et SHA3. Et c'est configuré pour que vous puissiez ajouter des protocoles additionnels.

ORATEUR: Je vous ai entendu dire poignée de main.

DAN YORK: Non, je voulais juste clarifier que je fais une signature et je communique quels sont les paramètres que j'ai utilisés pour faire cette signature et je m'attends à ce que le client valide, il n'y a pas de poignée de main il n'y a rien.

RUSS MUNDY: En partie de la signature, dans la signature du DNS xxx on peut permettre l'utilisation de l'algorithme, le validateur sait exactement quel est l'algorithme et il y a des gens qui travaillent sur certains qui font de la photographie de courbe, il y a aussi des autres algorithmes qui se sont ajoutés.

THOMAS: Registre allemand pour les structures privées et publiques, c'est très important que le secteur, et je voudrais savoir qui ont en charge est responsable de la clé racine et si la clé racines est compromise, est-ce que tout le DNSSEC et le processus de DNSSEC de résolution, qui est responsable?

RUSS MUNDY: Il y a une approche très bien documentée est très bien publié qui discret et décrit tout cela, ICANN et l'identité et l'entité fondamentalement responsable des clés de la zone racine, mais il y a un grand nombre de personnes de la communauté qui doive être présents lorsque quelque chose est fait en respect de la clé de la racine, il y a beaucoup de protection de disque dur et de protection physique de redondance et il y a beaucoup de deux communications là-dessus et vous pouvez aller en ligne et vous pouvez voir élire les archives sur les activités de signature de clé. Il y a un rôle dans le mécanisme de ICANN qui aide à qui il n'y a pas de compromis, et tout cela ne soit pas compromis. C'est un point simple de faire des chèques et si cette clé est compromise nous aurons un grand problème, il y a plus d'inquiétude que la clé soit détruite par accident.

WARREN: Y a que plus de concerne que quelqu'un que cette clé soit détruite, mais il y a beaucoup aussi de discussion en ce moment et comment nous irons la clé Racine. RFC-5011 en fait partie et ça n'a pas encore été testé, donc en théorie beaucoup de gens se rassemblent pour générer une nouvelle clé, mais ce n'a pas été testé encore de façon pratique et donc il n'y a pas vraiment une façon de comprendre, est-ce que l'on doit attendre que quelque chose de très mauvais se passe, il n'y a pas de politique autour de sa je pense qu'il y a une discussion actuelle en ce moment.

DAN YORK: Il y a deux aspects en premier pour répondre à vos questions, les documents dont on parlait si vous regardez en ligne pour le DNSSEC et

les politiques et les déclarations de politique de DNSSEC, vous trouverez les politiques qui sont déjà en place, les TLD qui sont signés ont déjà publié leurs propres xxx et déclare ce qu'il y a là-dessus. Si vous allez voir sur DNSSEC de ICANN je pense que c'est root.dnssec.org et tout cela est déjà là, les gens qui cherchent et qui veulent savoir comment signer leur ccTLD, allez voir les déclarations de DNSSEC parce que il y a des documents qui se réfèrent exactement à cela.

Quand il s'agit de la consultation, ICANN à une annonce pour un commentaire public et ça commence le vendredi le 2 avril, ils ont besoin d'information et de suivi et cela va vers le tout les meilleures pratiques, et il y a la clé pour signer la clé xxx et les clés qui sont utilisées pour signer les Data courant. Il y a donc des niveaux de protection, la clé au coeur de tout cela je ne peux pas en tant que… Ça doit être lancé durant les premières cinq années et c'est sous discussion en ce moment, et ICANN veut entendre vos commentaires là-dessus, ils ont mis en place une consultation et vous pouvez aller sur le site a été si vous voulez faire des commentaires.

JULIE HEDLUND: Pour la session de mercredi, il y a… Je voulais vous dire aussi que ICANN et Yab Ackerhaus du conseil il parlera de ce problème. SSAC consulte aussi ce problème et ils rejoindront la discussion mercredi, je pense que ce sera intéressant, je pense si vous intéressez-vous de veiller venir. Nous avons déjà dépassé le délai de cette session, est-ce qu'il y a quelqu'un qui aurait la dernière question avant que nous nous fermions cette session?

RUSS MUNDY: Merci beaucoup, très bonne question est très bonne interaction et si vous avez besoin de plus d'informations sur le DNSSEC, on commence à 8:30 mercredi matin par ce que nous avons une grande journée à planifier, si vous avez encore plus de questions venez mercredi.

JULIE HEDLUND: Il y aura le déjeuné mercredi mais vous devez participer à la session pour avoir ce déjeuner.