ABOU DABI – Atelier sur les DNSSEC - 3ème partie
Mercredi 1 novembre 2017 – 13h30 à 15h00 GST
ICANN60 | Abou Dabi, Émirats arabes unis

JACQUES LATOUR : Troisième partie de l'atelier DNSSEC. Nous allons prendre quelques minutes. Nous allons commencer. Vous m'entendez ? Nous allons commencer dans quelques minutes. Nous allons avoir une démo. Nous allons donc nous assurer qu'on puisse la visionner. Merci. On commence dans quelques minutes.

Et bien, bienvenue à toutes et à tous à cet atelier du DNSSEC, troisième partie. Nous allons avoir Wes Hardaker qui va faire une présentation sur la racine locale, LocalRoot. Nous allons donc sans plus attendre lui donner la parole.

WES HARDAKER : Très bien. Donc par curiosité, combien d'entre vous ont un résolveur récursif sur votre infrastructure ? Un bon nombre d'entre vous ? Combien gèrent ces résolveurs récursifs ? On peut leur dire quoi faire à ces résolveurs.

Alors aujourd'hui, je vais vous parler... Donc on va mettre cela sur l'écran tout entier pour la présentation. Voilà, on va faire cela. Ah, il semble qu'on ait perdu le document. Voilà. Très bien.

Donc, combien d'entre vous sont familiers de RFC 7706 ? Voilà, très bien. Donc vous êtes au courant de ce document. Très bien, c'est parfait. Ce qui est important au sujet de ce document et de son contexte, c'est de nous permettre de desservir la zone racine à partir de votre réseau local sans avoir à parler à la zone racine. Alors cela s'appelle LocalRoot, la racine locale. C'est un projet qui va vous permettre, donc, de télécharger des données de la racine dans vos résolveurs.

Premièrement, c'est quoi, LocalRoot, la racine locale ? LocalRoot en anglais, c'est un projet un petit peu de recherche qui vous permet, donc, de mettre ces données sur la racine. Donc voilà la résolution classique du DNS que vous voyez à l'écran. Vous avez une liste de clients. Ils essaient de trouver des pages web, ils passent par des résolveurs, ils font des mises à jour automatiques, ils travaillent à un ISP, donc un prestataire de service internet. Vous avez donc des résolveurs récursifs, et chaque requête qui est envoyée à ce résolveur parle au reste de l'infrastructure du DNS. Par exemple sur la droite, vous allez voir qu'il y a la zone racine .com, org, .example, example.com et icann.org. Voilà. Vous voyez [inintelligible]

Ça, c'est un exemple tout à fait classique. Moi, je veux aller à www.example.com. Vous avez un envoi qui part vers la racine en premier, et ensuite de la racine, il est responsable simplement de faire l'itération suivant, c'est-à-dire .com. Et ensuite, question

sur .com., requête, et on arrive enfin à example.com. Donc vous avez idée de ce concept.

Vous avez également une cache. Cela se rappelle que .com existe, que example.com existe, mais cela n'aide pas si le prochain client vient demander icann.org parce qu'org n'était pas le cache encore. Il n'y avait que com. Vous voyez, il faut recommencer le processus au départ. Cela aide.

Je ne suis pas grand fan d'Adobe Connect. Excusez-moi. Mais tous les clients vont demander exam.com. Donc étant donné que le résolveur est déjà au courant de .com, pas de problème pour com, mais il faut chercher exam. Donc vous voyez, il y a beaucoup moins de flèches sur l'écran parce que dans le cache, il y a déjà com.

Donc voilà ce que je propose de changer avec mon projet, que l'on puisse tous se connecter et mettre cela dans son propre résolveur donc, avec une racine plus locale, avec LocalRoot. Ce sera donc une pseudo-cache. Je vous donne toutes les informations sur la racine. Donc dans le cache, vous avez tous les TLD qui existent, com, org, net, cx pour les pays, horses. Donc c'est une pseudo cache que l'on utilise à ce niveau que l'on pourrait créer.

Et ce que cela signifie c'est que la résolution du DNS avec LocalRoot en place, et bien, vous avez beaucoup moins... Vous

voyez des flèches. Il y a déjà toutes ces informations dans le résolveur, donc il n'y a pas besoin de demander à la racine quoi que ce soit, donc on sait ce qu'est .com, .org, .net et ainsi de suite.

Alors, mon projet LocalRoot permet également de garder le résolveur local à jour. Et ça, ça le fait en envoyant des notifications DNS, comme si vous étiez un esclave de la racine pour une infrastructure locale. Donc ce qui se passe, c'est que lorsque la racine change, et bien le serveur local va dire : « Va chercher une nouvelle copie ». On est toujours à jour avec cela.

Alors pourquoi utiliser LocalRoot ? Pourquoi on fait cela ? Différentes réponses. Lisez RFC 7706 et vous verrez pourquoi c'est utile. Vous l'apprendrez dans ce document. Il y a beaucoup de délais lorsque l'on travaille sur une infrastructure qui est mondiale. Donc une pseudo cache permet de limiter les besoins de contacter la racine. On ne se préoccupe plus de la racine, et on a donc une plus grande rapidité au niveau du DNS pour rechercher le premier TLD. Donc ça se compte en quelques millisecondes.

Vous avez également la possibilité de savoir ce qui n'existe pas. Lorsque vous tapez, par exemple, eBay dans votre navigateur, la plupart des navigateurs disent : « Est-ce que vous vouliez dire eBay ceci, eBay cela, eBay.com... ? » Cela recherche beaucoup

de choses. Si vous faites cela, vous avez une résolution négative. Mais je ne sais pas si cela existe peut-être maintenant. Mais cela prend un petit peu de temps. Vous avez des réponses négatives. Donc vous avez une cache pour certaines réponses. Si vous allez demander eBay cinq minutes plus tard, cela ne va pas avoir de rappel de mémoire. Donc à la fois, vous allez avoir une copie mise à jour et cela peut-être un projet de recherche. Vous-même vous pouvez le faire, vous pouvez avoir des notifications du DNS, vous pouvez lancer des évènements. Il y a beaucoup de possibilités avec ce mécanisme de souscrire aux notifications inbound.

Donc au niveau de la sécurité, ce qui est très bien, c'est signé, il y a une signature. Donc on ne se préoccupe pas de l'arrivée des données. Et les données qui vous arrivent, ce sont des données qui répondent aux critères IANA. Donc tout le monde peut faire confiance à ces données. Et on transfère les données en utilisant la sécurité TSIG. Donc il y a une clé TSIG, et c'est une obligation. Il y a des gens qui disent que vous n'avez pas beaucoup plus de sécurité. Moi, je ne veux pas rentrer dans les détails, mais cela utilise, en tout cas, une sécurité TSIG. On pourrait peut-être mettre cela comme caractéristique optionnelle à l'avenir.

Donc démonstration. Plutôt que de le faire en direct, avec ces problèmes Adobe Connect, nous allons le faire avec des captures d'écran. Donc je m'excuse, c'est un petit peu petit pour

le lire sur l'écran. Donc vous allez sur LocalRoot.isi.edu. C'est une racine locale. Il y a donc des liens pour des informations sur les racines locales. Vous pouvez lancer quelque chose, vous avez quatre étapes pour avoir un résolveur. Puis la première chose que vous devez faire, c'est que vous devez vous inscrire. Donc vous taper votre adresse courriel et un mot de passe. Vous faites éventuellement une capture pour s'assurer que vous êtes bien un être humain, un test de Turing donc. Et une fois que vous êtes branché, connecté, c'est très simple. Premièrement, comme je l'ai mentionné, vous avez un lien pour avoir des documents pour savoir comment cela fonctionne. Vous devez créer une clé TSIG. Donc vous avez les quatre étapes, voilà. Et après ces quatre étapes, vous aurez donc un résolveur en place.

Voici une liste des clés TSIG. Cela nous dit qu'il n'y a encore aucune clé de générée. Donc vous cliquez, vous allez avoir un formulaire à remplir, vous pouvez mettre ce que vous voulez, vous donnez un nom à la clé, n'importe quel nom. Moi, j'ai mis « my cool TSIG key », ma clé TSIG cool. Et voilà donc, cela vous donne un algorithme et une valeur. Vous n'avez rien à faire avec cela. C'est automatisé. C'est configuré mais c'est une liste de clés qui existe. Vous n'avez pas à copier les valeurs.

Donc ensuite, vous passez à la liste de serveurs. C'est les résolveurs. On devrait changer ce mot. C'est une liste de résolveurs plutôt que de serveurs. Donc ce que vous voulez, où

vous vous voulez déployer votre racine locale, donc « Ajouter un nouveau serveur ». En dessous de cela, il n'y a que trois champs à remplir : nom administratif : vous pouvez l'appeler ce que vous voulez, donc le nom d'hôte de votre serveur, par exemple, c'est comme cela que l'on considère nos machines ; donc l'adresse protocole internet, IP – je n'ai pas IPv6 je crois là mais... ; quelle clé TSIG utiliser. Si je n'en n'ai qu'une, cela m'a déjà donnée ma clé. Vous pouvez choisir des détails de sécurité de clés TSIG.

Une fois que vous avez fait cela, vous créer votre serveur et vous avez une liste de serveurs. C'est difficile à lire une nouvelle fois, mais vous avez le nom, l'adresse de votre serveur, la clé TSIG et cochez que cela fonctionne, que c'est actif, et le bouton de configuration. Donc vous pouvez allumer et éteindre ces boutons. Ceux qui sont actifs, donc je ne voulais pas envoyer des configurations DNS, donc j'ai mis un petit peu plus de sécurité et de protection.

Vous devez faire manuellement un transfert AXFR avant que ce ne devienne actif. Donc cela est une étape de sécurité pour vous assurer que vous n'essayez pas d'utiliser l'adresse de quelqu'un d'autre. Donc vous avez une commande à ce sujet que vous pouvez utiliser, vous pouvez copier-coller.

Et enfin, donc, ce bouton de configuration va vous donner tous les codes dont vous avez besoin. Voilà à quoi cela ressemble. Ça,

c'est pour bind. On pourrait utiliser autre chose à l'avenir. Pas tous les résolveurs récursifs soutiennent les transferts AXFR. Avec bind, c'est un petit peu plus spécifique et un petit peu plus local. Donc vous faites copier-coller sur votre configuration et vous avez terminé. Vous avez tout ce dont vous avez besoin.

Et vous voyez cette liste en bas ? Ce sont des adresses IP qui vont vous servir de racine locale. On aura sûrement plus de copies de disponibles à l'avenir. Mais B, C, F, G et K, ce sont les serveurs racines. S'il y a un serveur racine qui n'est pas en ligne, et bien vous pouvez en utiliser un autre. Et ça, c'est une très grande sécurité parce que dans mon université par exemple, si le serveur ne fonctionne pas, vous pouvez obtenir des données d'un autre serveur. Donc en général, c'est automatisé, donc il n'y a pas de problème à ce niveau.

Alors, parlons un petit peu des effets dans le monde réel. Je suis chez moi, je veux avoir un résolveur récursif parce que je suis un geek chez moi à la maison. Et vous voyez sur la gauche, vous avez le nombre de requêtes à la seconde. Cela peut monter à 35-40 à la seconde et ensuite, plus rien, c'est plat. Et cela arrive lorsque je branche la racine locale. Ça passe de la racine B de chez moi, et ensuite, il y a beaucoup beaucoup moins. Donc c'est plat parce que je n'ai plus à parler à la racine, je ne communique plus avec la racine. La racine est chez moi. Je peux

l'éteindre et la rallumer et on va avoir beaucoup plus de requêtes qui vont arriver.

Donc les raisons pour lesquelles ce n'est pas totalement plat, vous voyez, c'est parce que les résolveurs récursifs passent dans une zone esclave. Mais parfois, ils font des requêtes quand même, ils envoient des requêtes pour s'assurer qu'il n'y ait pas de notifications de ratées. Donc cette liste continue à envoyer des requêtes et cela mesure, en fait, la racine. Donc il y a un petit peu plus de trafic pour moi parce que je suis connecté de cette manière de chez moi.

Alors des questions ? Essayez-le, dites-moi ce que vous en pensez. Je crois qu'il y avait un bug sur la page web, mais inscrivez-vous et j'aimerais savoir ce que vous en pensez. Est-ce que cela vous intéresse ? Est-ce que vous allez l'utiliser ? L'essayer ? Si vous faites une analyse, j'aimerais savoir quel est votre trafic, est-ce que cela va avoir un impact sur votre trafic. Parce que le trafic peut être augmenté parce que vous avez un impact sur la zone racine. Vous n'allez pas être connecté avec tous les TLD. Si vous voulez faire de la recherche, c'est très intéressant. Qu'est-ce que vous faites, j'aimerais le savoir ; c'est très intéressant d'échanger et quelles autres caractéristiques voudriez-vous voir dans la foire aux questions. Il y a un avenir pour cette zone racine LocalRoot. Et je viens de terminer cela la semaine dernière, donc j'avais toujours des expérimentations, et

il y a encore quelques modifications qui vont être faites au niveau des mots de passe et ainsi de suite. Et j'espère que ce sera populaire, que ce sera utile pour nous tous au niveau de nos environnements locaux. Donc voilà. Des questions sur ces services ?

CRISTIAN HESSELMAN : Bonjour, je suis Cristian. Est-ce que vous pouvez étendre ce concept au niveau des TLD et leurs noms ?

WES HARDAKER : Parce que je n'ai pas connexion aux TLD, je ne sais pas si les TLD voudraient faire cela. Il faudrait en parler avec eux. La réalité, c'est qu'il y a beaucoup de TLD qui ont des informations propriétaires, des informations restreintes disons. Ce serait intéressant d'en parler avec eux en tout cas. Je ne sais pas s'ils aimeraient que tout cela soit commun. Il faudrait voir.

ORATEUR NON-IDENTIFIÉ : Tous les gTLD seraient disponibles une fois dans la journée ?

WES HARDAKER : Il y a un système qui vous permettrait avec get Deltus de... Ce serait une bonne idée, en tout cas.

ORATEUR NON-IDENTIFIÉ : Mon impression, c'est que si vous êtes un petit peu stable...

WES HARDAKER : Oui. Une des choses que je pensais dans le futur, c'est pour diminuer la largeur de bande puisqu'on a trois signes trois fois par jour, des fois, on a un changement quelques fois par jour, mais c'est rare. Donc j'opère dans l'infrastructure pour la racine et je vois cela fréquemment. Les données elles-mêmes ne changent pas vraiment. Ce qui change, ce sont les signatures.

Donc une des choses que je peux faire dans le FAQ, c'est d'envoyer une notification de temps en temps, tous le tiers du temps de signature. Il devrait y avoir un code parce que l'on n'a pas besoin des données aussi fréquemment. Donc ce serait, pour moi, un projet dans le futur. Si quelqu'un est intéressé, dites-le moi.

ORATEUR NON-IDENTIFIÉ : Bien, tenez-nous au courant.

RAED AL-FAYEZ : Bonjour. Je voudrais savoir si ce projet est encore à l'état de concept. Est-ce que c'est déjà une meilleure pratique ? Est-ce que je peux demander à mon fournisseur internet d'utiliser ce concept ? Est-ce que c'est sûr ? Est-ce que c'est stable s?

WES HARDAKER : Très bonne question. Ce projet que j'ai créé, vous pouvez recevoir des notifications, vous pouvez vous inscrire. C'est tout à fait nouveau, et j'ai fait un projet beta. Maintenant, c'est à un niveau beta, c'est encore en développement.

Cela dit, la façon de concevoir la configuration que cela vous donne, c'est que même si mon serveur ne fonctionne pas, vous aurez quand même les données des autres racines. Et aussi, RFC 7706 est un standard public. Ce n'est pas expérimental... je crois que oui. Bien, en tout cas, la configuration que je vous donne ne va pas avoir de défaillance. Donc je vous dirais que vous pouvez l'utiliser de ce point de vue au niveau de la racine local et recevoir des notifications.

J'ai besoin de savoir si cela vous intéresse. Je ne sais pas quel niveau de développement je vais mettre en place. Dites-le moi. Si vous voulez, on peut correspondre et le voir ensemble. Merci. Mon adresse se trouve sur le site internet, en bas. Qui serait intéressé ? Vous pouvez lever la main. À moitié... Bien.

ORATEUR NON-IDENTIFIÉ : Moi, j'ai une question. Il y a de plus en plus de gens qui font cela, il y a de plus en plus de gens qui font ce résolveur récursif. Qu'est-ce que cela veut dire pour l'infrastructure de la racine ?

WES HARDAKER : Cela veut dire qu'elle va être moins utilisée. Une des questions à long terme, c'est quelle est la meilleure manière de distribuer des informations pour la zone racine. Et cela a été discuté à plusieurs reprises. Donc ça, c'est une option pour avoir une meilleure manière de recevoir l'information initiale pour les premières requêtes.

JACQUES LATOUR : Est-ce qu'il y a d'autres questions ? Cristian.

CRISTIAN HESSELMAN : C'est plutôt une remarque, mais je voudrais dire que si vous voulez étendre ce concept au niveau des TLD, vous devez aussi étendre votre résilience de DDos parce que vous allez mettre l'information à l'intérieur. Donc les choses vont continuer à fonctionner en termes de résolution.

WES HARDAKER : Oui, c'est une bonne chose. Le problème, c'est que les informations de TLD sont souvent plus importantes. La zone

racine est petite, donc on ne peut pas le faire. Et cela peut être intéressant de le faire pour d'autres domaines qui sont plus petits. Je pense que c'est une très bonne idée. Je vous en remercie, je n'avais pas pensé à cela. Je vais y réfléchir.

RUSS MUNDY : 7706 est informationnel.

WES HARDAKER : C'est un classement étrange.

MOHAMMAD : Ce que je vois dans votre présentation, c'est que c'est une transaction TSIG entre le serveur et le serveur racine. Donc d'après ce que je sais, l'administrateur zaroot utilise Config pour son serveur avec un TCK ou une clé TSIG.

WES HARDAKER : La clé TSIG est une clé partagée entre les deux serveurs. Cela veut dire, c'est comme si vous aviez un mot de passe partagé. Lorsque vous avez des dossiers compressés par exemple, c'est la même chose. Donc on essaie de s'assurer que vous n'êtes pas en train de chiffrer les données, mais on veut s'assurer que les données n'ont pas été modifiées pendant leur transit. Donc cette clé TSIG est générée. Elle se fait entre mon serveur local et

votre résolveur récursif. Cela n'a rien à voir avec la racine. Je reçois de notifications dans la racine, mais je vous envoie ces notifications. Tout est protégé de multiples façons. Mais vous ne devez pas vous occuper de l'autre racine.

MOHAMMAD : Donc votre serveur agit comme un point entre moi et votre serveur. Et dans ce cas, si votre serveur ne fonctionne pas, comment est-ce que je peux toucher l'autre serveur racine ?

WES HARDAKER : Votre serveur va continuer à les envoyer toutes les heures pour être sûr que les données sont reçues. Si vous ne recevez pas une notification, le résolveur récursif va vous annoncer que cela a été changé. Donc cela n'est pas un problème ; c'est sûr.

Merci beaucoup, merci beaucoup à tous.

JACQUES LATOUR : Bien. J'ai une dernière question ou remarque.

Donc je pensais, si on réplique cela pour dot quelque chose, est-ce qu'on peut utiliser un fournisseur internet pour résoudre .ca ? Vous pouvez choisir qui vous voulez avec ce même système ? Cela veut dire potentiellement qu'on a les nécessités pour d'autres infrastructures. Je n'ai pas besoin d'être énorme, je

peux avoir une infrastructure suffisamment bonne. Cela nous marque un peu la limite entre ce qui est grand et... Un fournisseur internet de grande taille peut-être peut faire cela.

WES HARDAKER : Je l'ai sur mon serveur. Je serais ravi d'en parler avec vous, je serais ravi de vous donner cette infrastructure. C'est quelque chose qu'on peut analyse.

JACQUES LATOUR : Merci.

Bien. Maintenant, nous avons Vittorio Bertola de Open-Xchange qui va faire une présentation sur les idées de domaines qui utilisent le DNSSEC pour la sécurité et le système numérique d'identité. Allez-y.

VITTORIO BERTOLA : Merci. C'est un grand projet de Open-Xchange, et nous avons une plateforme, et nous avons plusieurs applications. Mais c'est un projet conjoint avec DNIC, un registre de TLD.

Donc un des effets secondaires et une des raisons pour lesquelles je fais cela pour promouvoir DNSSEC, c'est que l'utilisation du DNSSEC se fait dans le cadre de ce projet. Je vais passer rapidement ici. Vous savez tous qu'il y a un problème au

niveau de l'identité des gestionnaires, au niveau du gestionnaire de mots de passe d'internet, trop de mots de passe, les gens utilisent les mêmes mots de passe s'ils le peuvent. Et à cause des différentes exigences concernant les mots de passe, cela devient de plus en plus compliqué. Donc tout le monde cherche une solution à cela. Et donc on propose ce système, un système qui s'appelle système d'inscription unique pour, donc, s'inscrire sur tous les sites internet avec le même mot de passe. Mais on a un problème avec cela.

Le premier type de système, c'est que le gouvernement utilise ce type de système. Le problème, c'est que c'est très lourd et qu'on ne veut pas donner son vrai nom, son adresse, etc. chaque fois qu'on s'inscrit sur un site. Donc par exemple, si vous voulez rentrer sur le site de votre banque, oui mais sinon, c'est trop long, et il y a une question de confidentialité. Donc ce que l'on commence à utiliser aujourd'hui, c'est ce système, un système OTT qui vous permet de vous inscrire avec votre compte Facebook, Google, Twitter ou LinkedIn.

Mais on pense que ce n'est pas vraiment la façon dont on devrait faire les choses parce que c'est entre les mains d'une seule compagnie. Et très souvent, ce sont des compagnies qui offrent ce service. Il n'y a pas vraiment de garantie concernant la confidentialité, et on n'a pas vraiment le choix. On devrait être capable de choisir le système que l'on préfère. Donc on va

essayer de trouver un moyen de créer un autre système qu'on va appeler DomainID, on cherche un meilleur nom.

Mais notre objectif est de créer un système unique public mondial ouvert qui soit la norme. On peut avoir différentes identités. Il va fonctionner comme cela, de façon à ce que tous les sites internet vont accepter l'inscription, la connexion à travers ce système, tous les fournisseurs. On pourra même installer cela soi-même. Donc un standard public, cela veut dire que l'utilisateur va pouvoir choisir quelles données il veut partager sur ce site internet. Il va y avoir différentes couches, différents contrôles pour savoir quelles sont les données qui sont partagées sur le site internet. Voilà, ça, c'est du point de vue technique.

Ensuite, se connecter sur ce open ID, nous allons construire cela sur le DNS. On a besoin d'un processus de découverte de façon à utiliser toute adresse courriel comme identificateur ou identifiant, de façon à pouvoir mettre son identité, son nom de domaine ou ce que l'on veut utiliser. Mais on a aussi besoin de certains mécanismes pour cartographier son identité. Donc l'idée ici serait que l'on va créer, on va utiliser un système basé sur le DNS pour avoir cette identité. Donc on a ce processus de découverte.

Et pour les propriétaires de sites internet, on va avoir un système de ce type. On va aussi avoir un système pour identifier le porteur. Si vous n'avez plus confiance, vous pouvez chercher un autre identificateur ou un autre système d'identification. Et vous pouvez changer de fournisseur et vous aurez un compte sur une compagnie.

Nous essayons aussi d'imiter l'architecture du système de noms de domaine avec des points qui sont séparés en plusieurs parties, de façon à avoir une autorité de l'identité qui serait l'équivalent du registre de TLD qui va gérer l'authentification, l'autorisation qui va contrôler votre mot de passe, etc. Et ensuite, on aura un agent d'identité qui est l'équivalent du bureau d'enregistrement qui va avoir la relation avec l'utilisateur. L'utilisateur va aller voir un de ses agents pour obtenir un service. Il va créer, donc, une autorité concernant son autorité.

On veut aussi donner à l'utilisateur la possibilité d'avoir un système de refus concernant les données qu'il accepte ou qu'il n'accepte pas d'échanger et de diffuser, de façon à ne pas être obligé chaque fois de diffuser toutes les données sur chaque site internet. Et puis, cela peut être partagé de manière individuelle sur les différents sites qui sont sous votre contrôle.

Alors, comment cela fonctionne au niveau technique ? On utilise donc un système hostname DNS. Ce peut être le même nom d'hôte de DNS, ce peut être aussi une autre chaîne ou le nom de domaine que vous contrôlez à la base. Ce que l'on va faire c'est avoir cet agent d'identité, lui demander le service. Il va vous donner un nom de domaine personnel. Vous pouvez avoir cela dans votre nom de domaine Telco ou autre. Vous pouvez obtenir cela auprès d'une compagnie, mais le mieux, c'est que l'utilisateur ait son propre nom de domaine. Donc on peut l'acheter, ce nom de domaine si on ne l'a pas. Et la seule chose qui reste à faire, c'est de créer un enregistrement DNS. Donc on va utiliser un registre TLD, et c'est une information de base qui va montrer quelle est votre autorité d'identité et agent d'identité de façon à ce que l'identificateur sache quel est le serveur qui doit être contacté si l'on veut authentifier cet utilisateur. Ça, c'est la partie de la création.

Ensuite, on va aller devant les autorités. Les autorités vont vérifier que ce soit fait correctement. On va confirmer l'identificateur et à la fin, on ira directement à l'autorité parce qu'un des points, des objectifs de ce système, c'est que les seules organisations qui peuvent voir votre mot de passe, c'est l'autorité. Donc il y aura un seul endroit où vous devrez sécuriser votre mot de passe. Et vous pouvez vous souvenir de cela parce que c'est le seul mot de passe que vous devez mémoriser. Le site

internet ne verra jamais votre mot de passe, il ne pourra pas voler votre mot de passe, ou on ne peut pas se faire passer pour quelqu'un d'autre et obtenir un mot de passe ou ce type de problème. Voilà.

Donc c'est ce qui se passe lorsqu'il faut se connecter. On va aller sur le site internet, on va passer par l'identificateur. Le site va faire cette requête du DNS pour voir quel est votre agent d'autorité. Ça, c'est la partie qui est sécurisée par le DNSSEC et nous imposons le DNSSEC par politique parce qu'il faut que ce soit sécurisé, sinon, cela ne fonctionne pas.

Et le reste du processus est un processus standard qui est mis en œuvre. On a une mise en œuvre gratuite, même, pour certaines parties. Donc je ne sais pas si les gens ici connaissent ce système, mais il s'agit d'une procédure qui permet à l'utilisateur de se présenter devant une autorité qui va lui demander son mot de passe. Et si vous avez une séance ouverte, vous n'avez même plus besoin de présenter votre mot de passe. Si l'autorité le veut, elle peut mettre en œuvre un facteur d'authentification qui est disponible pour tout type de connexion.

Et à la fin, lorsque vous êtes connecté, l'utilisateur va pouvoir partager des informations, surtout si c'est la première fois qu'il se connecte, avec le site internet. Le site internet va recevoir un token d'accès, et l'autorité va montrer la liste des utilisateurs.

L'utilisateur va avoir un contrôle complet des informations qui sont partagées avec ce site internet.

Donc il y a différents aspects. Les choses qui sont positives pour les utilisateurs, c'est que vous pouvez choisir votre identité. Vous n'êtes pas obligé de choisir le nom de domaine de la compagnie qui vous fournit une identité, que ce soit Google, Facebook ou autre. Vous pouvez aussi choisir votre fournisseur. C'est très important parce que c'est une façon de créer une relation plus sûre avec un utilisateur et un fournisseur d'identité. Si vous pouvez avoir différents fournisseurs, il va y avoir une concurrence pour offrir un bon service de confiance, et cela va être positif. On peut aussi choisir un fournisseur qui ne va pas vendre vos données. C'est important. DNIC, par exemple, travaille dans ce secteur et ne va pas vendre vos informations parce que c'est une organisation à but non lucratif. Donc c'est une manière d'augmenter la confiance pour les utilisateurs lorsqu'on utilise l'internet aussi. Et puis c'est plus sûr parce que c'est vrai que maintenant, vous n'avez qu'un seul endroit qui va être très très sécurisé. Toutes vos connexions vont passer par là, mais vous n'avez plus besoin d'avoir mis le mot de passe enregistré quelque part ou mémorisé.

Et si votre gestionnaire a un problème, vous pouvez en changer, et vous changez de mot de passe. À ce moment-là, vous pouvez de nouveau être actif en ligne.

C'est fait pour être plus confidentiel. Vous n'êtes plus obligé d'avoir plusieurs identités même si les gens ont différents courriels pour se connecter sur différents services. Là, ce n'est plus nécessaire. Et vous n'aurez plus besoin de vous connecter sur les sites puisqu'une fois que vous vous êtes connecté une fois, vos informations sont sur ce site. Vous pouvez choisir les informations que vous voulez partager, vous contrôlez vos informations de cette façon.

Et plus important encore, quelle est la valeur stratégique pour le nom de domaine et le monde du nom de domaine. C'est une manière de vendre davantage de noms de domaine. C'est une manière de promouvoir les noms de domaine, ce qui est toujours positif. Mais c'est aussi destiné à promouvoir le DNS, à maintenir le DNS en bon fonctionnement parce que c'est vraiment notre objectif.

Je sais qu'il y a beaucoup de gens dans cette salle qui pensent comme moi. Nous avons peur, un petit peu, de la direction, de ce qui se passe actuellement en ligne au niveau de la confidentialité, etc. Et d'un point de vue, la possibilité de contrôler et de surveiller l'identité des utilisateurs, c'est important. Si on a un bon système d'authentification, on peut lutter contre les différents usages malveillants et problèmes de sécurité. Mais nous ne voulons pas non plus construire un internet dans lequel tout le monde est contrôlé et surveillé.

Donc le suivi, c'est un point important pour le développement d'internet, et nous pensons qu'un gestionnaire d'identité, par exemple le courriel, permet aux utilisateurs d'être un moyen de s'identifier. Tout cela est important et stratégique pour le DNS.

Aujourd'hui, le DNS est un système qui permet d'avoir des identificateurs techniques, mais les informations des gens ne devraient pas être dans le DNS. Le système DNS est sûr si on utilise DNSSEC, et donc il faudrait vraiment que ce soit stratégiquement l'endroit où les informations concernant les gens sont stockées. Voilà.

Donc il n'y a pas vraiment d'autres façons de faire ce qu'on imagine. C'est pour cela que nous travaillons de cette manière. Nous voulons avoir un système public ouvert pour tous ceux qui veulent fournir des identités et qui veulent se connecter avec une seule identité partout. Voilà ce que nous construisons. Pour le moment, nous avons ce concept qui fonctionne.

Nous avons déjà une première partie qui a été soumise il y a quelques semaines, donc qui est déjà en ligne. Et nous voulons voir s'il y a des gens qui sont intéressés. Nous pouvons standardiser ce système ou travailler au niveau... En tout cas, nous en sommes dans la phase de présentation du projet à différents endroits et nous attendons un petit peu les

commentaires. Nous voulons aussi voir s'il y a des gens qui sont intéressés pour développer ce système avec nous.

Nous avons aussi reçu des commentaires de Telco parce que Telco a eu un problème avec le fait que les gens ne s'écrivent plus avec leur identité mais avec l'identité de Google. Et donc ils s'inquiètent un petit peu sur ce qui se passe.

Donc voilà, c'est à peu près tout ce que je voulais vous dire aujourd'hui. Je suis prêt à répondre vos questions maintenant. Merci beaucoup de votre attention. S'il y a des questions que vous voulez poser, n'hésitez pas.

ORATEUR NON-IDENTIFIÉ : Merci Vittorio. Je suis aussi du CZ.NIC et j'aime beaucoup l'idée ; le concept me semble tout à fait intéressant. À CA.NIC, nous sommes un fournisseur de service d'identité et on a 500 000 utilisateurs qui sont inscrits. Donc on peut avoir une identité ouverte et ça fonctionne avec l'IDN. Et il me semble qu'on a déjà parlé de cela avec Marcos du DNIC, et de la manière dont c'est conçu, je pense que ce sera très facile d'avoir nos utilisateurs qui utilisent le DNS pour leurs IDN. Donc cela me paraît tout à fait pertinent.

VITTORIO BERTOLA : Oui, ce serait excellent, oui, absolument. On essaie de promouvoir ces standards et l'idée, véritablement, c'est que toutes les personnes qui ont déjà une connexion avec une identification ouverte doivent travailler avec les archives du DNS et ce serait fantastique, cela. Donc, il faut convaincre les sites web et les prestataires. Mais je crois qu'en se basant sur les utilisateurs dans notre secteur industriel, ce pourrait être tout à fait intéressant d'inviter des personnes à soutenir ce concept.

JACQUES LATOUR : Russ, une question ?

RUSS MUNDY : Merci beaucoup, Vittorio, de votre présentation. C'était extrêmement intéressant, très bonne approche me semble-t-il. Et cela utilise beaucoup le DNSSEC.

Une question à laquelle j'ai réfléchi en vous écoutant. Clairement, certains changements seront nécessaires sur les sites. Est-ce que vous pensez à ce moment que ce serait facile ? Je crois que vous vous concentrez principalement sur les sites web. Mais par exemple, en ce qui concerne les réseaux sociaux, est-ce que cela vous demanderait beaucoup de travail pour participer à cette nouvelle manière de travailler sur l'authentification ?

VITTORIO BERTOLA : Oui, il faut bien connaître la mise en œuvre de la plateforme. Je crois que ce ne serait pas trop difficile d'utiliser ce type de connexion. C'est une question de volonté. Il y a des entreprises qui veulent contrôler l'identité de leurs utilisateurs. Donc on a choisi de choisir une voie qui créerait une facilité de se joindre à cela. Si vous voulez accepter ces identificateurs, c'est un autre point. Mais c'est une ligne de connexion avec une identification ouverte. Ce n'est pas très difficile en fait, pas très complexe pour d'autres utilisations.

Moi, je crois que c'est quelque chose qu'il faut promouvoir. Ce n'est pas vraiment une technique, c'est pus un problème d'adoption, un problème de choix.

JACQUES LATOUR : Merci beaucoup, très bien. Est-ce qu'il y a d'autres questions ? Ah oui, dans la salle nous avons une question.

ORATEUR NON-IDENTIFIÉ : Oui, je suis d'un bureau d'enregistrement et hier, nous avons parlé avec Jacques d'une identité par foyer et que le routeur crée le domaine automatiquement. Si je regarde, j'ai des jumeaux de 17 ans, ils veulent absolument une facilité pour se connecter, d'avoir leur propre domaine, d'avoir en quelques

secondes la possibilité de se connecter. Donc est-ce qu'on a une idée pour que faire ce premier essai, une première tentative pour travailler de la manière la plus pratique possible pour se connecter ? Vous avez des idées là-dessus ? Est-ce que mes enfants peuvent utiliser cela ?

JACQUES LATOUR : Oui. J'ai ajouté cela en tant que spécificité de fonctionnalité et cela marche. Oui, c'est satisfaisant.

VITTORIO BERTOLA : Oui, je vois qu'on peut inscrire un nom de domaine. Mais qui va payer pour le nom de domaine ? Telle est la question. Je crois que ça peut tout à fait se faire avec la création d'un nom de domaine. Je ne vois pas de problème.

JACQUES LATOUR : Alors qui fait la vérification d'identité ?

VITTORIO BERTOLA : Vous voulez dire qui vérifie le mot de passe ? Qui vérifie que je suis bien moi, que je ne mens pas sur mon identité, ça, ce n'est pas dans le cadre du protocole. C'est un processus d'identification où toutes les données sont identifiées. Et je déclare, évidemment, que c'est mon nom. C'est comme cela que

cela fonctionne aujourd'hui pour toutes les inscriptions que vous faites en ligne. Vous pourriez avoir un protocole un petit peu différent avec des parties tierces.

JACQUES LATOUR : Cela pourrait être vérifié différemment ?

VITTORIO BERTOLA : Une autre approche, oui, mais pour la plupart des sites web, je ne crois pas qu'on ait besoin de cela, de prouver que vous êtes vous-même, que c'est bien vous. Parfois, vous ne voulez pas, en effet, prouver cela parce que vous avez besoin de flexibilité. Il faut faire attention à ne pas se faire voler son identité.

JACQUES LATOUR : Merci. Excellent présentation, merci beaucoup. On vous applaudit, on vous remercie.

Et nous allons maintenant passer la parole à Ondrej Filip de CZ.NIC. Et nous allons donc parler de gestion des ensembles de clés automatisées.

ONDREJ FILIP Bon après-midi à toutes et à tous. Je m'appelle Ondrej Filip et je suis de République tchèque. Et je voulais vous montrer

comment nous essayons de faire en sorte que le DNS connaisse une croissance dans mon pays.

La situation n'est pas mauvaise, nous avons la moitié des domaines qui sont signés avec le DNS. Mais la vérité, c'est que ce sont des domaines qui sont sur les mêmes serveurs DNS des bureaux d'enregistrement. Donc il n'y a pas assez de communication entre les DNS et les bureaux d'enregistrement. Donc les prestataires, les fournisseurs de services DNS n'ont pas de relation avec le registre.

Donc les archives du DNS ne sont pas publiées dans le registre. Il y a plusieurs raisons pour cela. Ils ne peuvent pas soumettre, peut-être, la clé. On en a parlé avec différents fournisseurs de service DNS, ils nous ont dit qu'ils ne peuvent pas soumettre les documents parce qu'ils ne savent pas le faire. C'est le problème avec beaucoup de bureaux d'enregistrement. Donc on n'a pas un très bon soutien des bureaux d'enregistrement. Parfois, les titulaires de domaine ne comprennent pas le DNSSEC.

Donc une autre motivation pour que le DNS redeviennent grand, c'est un slogan de la campagne de Ronald Reagan. Vous savez, lorsqu'on utilise ces serveurs, cela fonctionne pour tout le monde, il n'y a pas de problème. Maintenant, avec le DNSSEC, vous devez faire le roulement de clés. Cela devient de plus en

plus complexe me semble-t-il. Donc on voulait essayer de s'assurer que le DNS soit plus simple.

Et le dernier et non le moindre, on ne pense pas seulement à la République tchèque, mais nous avons 11 autres pays qui utilisent FRED. Donc c'est pour cela que nous avons un registre open source, de source ouverte. Et c'est déployé dans ces pays. Donc nous avons une responsabilité par rapport à ces pays que vous voyez sur l'écran. Et nous essayons de travailler avec encore plus de pays.

Donc au niveau de nos standards, comment le faire, il y a des standards que vous connaissez, RFC 7344 qui parle de l'automatisation et de la maintenance des clés de confiance DNSSEC. Et très récemment, cette année en mars, nous avons le RFC 8078 qui parle de la gestion des fichiers DS avec la clé CDS CDN parente. Donc vous pouvez vous référer à ce document RFC 8078. Donc ce sont des RFC importants.

Nous avons également un nouveau document préliminaire. Je crois que vous êtes au courant. C'est un opérateur pour la partie tierce du DNS qui travaille à un protocole pour les bureaux d'enregistrement et les registres.

Donc je vais parler un petit peu des deux côtés du problème au niveau de la mise en œuvre. Nous avons les registres et nous

avons le travail sur les logiciels de DNS et les logiciels de signature.

Donc vous savez que le roulement de la clé dont on a parlé précédemment, le nouveau système de publier ces clés du DNS, ce n'est pas soutenu totalement. Je pense que le DNSSEC ouvert est planifié pour le début de l'année prochaine. Le POWERDNS a une publication semi-manuelle. Il faut utiliser des scripts de cron, ce n'est pas automatisé mais presque. Et nous avons Bind, nous avons Knot DNS 2.6 qui un soutien total, qui est totalement supporté. Donc c'est une version qui est totalement recommandée. Et d'un autre côté, nous avons également un logiciel pour les registres. J'ai parlé de FRED version 2.32 qui assure, également, un soutien total.

Donc, comment faire le roulement de la clé cryptographique KSK ? [inintelligible] et il y a un système de double signatures. Il y a une soumission optionnelle par l'intermédiaire de CDS et CDNSKEY. Et cela peut être avec des serveurs « autoritatifs » ou bien avec des résolveurs validant le DNSSEC. Il y a les deux possibilités, il y a des vérifications périodiques pour l'existence de DS par l'intermédiaire de noms de serveurs configurés.

Donc voilà un exemple de configuration que vous voyez à l'écran. Nous avons donc la durée de vie de la clé qui est définie.

Vous avez tous les fichiers CDS, et vous pouvez configurer les adresses IP protocole internet. Et tout est automatisé, donc.

Les caractéristiques qui sont supportées également, le CSK, c'est un type de signature unique. Ça n'a pas besoin d'avoir CDS et CDNSKEY. Donc vous avez une clé partagée et vous avez un roulement de l'algorithme également. Et ce qu'il faut mentionner très clairement, c'est que si vous voulez effacer les fichiers DS, vous devez utiliser CDNSKEY et cela doit se faire manuellement.

Alors la mise en œuvre du registre. Avant de commencer, nous avons parlé avec les bureaux d'enregistrement et nous leur avons montré trois options : ne pas mettre cela en œuvre, ne pas l'implémenter ; ou bien que les bureaux d'enregistrement se chargent de cela et publient les fichiers DNSSEC ; ou bien le registre se charge de cela et le registre va commencer à gérer KeySet lorsqu'un domaine publie CDNSKEY.

Donc c'est un nouveau concept avec cet ensemble de KEY. On est tombé d'accord, et ça semble, pour le moment, bien fonctionner. Nous en sommes assez satisfaits.

Voici l'architecture de tout sur le registre. Donc nous avons un scanner de clé CDN que vous voyez en haut, et c'est en C++. Et cela lit une liste de domaines, cela vérifie comment distribuer les

requêtes par serveur. Et cela permet de travailler avec ces DNS key.

Donc nous avons fred-amk qui est un outil [inintelligible] de cron qui a mis en œuvre une logique de gestion de process. Et là, on utilise un base de données SQLite. C'est fred-akmd en bas. Donc on utilise [inintelligible] et c'est un interface CORBA. Et en fait, nous publions tout en source ouverte, open source. Donc cela prouve bien que ce peut être utilisé de manière universelle.

Donc nous scannons tous les domaines dans le fichier de zone. Cela prend environ trois heures pour .cz. Et il y a trois catégories de domaine sans l'ensemble de clés KeySet, pas de fichiers DNS : ceux qui ont automatiquement générés des ensembles de clés ; ceux qui sont déjà dans le système des ensembles de clés, qui existaient déjà ; ceux qui avaient été créés par le bureau d'enregistrement.

Donc en ce qui concerne les domaines sans KeySet, ça, c'est plus compliqué, c'est plus difficile. Nous devons avoir un environnement sécurisé. Et nous scannons tous les serveurs de noms « autoritatifs » à partir de la base de données des registres par l'intermédiaire de requêtes TCP. Lorsque le CDNSKEY est trouvé, le contact technique est informé par l'intermédiaire d'un courriel. Et nous continuons à scanner pour sept journées supplémentaires. On a décrit cela dans le RFC. Et nous pensons

également que si cela dure plus de sept jours, il y a probablement quelque chose qui ne fonctionne pas. Nous pensons que c'est assez sûr pour le DNSSEC.

Si les résultats sont toujours les mêmes et s'il ne s'agit pas d'un DS qui a été retiré, et bien il y a un nouvel ensemble de clés KeySet qui est créé et mis en lien avec un domaine. Les titulaires de domaine, donc, en sont informés.

Là, avec les domaines d'ensembles de clés automatique, vous scannez. Ici, on retrouve une nouvelle clé CDNS. Elle est mise à jour automatiquement ou bien elle est retirée. À ce moment-là, il y a une notification du titulaire du nom de domaine ou du bureau d'enregistrement. Et une nouvelle fois, le contact technique est informé par courriel.

En ce qui concerne les domaines avec un ancien ensemble de clés, là, c'est scanné, évidemment. Et si on trouve une clé, on crée un nouvel ensemble de clés automatiques et on le remplace dans le domaine ou bien on retire l'ensemble de clés. Et une nouvelle fois, le contact technique est informé par courriel et le titulaire de nom de domaine est notifié par courriel ou bien le bureau d'enregistrement est notifié par EPP parce qu'évidemment, il y a maintenant une automatisation du processus.

Alors quelques statistiques maintenant. Nous avons commencé au mois de juin... Nous avons maintenant plus de 627 domaines qui sont gérés. Nous sommes au début de notre travail, nous savons que nous avons un grand potentiel à CZ.NIC, ce registre de domaines pour la République tchèque. Lorsque nous avons commencé à télécharger, remplacer et à automatiser le processus en octobre, à la suite de Verisign... Nous sommes au début, je vous lai dit, de ce processus mais il va connaître une forte croissance.

Et on a lancé le système. Il y a quelques roulements qui sont maintenant réalisés depuis le mois de juillet. Donc le système vous trouve automatiquement et place le DNSSEC. Et donc vous avez des extensions de sécurité renforcée avec ce registre. C'est relativement simple, c'est relativement automatique. Je crois que c'est un système qui peut être utilisé pour des noms de domaine qui existent déjà. Ça limite les complexités que nous connaissions auparavant, donc pour les bureaux d'enregistrement, pour les nouveaux domaines également et les anciens.

Donc nous avons d'autres débats et discussions à ce sujet. On n'est pas obligé d'utiliser ce système. Il y a des personnes qui ne veulent pas l'utiliser, qui optent pour ne pas l'utiliser. Ce devrait être une liberté que de l'utiliser ou pas pour nos utilisateurs. Si

quelqu'un publie des fichiers CDNSKEY, et bien c'est une possibilité, cette débattue.

Et pour qu'on ait plus de confiance dans le processus, on a besoin de plus d'emplacements pour scanner les données. Ça, c'est important, plus de sites pour accroître la sécurité du processus. Il faut qu'il y ait une meilleure notification des contacts, il faut qu'on mette à jour ces notifications, c'est vraiment important. Nous devons également avoir un modèle PUSH à la fois pour notre DNS et pour FRED comme le disait Jacques tout à l'heure. On a déjà le modèle PULL, on voudrait avoir le modèle PUSH. Donc ce serait important pour nos clés, je pense, à l'avenir, que ce soit poussé vers les registres avec un canal sécurisé, et que cela se passe immédiatement, que les logiciels DNS n'aient pas besoin d'attendre un jour pour faire le scan. Évidemment, on doit faire du marketing, on doit parler à plus de prestataires de services du DNS pour faire connaître, donc, ce système qui est tout à fait facile à l'emploi, qui peut accroître et limiter la complexité des opérations informatiques.

Je vous remercie de votre attention. Voilà ce que je voulais vous dire et je serai prêt à répondre à vos questions.

JACQUES LATOUR : Merci beaucoup Ondrej. Moi, je suis un fan de tout cela. Cela m'intéresse beaucoup. Y a-t-il des questions pour Ondrej Filip ? Oui, allez-y.

ORATEUR NON-IDENTIFIÉ : Merci monsieur. Je suis monsieur [inintelligible] et je crois que nous sommes intéressés par cela, par FRED, tout particulièrement pour le DNS. Mais parfois vous savez, je ne trouve pas les sources. Il y a des sites alpha ou beta pour FRED. Donc est-ce que vous pourriez m'indiquer comment je peux utiliser... me donner des conseils pour utiliser cela ?

ONDREJ FILIP : L'architecte de FRED est assis dans la salle et il est responsable pour un site, fred.com et tout doit être disponible. Donc je crois qu'il faut essayer de le convaincre. Si vous avez des besoins au niveau de FRED, posez-lui des questions pour qu'il y ait des versions plus avancées, pour qu'il y ait plus de fonctionnalités. Je crois qu'il est prêt à répondre à vos questions et également vous aider au niveau technique.

JACQUES LATOUR : Y a-t-il d'autres questions ?

Alors oui, moi, j'avais une question moi-même. Quand est-ce que cela va être mis en place par défaut une fois qu'on installe notre DNS, qu'on publie CDS ? Quel sera le cycle ?

ONDREJ FILIP : Mais c'est déjà par défaut, vous savez. Si vous enregistrez un domaine actuellement et si vous utilisez le DNS, après sept jours, le DNS est connecté.

JACQUES LATOUR : Alors si tous les prestataires des services soutenaient cela, ça pourrait s'accroître très rapidement ?

ONDREJ FILIP : Oui. Nous espérons vraiment que cela se développe beaucoup l'avenir avec beaucoup de support également, ce qui permettra de mettre en œuvre le DNSSEC. Et ça, ça n'apport pas de complexité opérationnelle supplémentaire. C'est pour cela que nous pensons que ce système est très positif et que beaucoup de systèmes et de prestataires peuvent l'utiliser.

ORATEUR NON-IDENTIFIÉ : Oui, un petit commentaire. Vous avez vu, il y a 600 ou 700 domaines ; 90 % de ces domaines sont des [inintelligible] qui soutient cette nouvelle manière de gérer le DNSSEC. Et nous

sommes actuellement en négociation pour avoir beaucoup plus de noms de domaine qui soient gérés de cette manière. Donc tout le monde n'a pas encore cliqué sur le bouton « Je veux le DNS ». On négocie avec [inintelligible] pour deux choses. Comment faire du marketing auprès des utilisateurs et des clients pour tout simplement qu'ils cliquent sur le bouton DNSSEC et voir s'ils peuvent passer de opt-in à opt-out, donc opter pour ou contre la mise en place de ceci. Donc on est en négociations. On espère que ces négociations finiront par être positives.

JACQUES LATOUR : Merci beaucoup. Et bien pour le prochain atelier DNSSEC, je propose qu'on en reparle. Y a-t-il d'autres questions ? Merci beaucoup Ondrej. Nous vous applaudissons.

Russ va nous parler du DNSSEC et de ce que l'on peut faire dans ce domaine.

RUSS MUNDY : C'est notre dernière séance de la journée. Je vais d'abord remercier tous ceux qui ont fait une présentation aujourd'hui, tous ceux qui ont participé en posant des questions aussi. C'est une des raisons pour lesquelles cette communauté nous a beaucoup aidé, et c'est aussi pour cela que le DNSSEC a aussi

bien marché. Donc nous les remercions, nous vous remercions tous.

Donc cela va probablement ne pas nous occuper jusqu'à la fin, mais je voudrais faire une petite présentation des différentes choses qui pourraient vous intéresser, ce que vous pouvez faire en cas de ce type de situation parce qu'il y a beaucoup de coopération dans la communauté. Nous avons un nouveau projet qui a été décrit par Wes. Il y a une série d'autres choses qui sont faites dans le domaine de la recherche qui sont très utiles. Il y a des statistiques qui nous ont été présentées à plusieurs reprises. Et dans ce cas-là pour les opérateurs de TLD – je sais qu'il y a beaucoup d'opérateurs de TLD dans la réunions d'ICANN – nous avons commencé notre séance en présentant le nombre de TLD qui avaient signé déjà, mais en montrant aussi qu'il y avait encore beaucoup de TLD qui n'avaient pas encore signé leur zone. Donc ceux qui ne l'ont pas fait, faites-le. Si vous avez besoin d'aide ou d'une collaboration de notre part, c'est ici que vous trouverez de l'aide parce qu'il y a beaucoup de gens qui seraient ravis de vous aider.

Ensuite, soyez sûrs de faire un plan général et ensuite, d'avoir des enregistrements DN et DNSKEY parce que c'est comme cela que l'on peut avancer dans la hiérarchie du DNSSEC.

Ensuite, le travail avec les bureaux d'enregistrement, certains bureaux d'enregistrement ont fait du très bon travail, mais pour beaucoup de TLD, c'est encore un grand défi. Les bureaux d'enregistrement ne sont pas préparés, pour différentes raisons, à faire certaines choses avec le DNSSEC. C'est pour cela que nous avons certains problèmes. Et je dirais que c'est très utile ce que vous avez fait ici. Et il faut, donc, dans beaucoup de pays, essayer de faire participer les bureaux d'enregistrement.

Ensuite, au niveau des statistiques. Il y a beaucoup de gens qui veulent savoir ce qui se passe. On veut voir les progrès qui sont fait. Et les statistiques sont très utiles aussi pour savoir quels sont les déploiements qui ont eu lieu.

Ensuite, les opérateurs de zone. Je pense que dans cette salle, on peut avoir un pourcentage élevé de personnes qui opèrent des résolveurs récursifs plus que partout dans le monde. Mais il y a d'autres endroits. Essayez de convaincre les personnes qui travaillent avec vous de signer. Faites vos vérifications DNSSEC, faites signer ces zones, dites à vos bureaux d'enregistrement que vous voulez qu'ils appliquent, qu'ils déploient le DNSSEC, et qu'ils vous fournissent des statistiques.

Au niveau des entreprises, il y a beaucoup de choses qui peuvent être faites pour déployer le DNSSEC. Au niveau des entreprises, il n'y a pas grand chose de très efficace. Mais en tout cas, ce qu'on

peut dire, c'est qu'au niveau des entreprises, il n'y a pas encore assez de DNSSEC de déployés. Il y a certaines choses qui pourraient être faites sur les lieux de travail, par exemple, analysez cette question, parlez-en aux responsables de la sécurité de vos départements qui s'inquiètent de l'évaluation du risque. Dites leur que le DNSSEC améliore cette évaluation de risques.

Lorsqu'on parle aux fournisseurs d'internet, c'est là que les fournisseurs d'internet ont un rôle très important à jouer parce que la plupart des gens n'utilisent pas ces résolveurs chez eux. Ils comptent sur leur fournisseur internet. Si on n'utilise pas un ISP genre Google, on n'a pas ce type de sécurité. Donc il vaut mieux demander à son fournisseur local d'utiliser ces systèmes. Et tous les ISP doivent eux-mêmes signer. Donc faites-les participer, essayez de les convaincre.

Tout le monde peut faire quelque chose pour le DNSSEC, et la coopération de tous ceux qui viennent à nos ateliers est importante. Essayez de participer, donc, à cette opération, de faire cela sur votre propre appareil, faites-le dans votre propre environnement, faites des expériences. Je pense que très souvent, les leçons finissent par être utilisées et incorporées de manière globale. Et cela commence par des idées toutes simples que des individus ont eues, et cela finit par être présenté devant l'IETF.

On aimerait aussi recevoir vos apprentissages. Depuis 10 ans, je fais cet atelier du DNSSEC et je dirais que nous avons encore beaucoup de gens qui viennent participer à ces ateliers. Nous constatons qu'il y a beaucoup d'intérêt pour ce DNSSEC. Donc nous continuerons à organiser cet atelier pour les autres réunions d'ICANN. Nous annoncerons cela à la fin du mois de décembre ou au début de l'année prochaine. En tout cas, nous aimerions connaître votre opinion et savoir si cela vous a été utile. Voilà, ateliers, d'autres réunions. Il y a beaucoup de choses qui ont lieu. Dans vos régions aussi, regardez s'il y a des choses qui sont organisées. Je sais qu'il y a eu des cours qui ont été donnés, aussi. C'est une très bonne manière d'apprendre, aussi, et de participer au travers ces types de formations.

Donc je remercie tous ceux qui ont participé, qui ont assisté à cet atelier. On remercie de nouveau nos sponsors qui ont sponsorisé cette réunion et le déjeûner des participants. Et nous avons reçu le soutien aussi de SSAC qui est un des comités consultatifs d'ICANN, est l'Internet Society et le programme Deploy360. Alors ici, nous vous donnons quelques URL, quelques liens pour ceux qui voudraient davantage d'informations.

Et je voudrais aussi remercier Julie, Andrew, Cathy qui ont permis à cet atelier d'être organisé. Je les remercie.

De nouveau, je vais vous donner la parole. Si vous avez des questions, des commentaires, des réflexions, allez-y. Wes ?

WES HARDAKER : Je vous avais dit que ma démo ne marchait pas. Ça y est, j'ai réussi à la faire marcher.

RUSS MUNDY : Wes, vous avez dit que pour C7706, les informations n'étaient pas mises à jour.

WES HARDAKER : C'est une très bonne question. La réalité, c'est que cela pourrait être expérimental, ce serait possible, mais ce n'est pas vraiment un changement de protocole. C'est seulement comment on veut déployer quelque chose. Et dans le cas d'un résolveur, c'est quelque chose qu'on aurait pu faire avant. C'est pour documenter le fait que c'est une solution. En tout cas, le 7706 est prêt.

RUSS MUNDY : Bien. Est-ce qu'il y a d'autres réflexions, d'autres commentaires ? Nous vous remercions et nous espérons que nous vous retrouverons la prochaine fois.

[FIN DE LA TRANSCRIPTION]