PRAGUE – ASO/NRO Presentation on RPKI
Wednesday, June 27, 2012 – 12:00 to 12:30
ICANN - Prague, Czech Republic

La Présidente Dryden: D'accord. Soyez le bienvenu. Soyez le bienvenu à l'ASO NRO. Il y a eu plusieurs membres du GAC qui ont été intéressés à nous éclairer sur cette question, et c'est quelque chose sur quoi la communauté a travaillé, c'est pour cela que je passe la parole à Monsieur Curran qui va se présenter de lui même, et qu'il présenterait.

John Curran: Je m'appelle John Curran, je suis le président de RPKI, qui est l'organisation de soutien de l'ICANN pour ce qui est des adresses. À mes côtés, il y a dans cette table le président de l'organisation de conseil support pour le nom, qui s'appelle Louie Lee. C'est un conseiller consultant.

Nous avons les PDG des RIRs qui constituent plusieurs de ces organisations, moi même, y compris, pour ARIN, ainsi que Raul Echeberria de LACNIC, Paul Wilson de APNIC, et Adiel Akplogan de AfriNIC. Nous allons aussi présenter des questions sur le RPKI.

Il y aura Geoff Huston qui va parler à partir dès maintenant. Merci Geoff.

Geoff Huston:

Bonjour à tous. Cette présentation est une présentation très technique, parce qu'elle s'occupe des technologies que nous n'utilisons pas normalement ou que nous nous ne sommes pas habitués à avoir en général. Il s'agit des technologies liées à la sécurité de notre infrastructure et de nos communications.

Il est intéressant de savoir qu'il y a beaucoup de raisons d'être méchant sur Internet, qu'il y a beaucoup de façons de faire des choses perverses sur Internet. Bien sûr, on peut envoyer beaucoup de courriels, et on peut essayer de corrompre l'exploitation sur le système de DNS. Et le DNS est constamment soumis à des attaques.

On peut aussi essayer d'envoyer des paquets très particuliers vers certains ordinateurs pour qu'ils fassent certaines choses qu'ils n'auraient jamais l'intention de faire. Il en va de même pour les virus, parce que les virus modifient l'exploitation du système qu'ils affectent. Milliards d'autres attaques qui sont même plus gênantes. Ces attaques n'essaient pas de modifier le fonctionnement de votre machine dans la mesure où la machine--l'ordinateur fonctionne bien l'attaque est plus {sévère}.

Il y a deux types d'attaques qui ne surviennent pas dans les ordinateurs individuels mais aussi dans la structure d'Internet en elle-même.

La première se produit sur le nom de domaine {DNS}, et c'est quelque chose sur quoi on est vraiment familiarisé depuis très, très longtemps. Et les efforts pour présenter des solutions par

rapport à la sécurité de DNS et de sa mise en œuvre, comme nous le voyons ici dans cette réunion d'ICANN, sont déjà en marche. Il y a beaucoup d'ateliers, une forte activité et une forte compréhension de la question.

Le routage est différent. Le routage est un problème très difficile vraiment. Pour pouvoir comprendre comment rediriger ces paquets vers leur destination, il faut utiliser des algorithmes très sophistiqués qui ont été établis. Le routage est un problème très difficile, même en termes de technologies sous-jacentes.

Lorsque nous avons construit pour la première fois le système de routage et je vais 40 ans en arrière, je vais dans les années 60s. Cela a été fait dans un milieu de recherche, et le milieu de la recherche tend à penser à certaines choses vraiment élémentaires, et l'une de ces questions concernait certains joueurs, disons. Tout le monde a fait la même supposition. Les algorithmes sont basés sur la confiance mutuelle.

C'est quelque chose très important pour Internet. La confiance mutuelle n'est pas le fait courant dans notre entourage, dans notre milieu. Comment faire si nous n'acceptons pas que tout le monde, enfin, que tous sont de bons joueurs? Quelle est la réponse?

La réponse est que tout le monde doit tout vérifier. Mais cette fonction de vérification est extraordinairement difficile, parce que chacun de joueurs qui met en route, fait un routage, doit

réunir beaucoup d'informations tout le temps, sur les adresses, sur les politiques de routage.

Donc, il n'y a pas de directoire centralisé. Il n'y a pas de répertoire centralisé sur cela. Il s'agit d'un travail très difficile.

Donc, au lieu de faire cela, nous allons appliquer une solution qui est efficace en ce qui concerne le coût. Et cette efficacité dans le coût revient à dire, qu'à la limite, il y a certains points un peu vagues, il y a des choses qui se passent, le système est {incertain}, il y a des incidents vraiment remarquables par le passé.

Beaucoup d'entre vous qui êtes dans le domaine de la sécurité, vous êtes sûrs et conscients d'un incident qui a eu lieu pendant deux heures, mais il y a deux années où un ISP dans le domaine de l'Asie, dans la zone asiatique a pu bloquer l'accès Internet sur une bonne partie de la planète. Et la plupart de ces incidents que nous voyons sont les résultats du voyage que font certains {difficultés}. Parfois les choses marchent mal et se propagent sur l'Internet.

Mais, les questions d'aujourd'hui sont les vulnérabilités de demain. Il se peut qu'il y ait des choses que l'on fasse accidentellement et d'autres que l'on fasse à propos.

Le système dans lequel nous travaillons n'est pas bon. Vous pouvez voir que vos systèmes peuvent être parfaitement sûrs, votre Notebook peut être extraordinairement sûr etc., et c'est vrai que ça peut fonctionner parfaitement bien. Mais si le

système de routage est compromis, les paquets ne parviendront pas à leur destination. Et ils peuvent passer par certains points qui n'étaient pas prévus, non souhaités, et parvenir à une autre destination.

Il est évident que nous {ne} pouvons {pas} voir chacun des paquets. Les paquets sont très nombreux, nous ne pouvons pas tout prendre en compte, bien sûr. Nous pouvons équiper les routeurs, des personnes qui soient derrière eux.

Nous devons chercher un problème automatisé -- un système automatisé qui travaille à la même vitesse des routeurs. Il faut donc mettre un élément de discrimination dans notre infrastructure qui nous permet de détecter, d'exclure les essais ou les tentatives de mettre une information fausse sur le système de routage. Il faut pouvoir distinguer le bon du mauvais de façon automatique.

Il y a très peu d'outils de base pour réussir à cela dans nos systèmes publics. Comme on va vous dire à la cryptographie, il est facile de créer des cryptographies très sécurisées d'une seule forme. Mais ce n'est pas comme ça que l'Internet fonctionne.

Il est facile de créer des systèmes cryptographiques lorsque les deux parties vont échanger des informations et trouver -- et échanger des secrets. Nous n'avons pas ce système. Dans notre système les parties essaient d'échanger des informations. Elles ne se sont jamais réunies, elles ne vont jamais se retrouver. Elles ne peuvent pas non plus se retrouver. Cela limite la

possibilité des outils dont nous disposons à un ensemble très restreint. Et cet ensemble est celui de la cryptographie publique.

Ce que nous utilisons, des signatures numériques conventionnelles, qui est une clé privée, et cette clé privée peut la débloquer. C'est la seule à pouvoir la débloquer avec un appareil numérique.

La chose suivante, c'est comment envoyer ces clés publiques le long du réseau, comment on distribue tout cela, comment on fait pour que ceci soit injecté dans le réseau?

Alors, il faut comprendre, en premier lieu, la manière dont on décrit la confiance. Qu'est-ce que c'est que la confiance? Moi, j'ai une adresse, mon adresse IP est un numéro. C'est bizarre, non? 3, 10, 1.000.220. Comment le reste du monde va-t-il savoir que cette adresse IP est valide?

Parce que l'Internet doit travailler d'une manière unique, parce qu'il y a un système qui attribue les adresses vers un système. Il s'agit du cadre d'allocation d'adresse. Il y a une hiérarchie qui fait l'allocation, puis on l'envoie, cela passe par IANA, et puis on l'envoie dans les registres locaux, au terminal des ordinateurs.

Moi, j'ai mon nom unique, parce que APNIC me l'a octroyé. Le numéro APNIC est unique parce que IANA l'a octroyé à APNIC.

Si l'on pourrait décrire cette chaîne, on aurait donc la possibilité de créer de la confiance. Ce que l'on fait, ce n'est pas d'obtenir de nouvelles données. C'est que l'on essaie, c'est de reformater,

pour que les mécanismes d'authentification soient vraiment efficaces.

Cela nous amène au concept d'un certificat de ressources. Un certificat est un appareil assez vieux dans notre monde. Il y a des certificats numériques, les certificats X.509 qui est là depuis plusieurs décennies, il s'agit d'un document numérique, qui réunit des ressources de numéros et clés publiques. Il signe les clés privées avec les certificats.

C'est donc un appareil capable de valider et de signer quelque chose en disant: « Eh bien, cette adresse m'appartient, vous pourrez vous rendre compte si je suis en ligne ou pas, si je mens ou pas. » Vous pourrez authentifier mon affirmation, cela est quelque chose de vraiment important.

Et ce n'est pas quelque chose que les RIRs ont inventé. Je peux dire que nous avons travaillé conjointement comme RIR et dans les forces du travail d'Ingénierie Internet depuis 2006 pour créer une technologie viable et des standards permettant de construire et d'exploiter cela de la manière appropriée. Il s'agit donc d'une approche qui regarde vers l'avant.

C'est une manière de publier les mêmes données que nous publions toujours. Il s'agit d'un format différent parce que ce maintenant ce certificat X.509, c'est-à-dire, c'est justement ce genre de certificat que l'on utilise et ceux qui l'utilisent justement ont la sécurité que la clé est associée avec les adresses IP sans aucun doute. Et cela est dérivé directement de

la base de données d'enregistrement sous-jacente. Donc, on a la même information.

Nous avons maintenant ce concept, c'est comme la hiérarchie de nom de domaine. Il s'agit d'une hiérarchie des certificats numériques connus dans le monde de la sécurité, parce qu'ils adorent inventer de nouveaux termes, ils créent de nouveaux mots, alors qu'on pourrait utiliser les vieux mots sans aucun problème. Mais bon.

On parle de ressources PKI. Il s'agit d'une hiérarchie des certificats qui nous parle non seulement de mon identité, pas sur mon rôle, pas de ce que parle normalement ce genre de certificats. Il s'agit d'une hiérarchie qui parle des ressources numériques de l'IP. Et cela permet des déclarations, comme par exemple: « Eh, bien, moi je suis le propriétaire d'une adresse en particulier, et cette adresse peut être signée de manière digitale pour n'importe qui d'autre. » Et toute autre personne peut vérifier si cette information est véritable ou non.

Lorsque je dis n'importe qui, je dis vraiment n'importe qui, ou n'importe quoi, même n'importe quel routeur, n'importe quel élément de switching au sein du réseau et même toute interface de commande ou de contrôle pour le soutien opérationnel du réseau. Parce qu'on peut mentionner des choses qui sont liées directement au routage et à l'origine des adresses Internet.

Moi, Geoff, le propriétaire de 1.1.0/24, et je le suis, je peux autoriser à AS23456 et seulement ce réseau va se router envers

moi. Le corollaire est que si quelqu'un essaie d'attaquer mon adresse, non seulement moi -- c'est-à-dire, moi, je vais savoir que l'on est en train de mentir, mais toute autre personne sur Internet va savoir qu'il y a du mensonge. C'est plus difficile de mentir quand on sait que l'on ment.

Voici un nouveau développement pour nous. La sécurité est très difficile et la communauté a mené de longues discussions. On est conscient que dans plusieurs régimes il y a eu des certificats numériques et il y a eu des intérêts pour que les régimes numériques éliminent les certificats numériques. Il y a eu des discussions au sein de la communauté concernant l'obligation de la part d'un tribunal pour altérer ou pour révoquer un certificat.

Nous n'avons pas obtenu de réponses pour tout cela, mais ce que l'on observe c'est le même processus judiciaire ou par devant les tribunaux, comme celui qui permettrait au propriétaire d'un registre de changer le compte tenu, de révoquer les certificats. Voilà pourquoi nous disons que nous n'avons pas de solution mais nous n'avons pas non plus présenté ni réduit les problèmes concernant ces questions externes sur l'intégrité de la totalité du système de registre.

Il s'agit d'une hiérarchie comme le DNS et si l'on réussit à engager la racine, l'effet va vers d'autres parties de l'infrastructure. Et si on est très haut sur l'infrastructure les risques et les dommages sont énormes.

Ceci c'est la même chose que les certificats utilisés par Visa ou MasterCard. Si vous pensez au chaos, pensez ce qui se passerait s'il se compromettait, s'il s'engageait vraiment. Beaucoup de systèmes numériques qui sont liés à l'économie ont les mêmes problèmes. L'industrie a créé beaucoup de normes, beaucoup de standards capables d'assurer l'intégrité et l'exactitude des certificats. Ce sont des standards types FIPS, qui essaient d'établir les clés pour gérer la question. Nous essayons de faire de notre mieux. Notre système de gestion des clés, nos certificats sont en haut vraiment des standards de l'industrie.

Il y a aussi une question de résilience, il y a des défaillances. Mais le système actuel, notamment pour ce qui est de la publication des politiques, fait confiance à l'existence d'un site unique où ces politiques sont hébergées. Et c'est la manière de réaliser cette chose qui donne l'intégrité. Les données signées, c'est différent. Si les données sont signées, elles peuvent être publiées par n'importe qui. Et toute personne recevant toute copie peut immédiatement dire si ceci est fiable, s'il s'agit d'une copie fiable de l'original. Parce que du point de vue numérique on ne peut pas les distinguer.

Vous pouvez prendre une copie et la republier. Mais si on prend ceci republiée, on peut assurer que c'est exactement pareil à l'original, octet par octet. Il y a d'autres questions pouvant provoquer des défaillances, mais tout cela est dans notre infrastructure.

Où on en est maintenant? Nous en sommes très avancés dans le processus, parce que le système de routage a des vulnérabilités et le système des noms de domaine d'Internet est important. Nous essayons d'avoir plus de vitesse. Quant à l'infrastructure des certificats, beaucoup de registres régionaux ont essayé d'incorporer cela dans leur système. Les membres de ces communautés notamment peuvent créer les certificats suivant leur souhait depuis maintenant.

On continue à travailler avec les communautés pour compléter les mises en place ou les mises en œuvre. Il y a beaucoup de travail spécialisé. Il y a des différences dans la mise en œuvre. Donc certains RIRs font leurs travaux de manière un peu différente, mais les résultats seront appréciés dans un futur proche. Nous travaillons sur tout cela et nous croyons que les RIRs finissent leur travail rapidement.

Les certificats ne sont pas tout. Il faut les intégrer au système d'exploitation actuel, il faut avoir un PPS comme notre système. On a beaucoup travaillé avec les RIRs, mais seulement avec IETF et d'autres organes publics pour créer les plug-in, le module plug-in. Il faut aussi distribuer, synchroniser ces informations sur la validité de toutes les adresses, de tous les routages sur Internet à tout moment. Pour être sûr que ces données soient complètes et exactes tout le temps.

En même temps, l'IETF mène un travail visant à assurer le protocole de routage spécifique PGP. Nous avons fait des progrès, nous avons résolu quelques questions liées à

l'intégrité, l'intégrité des sessions. Mais maintenant nous voyons qu'il y a un problème d'enchaînement qui nous amène à prendre une pause pour penser.

Toutefois, on est optimiste et les courbes de technologie {de la loi de Moore} pour une connaissance plus poussée de la cryptographie nous permettra de résoudre ces questions comme dans d'autres cas. Nous croyons donc que nous serons capables de le faire dans un futur proche. Nous passons à la prochaine la diapositive.

Je crois que j'ai mentionné tout ce que je voulais. Avec plaisir je répondrai à vos questions. Merci beaucoup.

La Présidente Dryden: Merci. Je vois que la Nouvelle Zélande a demandé la parole.

La Nouvelle Zélande: Merci. La question pour le GAC. Y a-t-il une politique publique ou un empêchement en termes de politique publique pour réussir à se faire quelque chose, que le GAC puisse faire pour accélérer la mise en œuvre de ce protocole? Merci.

Geoff Huston: Il est vrai que certains organismes internationaux, pardon nationaux, sont conscients de cette problématique. Ils ont travaillé très activement pour soutenir la recherche et le développement dans certains organismes des États-Unis. Ils ont travaillé pendant beaucoup d'années, mais ce n'est pas le seul

pays. Nous avons vu pas mal d'autres pays qui sont conscients du problème et qui donnent leur soutien aux activités. Et ça c'est bien.

Nous n'opérons pas dans les termes et les conditions et de l'immunité dans un environnement judiciaire. Mais lorsque l'on voit les certificats des communautés qui expriment leur préoccupation disant qu'un tribunal puisse dire qu'il faut révoquer un certificat parce que les conséquences de cette révocation, ce n'est pas seulement qu'elle ne va pas avoir cette adresse, c'est -- pardon, les certificats du routage disparaissent aussi. Cela veut dire que l'on enlève la validité de la présence de cette adresse et cette adresse disparaît pour tout le reste. Et si l'on introduit l'insécurité, on introduit ces autres facteurs innovants dans certains cas.

Je ne suis pas sûr d'avoir toutes les réponses. Je ne peux pas répondre à toutes les inquiétudes, mais il faut parler de cela dans les forums de politique publique.

La Présidente Dryden: Merci, John tu voulais répondre aussi et Paul demande la parole aussi.

John Curran: Pour ce qui est de l'encouragement de cette mise en œuvre, il est important de rappeler que la décision d'un fournisseur de service d'utiliser RPKI et d'avoir la sécurité de la politique de routage, c'est quelque chose de volontaire. Les fournisseurs de

service décident de participer de l'infrastructure RPKI et en faisant cela, le routage est moins vulnérable. De même, ils décident de faire attention à une autre information de l'RPKI parce que lorsqu'ils reçoivent les données, l'information de routage, ils ne vont pas recevoir des informations incorrectes.

Voilà pourquoi on utilise beaucoup l'RPKI et tout le monde fait attention aux données reçues. Mais pour les fournisseurs tout cela est justement une décision volontaire. Dans notre région il y a le Canada, les États-Unis et 26 économies des Caraïbes. Je suis conscient qu'aux États-Unis il existe des groupes de fiabilité d'Internet, il y a un groupe de meilleures pratiques parrainé par la sécurité.

Il y a de différentes manières de percevoir cette problématique. Mais ce n'est pas quelque chose que les RIRs exigent. Nous sommes dans un emplacement naturel pour fournir l'infrastructure. Et pour l'utilisation et l'emplacement et tout le reste dépend d'une décision volontaire. Merci beaucoup.

Paul Wilson: John a très bien travaillé sur d'autres questions qu'il faudrait rappeler pour voir le système actuel comme un système où les RIRs offrent les détails d'enregistrement des adresses que nous avons allouées. Les certificats, dans une certaine manière, dans la mesure où ils ont une signature de registre, sont gérés de la même manière qu'un courriel avec une signature numérique qui indique que l'origine est véritable.

John a parlé de ce processus qui est important. Le fait de considérer la décision des fournisseurs à travers l'option de participer voir que se passe-t-il dans la moitié de l'équation, et de l'autre part voir ce qui arrive avec données reçues. Ce système a évolué de manière absolument compatible avec le processus accordé de notre système des RIRs ascendant au lieu d'être imposé.

Le fait pour lequel nous faisons cette présentation c'est que nous sentons que notre système a été en développement pendant longtemps à travers ce processus et que les RIRs ont suivi le processus pendant des années. Nous trouvons que les questions sur le système ont commencé à se propager de manière plus systématique. Et cela est nécessaire pour que le GAC ait une perspective mise à jour. Pour ce qui est du fonctionnement du système et pour nous assurer qu'il y ait une compréhension commune, eh bien, il faut penser à ce système que nous venons de décrire, différent de celui du passé.

La Présidente Dryden: J'ai le Portugal, la Norvège, la Malaisie, la Commission Européenne. Le Portugal, s'il vous plaît.

Le Portugal: Merci beaucoup de la clarté de la présentation. Il s'agit d'une question absolument technique et vous l'avez présentée d'une manière absolument compréhensible.

Je savais du système à partir des efforts de la RIPE. Ma question a trait à ce que la Nouvelle Zélande a mentionné. Pour ce qui est du rôle du GAC, ce qui serait intéressant de savoir: « Qu'est-ce que vous pensez? » Il s'agit des questions que nous pourrions faire du point de vue du conseil que nous pouvons donner. Pour être clair je ne sais pas comment. Mais du point de vue de l'approbation des politiques au niveau national ou tout simplement pour sensibiliser. Ce serait bien d'établir clairement ce que les gouvernements peuvent apporter pour cela. Merci beaucoup.

Raul Echeberria: Merci Madame la Présidente. L'objectif pour lequel nous sommes ici en parlant de cette question avec le GAC c'est parce que nous voulons vous commenter ce que nous faisons pour que les gouvernements soient au courant de tout cela. Je crois qu'il s'agit d'un changement important pour l'Internet. Il s'agit d'un projet que, comme Geoff l'a mentionné, a déjà beaucoup d'années de travail. Il y a un grand investissement qui a été fait en termes de temps, travail et argent. C'est important pour l'Internet et il est important que les gouvernements le connaissent. Il est probable que ce soit la manière principale où ils puissent nous aider. S'ils souhaitent sensibiliser, il faut sensibiliser sur cette problématique au niveau des industries locales comme John l'a mentionné. Il y a un cas aux États-Unis. On peut le faire un peu partout.

Madame la Présidente: Merci Raul. La Norvège, la Malaisie, la Commission Européenne, l'Uruguay le Royaume-Uni.

La Norvège: Merci Madame la Présidente. Merci Geoff de cette mise à jour. Et merci de toute l'information si importante que tu nous as donnée.

Je crois que pour nous en tant que gouvernement il est important de savoir ce qui se passe avec ce système parce que l'on prend des mesures de sécurité très importantes sur Internet. Et je voulais aussi commenter, faire des commentaires sur les questions liées aux politiques publiques. Je crois que la question que nous avons traitée nous amène à penser que nous pouvons créer conscience et aussi favoriser les meilleures pratiques dans les régions avec des réglementations dans différentes parties de l'Europe à laquelle appartient la Norvège. Nous avons les entités de régulation capables d'établir des mesures de sécurité pour les fournisseurs des services Internet si l'on considère que cela est approprié. Nous pouvons donc travailler en Norvège de cette manière-là.

Nous sommes en mesure d'établir ce mandat pour les ISP norvégiens. Mais je crois aussi que ceci peut devenir une meilleure pratique entre les ISP du monde. Et avec l'Internet on ne peut pas appliquer des mesures isolées, parce qu'il s'agit d'un système mondial. Alors il est important de le voir à partir de cette perspective.

Une question technique. À vrai dire, il y en a deux. Il y en a une qui est plus technique et une autre qui a trait aux délais.

Quand est-ce que le système va être opérationnel? Quand est-ce que les candidatures, les routeurs vont être prêts et quand est-ce que l'on va réaliser la standardisation pour que ceux-ci soient mis en place et finalisés?

L'autre question est liée aux certificats. Les RIRs vont avoir des certificats à signer qu'ils vont pouvoir utiliser pour signer les ressources. Parce qu'il y a des inquiétudes, des soucis de certains gouvernements, pas du nôtre. Les inquiétudes concernent les RIRs et si les RIRs vont avoir des certificats signés, s'ils vont être contrôlés par une autre partie. En cas de révocation des certificats ceux-ci pourraient gâcher tout l'Internet. Je voudrais savoir comment cette chaîne de confiance va-t-elle être construite au sein du système RPKI?

La Présidente Dryden: Geoff tu veux répondre ça.

Geoff Huston: Je veux dire quelques mots et ensuite je passera le micro à ma collègue.

Lorsque l'on parle de meilleures pratiques par opposition à une condition réglementaire pour l'utilisation de ce type et pour la mise en œuvre de ce type de technologie et c'est vrai que dans le DNSSEC {si j'ai Geoff.potaroo.net, il sert à rien de le signer

sauf si potaroo.net est signé aussi.} Parce que c'est ça qui est important dans la DNSSEC, qu'il faut arriver à ce niveau de la racine, mais notre système de routage n'a pas cette possibilité d'établir une hiérarchie de routage.

Si nous avons assuré BGP et ensuite nous passons à une information de routage moyenne d'une section d'Internet qui ne met pas en ouvre cette modalité de BGP toute l'information de sécurité est perdue. Et lorsque nous arrivons à notre point où cela a été mis en œuvre cela ne parviendra pas à ce point.

Donc BGP est un protocole qui peut nous donner bon nombre de bénéfices, et l'un de ces systèmes. s'il était utilisé partout. fournirait un grand bénéfice au niveau universel. Si on le fait par partie il faut voir qui va recevoir les bénéfices et qui peut être assuré en termes de routage ; parce que ce bénéfice s'est énormément réduit finalement.

Donc il faut réfléchir soigneusement à cette question sur ce qui peut être une meilleure pratique de l'infrastructure au niveau régional et international. Et il faut penser soigneusement comment élargir au plus grand nombre tout cela et ne pas imposer en même temps des coûts prohibitifs de haut risque à l'environnement et d'exploitation. Il est évident que cela fait partie d'un ordre du jour des politiques publiques au niveau national qui doit traiter la manière dont on effectue la mise en œuvre, partie par partie, pour la technologie. Parce que cela n'est pas aussi bénéfique qu'une mise en œuvre à l'échelle universelle.

La Présidente Dryden: John, je suggérerai -- enfin, nous pourrions peut-être parler de BGP un tout petit peu et nous mettre en contexte parce que tout le monde ne connaît pas ces normes.

John Curran: Je m'appelle John Curran et je vais prendre les trois autres questions qui étaient implicites dans cette question explicite.

En premier lieu, je veux dire que par rapport au temps les RIRs {ont leurs} propres calendriers de mise en œuvre. Et ceci pour la structure, pour les certificats numériques. Que ce soient les missions ou les liens avec les fournisseurs de service. Donc, dans ce cas particulier nous avons un calendrier. Il y a d'autres RIRs qui sont beaucoup plus avancés qu'ARIN. Et la manière dont fonctionnent les responsabilités dans notre région est telle qu'il faut que nous prenions beaucoup de précautions pour nous assurer d'associer nos activités de signatures numériques avec toutes les organisations pour qu'il n'y ait pas de rejet.

C'est-à-dire que nous puissions confirmer que l'ISP a vraiment demandé ces certificats. Ceci nous demande de travailler plus fortement. C'est peut-être nous qui sommes le plus en retard. Et nous réfléchissons à une date entre cette année, la fin de l'année prochaine pour avoir ce service. Je crois que le reste des services régionaux ont déjà préparé leur propre service à l'heure actuelle. Donc leurs délais sont beaucoup plus courts.

Par rapport aux certificats utilisés par les RIRs et l'ancre de ce que nous appelons la confiance, l'ancre de confiance, il y a beaucoup d'information pour établir un élément numérique dans les systèmes qui suscitent la confiance. Si nous parlons de plusieurs routeurs et que nous pouvons avoir ces ISP vous pouvez configurer votre registre avec cette ancre. De cette manière, vous pensez que cela a été émis sur ces cinq RIRs et surtout ce qui est en dessous.

Il est vrai qu'il faudrait aussi, il vaudrait mieux avoir une seule ancre de confiance globale et que l'IETF pardon puisse émettre ceci avec les RIRs. Nous allons avoir une réunion avec l'équipe d'Elise Gerich pour voir que cela soit faisable. C'est là que nous allons pouvoir travailler non pas avec cinq ancres mais avec une seule ancre globale qui utilise les ressources des cinq RIRs avec d'autres ressources préservées, des ressources des adresses hyper réservées à des propos spécifiques.

Ceci peut être configuré de façon individuelle. C'est ça qui est bon. C'est-à-dire qu'une partie qui dépend d'un seul ancre d'un seul RIR peut l'activer de cette façon ou pas.

J'ai entendu dire qu'on avait parlé de régulation et de la manière dont cela peut nous aider. Il y a une étape préalable à celle de la régulation en termes d'influence et d'incidence. Beaucoup de gouvernement sont utilisateurs de la terminologie « technologitique. » Parce que vous voulez des fournisseurs de service qui vous offrent un routage sûr. Vous en tant que clients, vous devriez leur demander de le faire. C'est une bonne

manière de distribuer ou de susciter l'intérêt ou de diffuser l'intérêt que vous portez à la mise en œuvre de cette technologie.

Je ne veux pas omettre cette étape intermédiaire où vous en tant qu'utilisateurs des ITC ; vous pouvez demander la qualité des services pour un routage absolument sûr.

La Présidente Dryden: Je donne la parole à la Malaisie.

La Malaisie: Merci beaucoup Madame la Présidente. Merci de nous avoir présenté cette technologie. Je voudrais dire qu'en ce moment il y a beaucoup de défis à soulever pour promouvoir le DNSSEC parmi nos ISPs. Même si nous avons une réglementation nous voudrions que cela se fasse de façon volontaire et vous devez comprendre que la mise à jour est très lente. Je suis très intéressé à la question des dates butoir et des délais des programmes de diffusion pour que nous puissions promouvoir cette technologie dans nos pays et parmi nos ISPs. Merci beaucoup.

Madame la Présidente: Est-ce que tu voudrais répondre Adiel?

Adiel Akplogan: En termes de délais nous travaillons tous ensemble pour pouvoir établir les mêmes délais, les mêmes dates butoir et avancer en ce sens-là. Nous pensons à une plateforme pour pouvoir avoir des certificats et pouvoir signer. Le système est déjà en marche. Il peut déjà être utilisé. L'objectif de la présentation d'aujourd'hui est de sensibiliser les gens au sein du GAC pour que vous puissiez à votre tour sensibiliser à ce sujet localement.

Nous avons aussi une bonne approche des fournisseurs qui ont intégré cette technologie dans l'IOS de telle façon qu'on puisse l'utiliser dans le monde réel d'Internet. Bien sûr la mise à jour va être lente, mais elle est là, et c'est sûr que nous allons pouvoir encourager les gens à s'en servir aussi vite que possible.

Madame la Présidente: Merci beaucoup. Nous avons la Commission Européenne, l'Uruguay, le Royaume-Uni et ensuite nous allons clore la séance.

La Commission Européenne: Merci beaucoup Madame la Présidente. Je voudrais remercier aussi les présentations qui ont été faites et leurs auteurs d'avoir parlé d'une technologie très importante et de la rendre compréhensible pour tous. Nous savons que ce n'est pas une tâche facile. C'est pourquoi nous leur exprimons notre reconnaissance.

J'ai deux questions à répondre qui peuvent avoir votre réponse par n'importe qui. En ce qui concerne l'ancre de confiance, nous ne parlons que des registres d'Internet ou nous parlons d'autres registres qui pourraient avoir des ancres fiables dans le système. Est-ce qu'il y a des conditions ou des contraintes pour une entité pour qu'elle puisse être une ancre de confiance, pour qu'elle puisse donner ce type de services Internet aux opérateurs Internet?

Une deuxième question c'était – au début, j'ai entendu dire au début que c'était Monsieur Huston qui parlait du fait que la communauté s'inquiète à propos de la prise des décisions impliquant la révocation du certificat numérique par l'utilisation du système de RPKI.

Je voudrais savoir si vous pouvez m'expliquer quelle partie de la communauté a cette inquiétude ou ce doute, s'il y a eu des cas de rejet ou si cela pourrait avoir lieu à court terme.

En tant que Commission Européenne nous n'allons pas faire de commentaires sur ce que font ou ne font pas les communautés locales, parce que ce n'est pas notre travail. Mais nous voulons savoir si cela se passe déjà ou si c'est une inquiétude hypothétique comme celle que nous en tant qu'autorité publique nous, enfin -- sommes accusés d'exposer publiquement. C'est pur ça que je vous demande cette précision.

Geoff Huston: Qui peut être une ancre fiable? Bon, nous allons aller revenir. Qui peut émettre des certificats démontrant que l'une des parties a une ressource? Où est la titulaire d'une ressource?

{En théorie,} n'importe qui pourrait le faire. Mais qui peut-on, doit-on croire? La partie qui a emis les ressources, c'est la meilleure ; c'est celle qui peut émettre les certificats. Donc si APNIC crée un blog d'adresse vers un registre Internet local, alors ce que les certificats que l'APNIC émet c'est les certificats auxquels il faut faire confiance.

Et il y a une autre sortie digitale et c'est sur cela -- et c'est à cela qu'il ne faut pas faire confiance. Donc la question de la confiance a été très clairement, le modèle de confiance a été très clairement dessiné par rapport aux modèles des adresses, allocation d'adresse. Dans la mesure où ce sera sûr n'importe qui pourra choisir le modèle qu'il voudra. Mais nous allons leur recommander d'utiliser l'ensemble de confiance correspondant aux agences qui alloue les ressources en premier lieu.

Qu'il s'agisse de donner de confiance de matériel émis par n'importe lequel de cinq RIRs ou que l'on se serve d'une entité de confiance pour décrire l'IANA, cela dépend de vous. Mais il ne serait pas très intelligent de reproduire ce que nous avons fait sur les navigateurs, parce que nous avons eu davantage plus de 700 entités. C'est trop. Donc il vaut mieux que ce soit un nombre soit plus réduit mais nous avons besoin d'avoir un certain -- mais on n'a pas besoin d'avoir un seul nombre.

Quant aux inquiétudes il faut dire qu'elles se rapportaient plutôt aux domaines européens et que cela devrait être discuté dans les forums appropriés. Malheureusement Axel n'est pas là.

Il y a eu des moments où dans un espace différent pour des raisons différentes il y a eu des ordres de révocation de certificats avec d'autres objectifs des tribunaux. Est-ce que nous pouvons donc appliquer cela aux certificats numériques? Nous voudrions penser que ce n'est pas possible parce que les certificats sont un miroir du compte tenu du registre sous-jacent. Et révoquer un certificat ne change en rien le registre en lui-même mais le rend un peu plus difficile et je ne suis pas très sûr que cela ait été l'intention dans ce processus-là.

J'aimerais bien penser qu'au fur et à mesure que l'on avance dans ce processus et que nous comprenons davantage quelle est l'intégration des attestations et la cryptographie numérique dans cette infrastructure le risque que les sociétés, les institutions et les outils fonctionnent avec ça et qu'ils apprécient leur propre rôle et leurs responsabilités par rapport à ça, la révocation n'aidera en rien. Merci beaucoup.

La Présidente Dryden: Merci beaucoup. Maintenant donc c'est l'Uruguay qui prend la parole.

L'Uruguay: Merci beaucoup de la présentation.

Je ne sais pas si je l'ai perdu mais je voudrais comprendre comment cette infrastructure est liée à l'infrastructure nationale publique. Non seulement par rapport au point de vue technique, mais aussi au point de vue légal.

Vous savez que dans chaque pays la valeur légale d'une -- d'un certificat, pardon, et de la confiance dans les systèmes de l'infrastructure est liée aux autorités de certification qui ont le pouvoir d'émettre ces certificats donnés par une entité de réglementation. C'est-à-dire l'infrastructure publique nationale est liée avec un certain type d'adéquation. Je veux savoir comment cela est lié. Je voudrais savoir s'il y a un certain type de compatibilité ou pas.

John Curran: Vous posez une question légale et moi, je ne suis pas avocat. Une fois dit ceci, dans le processus d'exploration des aspects pour l'émission de certificats RPKI il semblerait bien que chaque pays a son propre cadre pour l'invalidité légale d'un document avec une signature numérique, cela signifie que les RIRs lorsqu'ils émettent ces certificats. Enfin, nous nous assurons que nous savons, que nous pouvons savoir la signification de ces certificats.

C'est-à-dire nous parlons du possesseur des ressources et ce que ce possesseur considère, ou à quelle entité il donne la possibilité de mettre en route, de faire le routage de ces certificats. Je sais que dans certains pays il y a des juridictions nationales qui font ces certificats et les rendent équivalents aux

documents signés, émis par le registre. Cela a des implications pour le registre qui émet ce document et cela fait que nous devons tous être très attentifs à la façon dont on les -- nous faisons le routage. Mais cela est une situation qui est définie pays par pays.

Je ne peux pas donner une réponse générale. Je peux dire cependant que les fournisseurs des services dans les pays qui émettent ces certificats doivent pouvoir comprendre qu'ils émettent, donc parfois des documents qui ont la même force légale.

L'Uruguay: Si l'ISP a une responsabilité légale au cas où il commettrait un délit en tant qu'ISP le cadre légal dans lequel nous travaillerions c'est le cadre national. Et ce cadre légal est réglementé par ces lois nationales et ces lois nationales ont une infrastructure nationale.

Pour l'une des questions. Donc, que peut faire le GAC pour essayer de résoudre cela? Avoir peut-être une certaine compatibilité, établir une certaine compatibilité entre les cadres nationaux et ceci pour pouvoir donner une base légale au travail que l'on fait avec les ISP au niveau local. Mais je crois que nous devons avoir davantage d'informations de votre part pour pouvoir savoir comment travailler chacun de nous dans nos propres pays.

John Curran: Je suis d'accord.

La Présidente Dryden: La parole à Raul Echebarria.

Raul Echebarria: En ce qui concerne IDN il s'agit d'une infrastructure séparée. Les certificats émis dans ce cadre n'ont pour objectif que l'utilisation, leur utilisation pour le routage. Donc il n'y aura pas de transactions dans l'utilisation de ces certificats.

Les ISPs ne vont pas se servir de ces certificats pour faire des transactions au niveau local. Il n'y aura aucune responsabilité légale à cet égard. Ils vont utiliser cette information seulement pour savoir si le réseau qui annonce un block d'adresses Internet est le réseau qui a l'autorité pour le faire ou pas. Cela va permettre de prendre une décision sur le routage et rien d'autre.

Donc c'est pour cela que ces certificats ne vont être utilisés dans aucun pays pour qu'un objectif réglementé dans le cadre légal de chacun des pays.

Je ne sais pas si cela répond à votre question.

L'Uruguay: Au cas où l'ISP n'utiliserait pas de façon incorrecte le routeur pour utiliser le réseau ou pour endommager le réseau.

Geoff Huston: Il y a beaucoup de certificats. Il y a en qui sont utilisés dans le système des noms de domaine pour les sites web http. D'autres sont utilisés pour démontrer l'identité des citoyens d'un pays. De façon conventionnelle, nous trouvons que normalement les certificats qui ont un intérêt national réglementaire sont des certificats qui prouvent l'identité et le rôle des gens.

Mais les certificats peuvent faire bien plus que cela et ceux avec lesquels nous travaillons, sont des certificats beaucoup plus semblables à ceux qui sont utilisés dans le système des noms de domaine. Quant à l'association d'un nom de domaine avec une adresse IP pour les sites web sûrs. De façon conventionnelle, ces certificats qui tombent directement dans le cadre réglementaire, légal par eux-mêmes de manière conventionnelle ont dans beaucoup de cadres un plus fort lien avec les pratiques nationales de l'industrie. Nous dirions que ces certificats qui ne prouvent pas l'identité, qui ne prouvent pas le rôle joué, mais qui associent deux clés ont une réflexion d'un appareil technique qui est différent de rôle.

Donc, il se rapporte plutôt au domaine réglementaire qui parle des artéfacts techniques et les questions techniques telles que les certificats de domaine qui sont différents de certificats d'identité ou les certificats de rôle. Je ne vois pas donc quel est l'intérêt de réglementation dans ce domaine, dans ce type pardon de chose comme c'est notre cas.

La Présidente Dryden: Nous allons devoir écouter notre dernier orateur. J'espère que cet échange pourra continuer off line et nous allons pouvoir continuer à parler de cela dans l'avenir au sein du GAC.

C'est le Royaume-Uni qui prend la parole et enfin nous allons clore la séance.

Le Royaume-Uni: Merci Madame la Présidente, merci de la présentation. C'est très utile pour nous et cela est un complément pour l'information reçue en Europe de la part des gouvernements européens.

Ce c'est qu'on nous avait dit en ce sens-là. RIPE NCC nous l'avaient dit et cela nous rappelle que le routage sûr continue à être notre objectif pour la communauté. Nous espérons que ce but pourra être atteint.

Et d'après ce que je me rappelle, selon les rapports européens que nous avions reçus il était clair que toute l'industrie n'était pas en ligne avec certaines des réponses que vous aviez données ici. Je parle des ISPs, bien sûr.

Pour le gouvernement il est évident que nous devons continuer à voir si l'industrie enfin ne parle pas d'une voix unanime. Et lorsqu'il s'agit de voir ce que nous pouvons faire pour promouvoir la sensibilisation et la prise de conscience. Nous avons un peu la sensation d'avoir une seule main disponible. Et nous disons à l'industrie: Ok, il faut trouver une manière d'aller de l'avant et je connais RIPE NCC et il nous montre le travail

qu'il fait dans ce domaine et quels sont les rapports. Nous allons avoir assurément davantage d'informations sur ceci lorsque nous nous réunions avec eux.

Il y aura aussi d'autres RIRs qui vont nous donner de l'information. Au ministère où je dirige le conseil technique...les points techniques.

Je veux faire, je veux poser deux questions de base qui ne sont pas techniques. D'abord si l'extensibilité du système du nom de domaine qui a des milliers de gTLD possibles pour les prochaines années, dix années à venir, et qui va permettre d'ajouter -- enfin, d'ajouter plusieurs gens à ces travaux-là.

Et ensuite la deuxième question c'est pourquoi la mise en oeuvre du RPKI n'aura pas d'impact significatif sur l'abus du système de DNS, d'usage frauduleux du système de DNS. Merci beaucoup.

Geoff Huston: La question est simple, la réponse ne l'est pas. Les noms et les chiffes fonctionnent de manière différente et c'est pareil dans ce cas particulier. Et l'expansion de l'espace des noms dans le nouveau gTLD n'a aucun lien avec ces ressources de RPKI. Ils sont complètement séparés, ils n'ont aucun lien.

La question de l'extensibilité, enfin de l'augmentation de l'insécurité sur l'Internet est très intéressante. Il y a 15 ou 20 ans, l'insécurité était le produit d'un enfant de 15 ou 16 ans, très aventurier, qui n'avait rien a faire pendant l'après-midi.

Maintenant lorsque nous voyons l'insécurité nous voyons que cela est devenue une industrie, une industrie criminelle, mais une industrie en fin du compte.

Et bien sûr avec la valeur des transactions sur Internet, modifier l'opération normale d'Internet de façon malicieuse c'est quelque chose qui est très intéressant pour les joueurs qui ne jouent pas de façon légitime et qui ne méritent pas notre confiance. L'attaque au routage c'est quelque chose que l'on peut faire avec des ressources et des connaissances et qui peut être une attaque très efficace. On peut attaquer des points spécifiques sur les réseaux ou bien on peut élargir l'effet d'une attaque.

Ce n'est pas une situation confortable et certainement il y a des mesures à prendre pour assurer le routage qui ne sont pas mis en œuvre parce que nous n'avons rien à faire la semaine prochaine mais tout simplement parce que nous avons un agenda vraiment très chargé. Donc l'infrastructure de la insécurité est le plus terrible des problèmes auxquels nous devons faire face. Tout le reste peut fonctionner comme il le faut. Mais si l'infrastructure, si le triangle va dans la mauvaise direction, le triangle avance de toute façon.

Mais certainement nous voyons qu'il y a une mise en œuvre comme un facteur d'atténuation des questions potentielles sur lesquelles l'Internet peut être modifié de façon malicieuse. Donc tel est l'effet de la base criminelle ou d'autres modalités de criminalité organisée. Voilà, c'est important.

La Présidente Dryden: Je vous remercie comme d'habitude. Je remercie le NRO, l'ASO d'avoir présenté ce thème. Il y a eu un haut niveau d'intérêt qui a été exprimé, c'est pour cela que je ne voulais pas interrompre le débat. J'espère que nous pourrons revenir sur ce thème dans l'avenir et je vous remercie encore une fois.

Pour le GAC, nous n'avons pas, nous nous sommes pas bénéficiés par des déjeuners très court. Je suggère de revenir à 2:45 et nous allons reprendre notre agenda à 2:45.

J'espère que vous auriez un bon appétit.

{Fin de la transcription}