ICANN79 | Forum de la communauté – Séance plénière d'At-Large 2 : renforcer la confiance dans Internet grâce à la vérification des titulaires de noms de domaine
Mercredi 6 mars 2024 – 4h15 à 5h30 SJU

MICHELLE DESMYTER: Bonjour, bienvenue à la deuxième plénière de l'At-Large, construire la confiance sur l'internet grâce à la vérification des titulaires, je suis la responsable de la participation pour cette séance. La séance est enregistrée et régie par les normes de comportement attendues par l'ICANN.

Les questions et commentaires pendant cette séance seront lus à voix haute si elles sont soumises par le biais des questions et réponses sur Zoom. Si vous souhaitez prendre la parole pendant la séance, levez la main sur Zoom et quand on donnera votre nom vous pourrez allumer votre micro sur Zoom. Dans la salle vous pourrez prendre la parole avec le micro.

Nous aurons l'anglais, l'espagnol et le français comme interprétation. Donnez votre nom et la langue que vous allez parler si ce n'est pas l'anglais. Sur ce, je cède la parole à mes collègues.

MICKAËL PALAGE: Je suis le coordinateur de la séance avec Avri Doria, voici comment cela va se passer. Notre séance sera très interactive avec les participants tant en ligne que dans la salle.

Je vais m'occuper principalement des activités des personnes qui sont dans la salle et Avri s'occupera de tout ce qui est sur Zoom et dans la rubrique questions/réponses.

Comme vous avez vu, nous avons deux panels différents, le premier va s'occuper de l'aperçu de la question de la confiance, nous avons 3 éminents intervenants aujourd'hui. Et la deuxième partie de la séance sera consacrée à un tour de table, c'est comme ça que fonctionne notre centre. Et ce sera là l'occasion pour comprendre comment les opérateurs de registre individuels s'occupent de la vérification de nom de domaine et comment il intègrent différents aspects de la qualification des identités numériques pour en tenir compte.

Voilà la feuille de route. Et, pour ne pas perdre de temps, je passe la parole à Finn, directeur d'International ICT, une agence de relation pour le gouvernement numérique. Il va parler de NIS2.

FINN PETERSEN : Merci. Voici mes diapositives à l'écran. Merci pour l'invitation. Je travaille à l'agence, comme vous l'avez dit, et je suis aussi président de deux groupes de travail de l'UE sur des directives. La première concerne les mesures de sécurité numérique pour l'infrastructure et les services numériques. Et je préside aussi au flux de travail sur le WHOIS. Et c'est à ce titre que je vais parler de l'article 28.

Diapositive suivante s'il vous plait.

Voici, en quelques mots, l'essentiel dans la directive NIS au sujet du WHOIS et l'article 28, je vous encourage tous à le lire, j'ai essayé de le

résumer un peu. Et ce qui se passe sous cette obligation ce sont les registres et l'octroi de services d'enregistrement de noms de domaine.

On a les opérateurs de registre, les fournisseurs privés, les fiduciaires. Donc voilà les obligations qui leur incombent s'ils ciblent des clients en Union Européenne, qu'ils aient leur siège en UE ou ailleurs.

Donc il y a des exigences pour ce qui est de la collecte de données WHOIS. On s'est posé la question du RGPD, mais ici il est clairement indiqué dans le NIS2 qu'il faut collecter les données à des fins de sécurité, de stabilité, de fiabilité de l'internet. Donc c'est légitime.

Ces deux directives précisent également quel genre de données il faut recueillir : le nom de domaine, la date d'enregistrement, le nom du titulaire de domaine ainsi que son adresse email et un numéro de téléphone.

Et si vous avez chargé quelqu'un de le faire et bien c'est son adresse et son numéro de téléphone qui doivent aussi être recueillis.

Ces données doivent être exactes, actualisées et vérifiées. Donc toutes ces données doivent être exactes, complètes et vérifiées.

Les intéressés sont également tenus de publier sur le site web WHOIS les informations qui sont de nature non personnelles. Il est aussi obligatoire de publier des informations au sujet des entités juridiques, leur nom également, même si cela contient un nom personnel. Par exemple si j'ai une entreprise qui s'appelle Finn Petersen, et bien cela doit être présent dans le WHOIS ouvert.

Il existe aussi une obligation de donner accès aux données WHOIS aux demandeurs d'accès légitimes, à des fins légales.

Prochaine diapositive.

Voici une disposition qui sera traduite et mise en œuvre dans les lois nationales des pays de l'UE dans 7mois et demi. Et il appartient aux États membres de les mettre en place dans un certain degré de liberté. Il y a quelques exigences minimales et ils peuvent rajouter certaines dispositions supplémentaires.

Et dans cette directive il y a un groupe de coopération composée par les États membres, la Commission y participe et l'ESA, l'agence de sécurité de l'Europe y participe également. Ensemble ils sont 27, j'en ai fait une petite liste, ils ont fourni une information des meilleures pratiques pour ce qui est de la mise en place de cette directive.

Prochaine diapo.

Ils ont créé un flux de travail, ce qu'on appelle un work stream, c'est moi qui m'en charge en partie sur le WHOIS. Et cela a pour objectif d'écrire des lignes directrices basées sur l'article 28 et afin d'avoir une approche harmonisée pour ce qui est de la mise en œuvre de l'utilisation des dispositions dans la directive.

Les membres jouissent d'une certaine liberté, mais nous espérons qu'avec ces lignes directrices nous saurons harmoniser le paysage en Europe et nos approches. Nous savons qu'il ne devrait pas y avoir de différence de condition, peu importe l'État membre en UE.

Prochaine diapo.

Nous avons également créé deux équipes d'experts, la première est la task force sur la vérification et cette équipe s'attachera à écrire des lignes directrices pour vérifier les données WHOIS et pour voir comment vérifier des données WHOIS qui sont déjà existantes. Dans cette directive, aucune distinction n'est faite entre les anciennes et les nouvelles données des titulaires de nom de domaine, elles devraient toutes être actualisées, vérifiées et exactes. Donc nous essayerons d'émettre des lignes directrices et l'équipe devra aussi passer en revue des données que vous avez déjà collectées.

Mais, quoi qu'il en soit, c'est une exigence au titre d NIS2.

L'autre équipe d'experts se penchera principalement sur les accès légitimes qui devraient être considérés comme étant demandeur d'accès légitime. Certaines dispositions servent de réponses aux demandes de ce qu'on appelle la partie fermée du WHOIS. Et nous préciserons quel genre d'informations doivent être révélées dans les 72 h et nous verrons aussi les requêtes urgentes. Nous écrirons des lignes directrices à ce sujet. Et s'il n'y a pas de ligne directrice ou pas de mouvement dans cette communauté et bien nous pallieront cette lacune avec l'entremise des États membres. Et le but, encore une fois, c'est l'harmonie d'un bout à l'autre du système.

Et je répète, pour ces deux paragraphes, il appartient aux États membres de le mettre en œuvre ; vous pouvez lire le texte et l'interpréter d'une manière ou d'une autre.

Vous savez, le diable est toujours dans les détails quand on parle des États membres et de NIS2, donc on va essayer d'avoir le même diable dans les États membres. Reste à voir si les États membres vont se plier à ces lignes directrices. Nul ne le sait pour le moment, mais au moins, si nous nous mettons d'accord sur les lignes directrices, cela pourra aiguiller les États et ils pourront œuvrer dans le même sens, c'est beaucoup mieux que si personne n'émettait de lignes directrices.

Encore une fois, le mot clef c'est l'harmonisation de notre approche.

Voilà pour l'article 28, il y a d'autres dispositions dans cette directive qui, bien entendu, concernent les TLD, les fournisseurs de DNS, les CDN, etc., et il s'agit là de mesures de sécurité.

D'autres règles sont à venir de la part de la Commission Européenne, je suis responsable d'un groupe – entre autres – qui a participé à cette réflexion. Et certaines de ces lois ne sont pas toujours adoptées par les États membres à titre national, mais sont quand même applicables à tous ceux qui sont dans le champ d'application de NIS.

MICKAËL PALAGE: Très bien, Finn doit retourner au GAC, et au communiqué. Donc s'il y a des questions, soumettez-les dans la rubrique questions et réponses sur Zoom et tout le monde pourra les lire.

FINN PETERSEN : Merci, c'est bien plus intéressant que le communiqué au GAC, mais je dois vous quitter, malheureusement. Merci.

MICKAËL PALAGE: Prochain intervenant, Karla, la directrice des normes au GLEIF, la fondation des identifiants des entités juridiques mondiales. C'est une de mes entités préférées, j'en parle souvent pour ceux qui me connaissent bien. Je laisse la parole à Karla qui va parler du GLEIF, ce qu'il fait et comment cela pourrait constituer une feuille de route de ce que nous voulons faire au sein de la communauté, ici.

KARLA MCKENNA: Merci. C'est un plaisir d'être ici, je peux enfin vous présenter ces sujets. Prochaine diapo.

Juste pour confirmer l'ordre du jour, je vais d'abord faire un aperçu du système LEI mondial, je vais revenir sur certains points forts de l'histoire, certains qui remontent à la crise financière de 2008 et ensuite je vais vous expliquer comment le LEI forme le fondement de la stratégie numérique sur laquelle travaille le LEI depuis plusieurs années.

Le système global LEI avait été préparé après la crise financière pour pouvoir créer un système d'identificateur au niveau mondial pour tout ce qui est transaction financière. Et ce système pourrait identifier les institutions financières et aussi pourraient être assigné à un environnement plus large, une liste plus large d'entité sur le terrain au niveau international. Toutes les entités qui participent à des transactions financières.

Donc les entités juridiques, donc la fondation a donc été mise en œuvre après l'appel du G20 et cela a été lié à la crise financière pour pouvoir

aider les régulateurs et les entreprises du service public pour mieux comprendre quelles étaient les entités responsables pour les rôles différents dans les transactions financières, les entités responsables pour la transparence, etc.

Nous avons été créés sous une certaine règlementation. Vous voyez le comité de supervision au niveau de la règlementation, voilà le GLIEF est donc l'opérateur du système LEI au niveau mondial. Nous avons aussi des partenaires, il y a un réseau de partenaires qui valident les entités juridiques. Et ces informations de validation sont envoyées à GLIEF et sont publiées sans restriction et sans aucune licence ou accord vis-à-vis des utilisateurs. C'est pour cela que nous appelons cela un système mondial.

Prochaine diapositive, un peu plus sur GLIEF.

Nous avons un conseil d'administration, nous sommes une fondation suisse à but non lucratif, nous avons plus de 2 millions de LEI qui ont été publiés jusqu'à présent.

Prochaine diapo.

Il est important de savoir que l'identificateur des entités juridiques est sous ISO, nous avons pu être capables de communiquer à travers les frontières. Et, dans certains cas même lors de la même juridiction au sein des mêmes agences. À l'époque rien n'existait au niveau international, c'est là que je me suis impliquée avec ce qui est devenu le GLIEF parce que je faisais partie du groupe ISO et nous avons mis en place le groupe LEI et ces standards ont été mis en œuvre par ISO.

Prochaine diapo.

Voilà les partenaires qui ont été obtenus dans le système mondial qui valide le système des entités juridiques et qui vérifie les informations, cela permet à GLIEF de pouvoir avoir une bonne empreinte, une bonne base LEI pour pouvoir, encore une fois, réfléchir sur les manières de rendre le système LEI plus utile. Donc, en fait, nous avons un code qui est axé sur un ensemble de références, de standards. Et nous avons commencé à réfléchir sur les manières dont nous pourrions agir pour pouvoir rendre les choses plus pertinentes au niveau numérique, avec une perspective plus numérique.

Prochaine diapo.

Nous avions pensé que ce que nous avions était une bonne base pour fournir les LEI vérifiables. Et alors, ce que nous offrions vraiment était la possibilité de l'identité organisationnelle, donc l'habilité pour une personne ou une chose de pouvoir prouver qu'ils avaient l'autorité de représenter une organisation, représentée par le LEI, soit en externe soit en interne. Certaines organisations sont très importantes et larges et tout le monde ne se connait pas forcément donc il fallait qu'il y ait un rôle d'autorité. Donc on a commencé sur ce parcours pour pouvoir créer un LEI vérifiable. Et nous avons créé des points de références pour les entités pour qu'il y ait une certaine manière de vérifier les données.

Prochaine diapo.

Donc ce que nous offrons vraiment c'est un ensemble de données pour vérifier les LEI, c'est une architecture que nous utilisons, nous utilisons

les points de référence organisationnels. Nous voulons aussi soutenir le mouvement pour pouvoir modifier les comportements des utilisateurs qui reçoivent des documents, des dossiers et autres matériels ou données d'informations ou même lorsque ces personnes s'impliquent dans des transactions financières et font des transactions entre entreprises ou entre consommateurs. Nous voulions faire partie de ce mouvement pour pouvoir offrir des caractéristiques, des signatures multiples pour faire ces vérifications. Et aussi utiliser des clefs crypto pour pouvoir assurer la sécurité du LEI

Nous voulions donc protéger les entités.

La prochaine diapo décrit des références. Prochaine diapo. Excusez-moi, j'oublie que j'avais une diapo entre les deux.

Ce que nous avons créé ici c'est la capacité pour une organisation de personnes qui publie justement le LEI de pouvoir mettre en place un programme pour pouvoir fournir à l'organisation des références au niveau du LEI. Et donc nous appelons cela des références de rôle. Il s'agit là d'informations sur l'organisation, sur les personnes et sur le rôle qu'ils ont au sein de l'organisation.

Donc nous avons rassemblé le monde réel et le monde virtuel et ainsi nous pouvons identifier les personnes en utilisant des éléments d'identification et nous pouvons ainsi aussi identifier le rôle de cette personne.

Nous avons fait cela de deux manières. Nous avons essayé de comprendre comment nous pourrions faire cela pour quelqu'un qui a

un rôle d'administration, un administrateur ou à la suite de recherches que nous avons faites avec des personnes de l'industrie, dans le même secteur. Nous avons vu que nous pouvions utiliser ce genre de qualification pour pouvoir soutenir des rôles fonctionnels ou pour définir certains rôles pour pouvoir donner une certaine valeur à ce programme.

Prochaine diapo.

Nous allons vous faire passer par la chaine de confiance que nous avons établie. Nous représentons la fondation, la base de la confiance, ces qualifications ou ces identifications changent, il y a de nouvelles technologies ou protocoles que nous utilisons pour créer une chaine de confiance, pas seulement en utilisant ces identifiants, mais avec des identifications cryptographiques.

Le GLIEF nous permet de qualifier ces personnes qui publient les données LEI et ainsi nous pouvons rallier toutes les organisations en utilisant ces identifiants de la part et pour nos clients. Et nous pouvons aussi utiliser tous les identifiants, les qualifications pour les différents rôles et nous travaillons pour les organisations qui publient tous ces LEI.

Cette chaine de vérification est sur un principe de confiance, cela nous permet d'identifier ou de vérifier les qualifications ou les identifications et nous pouvons ainsi comprendre que ces personnes sont enregistrées dans ce système.

Pour utiliser le LEI j'ai essayé de donner quelques exemples sur la manière dont la vérification de l'identité puisse être utilisée dans le

secteur des entreprises. Nous voyons des entreprises qui voulaient du soutien au niveau des ressources humaines, quand il s'agissait de l'on-boarding non seulement des employés, mais des clients. Nous avons la signature et la soumission des rapports, de certains formulaires, de formulaires spécifiques, ils voulaient pouvoir signer des documents.

Nous voulions aussi utiliser cette opportunité pour donner l'accès au service du secteur public pour pouvoir utiliser ces LEI.

J'ai donné deux exemples, voilà la prochaine diapositive.

Donc un cas d'utilisation dont je voulais vous parler c'est la signature numérique, c'est un projet sur lequel nous travaillons activement en ce moment. Cette utilisation de la signature numérique est importante pour toutes les soumissions volontaires ou non. On commence par toutes les entités qui soumettent des rapports, qui déposent des dossiers avec les autorités de règlementation, les entités qui reçoivent ces documents peuvent vérifier la signature et ensuite peuvent ainsi vérifier que les organisations qui reçoivent les LEI est bien l'organisation ou la personne dont ils attendaient une réponse.

C'est un petit peu un système de vérification à l'arrivée et à la réception.

Nous avons aussi sur la prochaine diapositive un pilote, un projet sur lequel nous travaillons. Il s'agit des autorités bancaires d'Europe, il s'agit là du secteur privé. Là nous avons la participation de 17 banques, il y a un document qui a été publié récemment. Nous attendons une rétroaction d'ici fin mars après la conclusion de ce projet pilote. La décision sera annoncée à savoir si le système sera utilisé ou non. Et

ensuite le système sera mis en œuvre pour un total de 600 banques qui vont faire un rapport direct au EBA. Et l'EBA reçoit maintenant des rapports de toutes ces entités. Donc il y aura une méthode de vérification et cela couvrira l'authentification, la vérification de tous les utilisateurs qui fournissent des documents à l'EBA.

Il reste une diapositive avant que j'en termine avec cette présentation. Nous voulions aussi parler de notre système d'infrastructure VLEI qui est gouverné par un cadre de travail de gouvernance de 24 documents qui ont été publiés en totalité. Cela couvre tout sur la publication, la révocation de qualification, les révocations des clefs, les exigences pour les personnes qui publient ces VLEI. Et donc tout ce qui qualifie les utilisateurs VLEI et tout ce qui est des exigences gouvernementales nécessaires pour les utilisateurs.

Nous voulons proposer, donc, ce logiciel à tous les fournisseurs qui veulent utiliser ce VLEI.

MICKAËL PALAGE: Merci. S'il y a des questions, nous y répondrons tout à l'heure. En attendant, je voudrais passer à la prochaine présentatrice, Avri Doria, qui est une amie de beaucoup de personnes au sein de la communauté. Nous allons mettre à l'écran les diapositives de Avri.

AVRI DORIA: Merci, Michael, et merci pour cette présentation. En fait, je vais essayer de parler de pourquoi il est si difficile de trouver un espace de solution

pour vérifier les identités ? Et je reviens vers ICANN, quelle est notre responsabilité par rapport à cette confiance d'un système multipartite ?

Pendant des années, nous avons parlé de la vérification des identités et nous avons parlé du RDAP, de SSAC, etc., et dans la plupart des discussions nous avions décidé que le problème était beaucoup trop compliqué, nous avons eu des difficultés à arriver à un consensus surtout lorsqu'il s'agissait d'élaboration de nos politiques, nous n'avions pas une très bonne vision de la protection des données et de la responsabilité par rapport à la confidentialité, l'accès et la sécurité des informations. Et c'est pour cela que nous parlions d'opérateurs individuels, d'organisations. Et nous parlions de toute sorte d'autorisations.

Donc nous devons continuer à travailler sur ces questions de consensus et nous devons développer des compétences et évaluer l'impact que nous avons sur la vie des êtres humains. Et, surtout, nous ne croyions pas qu'il y avait une architecture ou un ensemble de protocoles qui pourrait être utilisé pour faire le travail, c'était compliqué, de façon collective nous ne croyions pas qu'il y avait une solution technique. Et la plupart d'entre nous disaient : nous ne voyons pas une solution. Nous ne pouvions pas résoudre un problème et dans ce cas cela ne nous arrangeait pas au niveau de la confiance. C'est pour cela qu'il nous fait absolument examiner cela afin de trouver une solution, car c'est vraiment un problème.

Donc, plus tôt aujourd'hui, j'ai écouté une discussion sur le nombre de bureaux d'enregistrement et ils trouvaient que ce problème était

beaucoup trop compliqué et ils avaient trouvé des solutions, mais qui n'étaient pas atteignables.

Donc je pense que 100 % du problème, résoudre un problème avec très peu d'outils n'était pas possible.

Est-ce qu'on peut utiliser une combinaison d'outils politiques pour pouvoir résoudre des problèmes ? Est-ce qu'il y a un rôle au sein de l'ICANN pour aider et pour coopérer pour faire le travail nécessaire pour trouver une solution ?

Alors que la disponibilité des protocoles et des architectures semble poser un problème vis-à-vis de cette question, il nous faudrait examiner ces protocoles, peut-être commencer à parler avec des experts. Nous avons aussi une galaxie de solutions numériques.

Alors j'ai commencé à examiner cela et j'ai vu qu'il y avait beaucoup de protocoles et il y a une richesse de choix. Il y a des protocoles pour les signatures électroniques, pour toute sorte d'authentification et il y a des cadres de travail, des cadres de confiance, de vérification de cadres de confiance, des tas de solutions. Il y a beaucoup de systèmes dans cette galaxie.

Mais il n'y a pas un seul outil qui nous permettait de résoudre le problème de manière générale. Et donc j'ai assisté à une présentation durant la journée, j'ai vu beaucoup de ccTL et autres entités qui utilisaient une combinaison d'outils pour construire des systèmes qui fonctionnaient.

Je recommande cette séance, si vous n'avez pas participé vous pouvez la réécouter. Il y a des carences.

Donc j'ai étudié plusieurs solutions, les mises à l'échelle, et nous devons examiner la galaxie de solutions numériques. Et il semble qu'il y aurait peut-être un outil pour chaque solution ou chaque problème.

Par exemple, j'ai écouté ce qui a été discuté à l'IETF, il y a un groupe de travail qui voulait travailler sur la combinaison d'outils qui ont été utilisés il y a plusieurs années.

J'ai commencé à recueillir des informations.

Prochaine diapo.

J'ai commencé à recueillir des informations sur plusieurs protocoles qui se trouvent dans cette galaxie et j'ai essayé de comprendre les protocoles utilisés et pour quels buts pour mieux comprendre les utilités pour la protection des données. J'ai fait un tableau qui pourra être complété.

J'ai commencé par penser à une solution technique, je sais qu'il y a beaucoup de travail qui doit être fait, mais je pense qu'une solution technique peut être possible.

Nous allons parler en plus de détail de tout cela aujourd'hui et nous allons pouvoir adresser ces inquiétudes de protection de données et ces protections des droits de l'homme.

MICKAËL PALAGE: Merci. Nous allons passer au prochain panel de cette séance, nous allons faire un tour de table et nous allons faire des présentations de deux ou trois minutes par nombre d'opérateurs TLD qui ont des systèmes de vérification et de protocoles numériques à différents niveaux. Nous allons parler tout d'abord à Lucas qui est ingénieur télécommunication à l'OFCOM. Il va nous parler du gTLD .SWISS.

LUCAS PRÊTRE: Bonjour, merci de me donner la possibilité de faire cette présentation devant votre communauté. Nous allons parler de ce que nous faisons à .SWISS gTLD, pour ce qui est de la vérification des titulaires de noms de domaine.

Alors .SWISS est alloué à des entités spécifiques basées en Suisse. En général ce sont ceux qui sont dans le registre du commerce en Suisse, mais il y a certaines exceptions.

Les critères sont définis dans l'ordre des noms de domaine, ce qu'on appelle l'OID. Les candidatures contiennent ce que l'on appelle un UID, donc un numéro d'identification des entreprises. Ce numéro nous permet de faire des demandes à une base nationale de données pour obtenir des informations. Donc nous avons soit trouvé, soit non trouvé.

Quand les informations n'ont pas été trouvées, cela veut dire que l'UID a été mal composé ou écrit ou que les données ou le dossier n'existe pas. Et dans ce cas la candidature est rejetée avec le code approprié.

Si les informations sont trouvées, nous recevons les détails liés à l'entité et un formulaire juridique qui nous permet de pouvoir remplir un outil d'évaluation qui est développé pour, justement, .SWISS.

Donc cet outil nous permet de vraiment définir toutes ces données liées à l'entreprise du titulaire de domaine en question. Alors certains de ces formulaires juridiques sont spécifiques à la Suisse et ces entités ne sont pas obligées de faire partie du registre du commerce suisse, mais l'enregistrement est obligatoire pour savoir s'ils sont éligibles.

Le résultat est une décision positive, la décision doit être prise et lorsque les informations sont reçues et sont éligibles nous évaluons la relation entre le nom de domaine demandé et le candidat. Et savoir ce que ce candidat va faire avec ce nom de domaine.

Prochaine diapo s'il vous plait.

Nous avons 4 types de relation, c'est donc une marque déposée au niveau du registre suisse, c'est un nom basé sur le nom de l'entreprise, ça peut être une reconnaissance générale, ça peut correspondre à un produit ou un projet de l'entreprise. Sinon, il y a un rejet de la candidature et nous considérons cela pour deux raisons : pas de lien ou de relation ou c'est un terme générique. Donc cela cause aussi un rejet de la part du système.

Comme vous l'avez vu auparavant nous avons une modification au niveau de cette éligibilité qui a eu lieu le 24 avril 2024. Nous avons ouvert le gTLD .SWISS aux personnes légales, donc nous avons ce code que

nous utilisons pour une utilisation. Il s'agit d'un chiffre qui correspond au numéro de sécurité sociale en suisse.

Je pense ne plus avoir de temps, je suis désolé.

Si vous voulez avoir plus d'informations sur RDAP, je peux faire cela brièvement.

MICKAËL PALAGE: Oui, si vous pouviez le faire en 30 secondes, ce serait bien.

LUCAS PRÊTRE: Prochaine diapo. Notre partenaire technique fait une recherche RDAP sur le nom de domaine, c'est l'UID. L'UID n'est pas publié, mais si on ne peut pas le voir… Passez à la prochaine diapo. Cela dépend du client, vous pouvez voir cette identification ici, c'est une identification publique qui se trouve dans la base de données. Merci.

MICKAËL PALAGE: Les diapositives sont en ligne, je vous encourage à aller voir. Pour faire plus vite, nous allons passer à notre prochaine intervenante, Niamh, experte en politique et santé numérique séniore à l'association nationale des conseils administratifs pharmaceutiques, NADP. Vous êtes là ?

NIAMH LEWIS: Oui. Je vais faire vite parce que je suis dans une autre conférence en ce moment, donc peut-être je vais durer moins de 4 minutes.

Alors le NBAP s'occupe des TLD .PHARMACIE, je vais vous raconter comment ça se passe. Nous avons 120 ans, il s'agit ici d'une organisation à but non lucratif qui siège aux États-Unis, les membres sont les 50 régulateurs étatiques des États aux États-Unis de la pratique de la pharmacologie ainsi que des autres régulateurs de la pharmacologie des territoires américains et des provinces canadiennes.

Donc on NABP est là depuis longtemps, .PHARMACIE est une partie de notre activité, nous sommes axés sur les missions. Notre objectif est de protéger la santé publique et nous comptons plus de 180 employés, plus de 10 pharmaciens permanents plus les contractuels, les professionnels de la règlementation, beaucoup d'avocats, y compris moi-même.

Nous avons beaucoup de programmes conçus pour protéger la santé publique. Et le gros de notre activité est que chaque pharmacien habilité aux États-Unis est accrédité, nous avons plusieurs programmes d'accréditations, des inspections et nous faisons des transferts de permis ou de qualification quand on passe d'un État à un autre aux États-Unis.

Prochaine diapo ;

Qu'en est-il de .PHARMACIE, ce TLD de premier niveau est disponible pour les vendeurs de services de santé ou les fournisseurs qui ont reçu l'accréditation de fournisseur de service de santé NABP. Pour le moment il n'y a qu'une accréditation, celle de fournisseur de service de santé et ce TLD est aussi disponible pour les régulateurs de pharmacie. Cette accréditation fournisseur santé est un programme mondial, il faut qu'ils satisfassent à nos critères d'éligibilité et doivent satisfaire nos 10 règles

du programme, par exemple est-ce que vous avez obtenu votre permis en règle ? Est-ce que vous respectez les lois ? Où sont vos patients et est-ce que vous respectez les données de vie privée ?

Ensuite, quand on examine des demandes aux États-Unis et en dehors nous collaborons avec des régulateurs, la Santé Canada, HRA au Royaume-Uni, NAPRA c'est un peu comme NEBP, mais au Canada. Les examinateurs sont entre autres des avocats, des pharmaciens ou les deux.

Comment les gens utilisent ce TLD .PHARMACIE ? Il y a des tiers qui l'utilisent. Comme Mickael l'a dit, cela peut intéresser plusieurs personnes. En deux mots, cela sert un peu de barrière anti-fraude. Il y en a beaucoup, mais beaucoup ne sont pas accréditées par les organismes et organisations affichées sur leur site web. Et le TLD, en fait, c'est vraiment infaillible. Il y a des parties prenantes tierces qui demandent certaines accréditations, la nôtre en est une, il y en a d'autres, mais si vous voulez faire de la pub sur des plateformes en ligne, Visa et Mastercard reconnaissent notre accréditation, ils ont leur liste d'exigences sur ce qu'ils appellent les pharmacies sans cartes, en fait il s'agit de pharmacies qui font des transactions sans le passage de la carte dans la machine, donc c'est à fort risque, donc ils exigent davantage d'accréditation.

À l'heure actuelle, il y a 600 noms de domaine .PHARMACIE qui sont enregistrés.

MICKAËL PALAGE: Très bien, nous sommes dans les temps, je vous laisse retourner à l'autre conférence.

Passons maintenant à Craig, directeur-gérant des services de registre fTLD. Allez-y.

CRAIG SCHWARTZ: Très bien. Merci de me donner la possibilité de parler de .BANK et .ASSURANCE.

Il s'agit ici des distributeurs et producteurs dans l'assurance, les associations commerciales et les régulateurs. À cause de ces régulations, le bassin des titulaires de nom de domaine est assez réduit. Et, vous savez, il y a plusieurs façons de mesurer le succès. Comme on l'a dit 70 % des banques aux États-Unis utilisent le .BANK pour présenter aux clients. Donc nous sommes très fiers.

Et pour ce qui est de ce que Karla a dit sur les LEI, identificateurs de personnes juridiques, 80 % des titulaires aux États-Unis ont déjà ces identifiants, donc nous essayons de mettre cela dans notre processus de vérification.

Nous sommes un des rares gTLD qui mène toujours des vérifications de TLD, je vais en parler dans une minute, ce qui nous distingue aussi et donne plus de sécurité c'est que nous demandons plus de technologie et protocoles pour des domaines dans notre zone. Par exemple DNSSEC, un bon chiffrement HSBS, et en plus nous faisons un suivi quotidien du respect de ces règles.

Et je suis ravi de rapporter qu'en 10 ans d'activé nous n'avons eu que 18 rapports de fraude. Et, finalement, c'était des fausses alertes. Donc tout est solide depuis le premier jour.

Outre les exigences de sécurité pour les domaines de deuxième niveau, nous veillons aussi à la hiérarchie pour les TLD, donc en 2018 nous sommes devenus le premier TLD hors Google à être ajouté à la liste d'excellence. Donc si vous avez le certificat près-DLS vous êtes considéré comme ayant une connexion HTTPS. Et au cours des 5 dernières années, y compris le processus RTFC nous avons mis en œuvre ce qu'on appelle les domaines publics des marques qui rajoute une couche de protection des hameçonnages pour les domaines non existants. Et si cela vous intéresse, vous pouvez aussi venir me parler sans problème.

Prochaine diapo.

Nous avons toujours eu un registre qui nous permet, manuellement, d'approuver tout enregistrement pour que les données d'enregistrement correspondent à ce que nous avons vérifié et nous faisons en sorte que rien ne soit passé inaperçu. Et pour la vérification nous utilisons surtout des bases de données régulatoires publiques quand on confirme par exemple l'éligibilité d'une organisation, l'éligibilité pour la sélection d'un nom, l'adresse email, est-ce qu'il figure sur des listes noires, les listes du trésor américain.

Et nous veillons aussi à ce que le contact du titulaire ait l'autorité de l'organisation pour s'enregistrer et maintenir le nom. La vérification se

fait avant l'enregistrement initial, une fois par an et quand il y a des changements de données.

Avant, on sous-traitait à Symantec, c'était très difficile pour les bureaux d'enregistrement et les opérateurs de registre. En 2017 on a décidé de créer le DRV, la vérification dynamique pour rapatrier cela, ce qu'on a fait avec réussite déjà depuis 5 ans.

C'est encore manuel, mais ça vaut quand même l'inconfort pour renforcer la confiance dans les TLD.

Pour finir, la prochaine version va être de plus en plus automatisée, il va peut-être être possible d'inclure les LEI et l'IA si c'est possible.

MICKAËL PALAGE: Merci, Craig. Et si je peux faire un suivi aussi, Alan Greenberg nous demande quel est le coût de ces LEI, combien ça coûte par an ?

CRAIG SCHWARTZ: Je crois qu'on a payé 60 ou 80 USD pour cet identificateur de personnes juridique.

MICKAËL PALAGE: Très bien. Je me tourne maintenant vers notre prochain intervenant, Thomas, membre du conseil d'administration de DENIC.

THOMAS KELLER : Merci de me donner le temps de parler de ce que nous faisons, alors que nous sommes assujettis au DNS2, ce qui entrera en vigueur cette année. Quelques mots au sujet de DENIC, association à but non lucratif à Frankfort en Allemagne, et nous sommes une entreprise auto-financée. Nous avons fait beaucoup d'efforts pour décider ce que nous allons faire.

Je peux vous montrer notre pensée. Nous sommes détenus par nos propres membres. Nous attendons avant de faire toute mise en œuvre. Nous ne savons pas encore si ce sera une bonne idée, mais je peux vous montrer comment nous raisonnons.

Prochaine diapo.

DENIC compte presque 18 millions d'enregistrements, ce qui fait de nous le deuxième plus grand TLD, nous avons 290 membres et une des faibles utilisations mauvaises dans le monde. L'opération, comme vous le voyez, est de grande ampleur. Il faut faire attention. À chaque pas nous avons beaucoup d'enregistrements déjà là. Nous ne partons pas de peu, mais c'est quand même très compliqué pour nous.

Prochaine diapo.

Quand on a composé le groupe pour décider de la suite, tout d'abord on s'est donné quelques principes. Les principes doivent être tournés vers l'avenir, il ne faut pas avoir un processus qui coince ou qui doit être changé pour repartir de zéro, il faut que ce soit amplifiable et flexible et cela doit être une approche basée sur les risques. Ce qui veut dire que nous effectuons des vérifications obligatoires quand vous transférez ou

mettez à jour des noms de domaine et nous vérifions aussi les domaines sur une base de plaintes. Donc si quelque chose cloche nous repartons du début.

Ensuite nous vérifions avant et après. Une idée, je ne sais pas si cela a été concrétisé finalement, mais la vérification peut être utilisée une nouvelle fois même pour les autres TLD. Ça, c'est un des concepts que nous essayons de mettre en place, on va voir si cela peut se matérialiser.

Prochaine diapo.

Qu'allons-nous vérifier ? Rapidement, le nom et l'adresse, l'email et le numéro de téléphone.

Prochaine diapo.

Le processus que nous allons mettre en œuvre est que si une requête arrive, ça peut être un nouvel enregistrement, une plainte ou peu importe, nous faisons des vérifications pour voir si c'est complet, ensuite ça peut être rejeté ou accepté, c'est la phase de vérification et d'évaluation des risques. Il y a un peu de magie et d'IA, nous avons toutes les données du titulaire de l'enregistrement, et on se dit : est-ce qu'il y a quelque chose qui cloche, quelque chose qui devrait nous dissuader ? Dans ce cas-là nous aboutissons à une identification de haut risque, nous décidons de ne pas déléguer et il faut que ce soit vérifié autrement. Quand c'est un risque élevé, le domaine est délégué et la vérification est exigée, il y a une date butoir de 2 semaines. Quand c'est un risque faible, la délégation est faite et il n'y a aucune vérification nécessaire.

Prochaine diapo.

Qui s'occupe de la vérification ? Le débat était long. On s'est demandé si c'était nous, on est allé voir les opérateurs de registre qui nous ont dit que les opérateurs de registre étaient tenus contractuellement de faire cette vérification et qu'ils offrent tout un éventail de vérifications permises, ça peut être la vérification de la pièce d'identité, la photo, les processus, ils peuvent regarder les données enregistrées. Et nous faisons beaucoup de nouveaux essais avec les choses qui fonctionnent et ce qui fonctionne un peu moins.

Merci de m'avoir donné ces quelques minutes.

MICKAËL PALAGE: Merci. Merci pour ce travail de sensibilisation et l'engagement auprès des opérateurs de registre pour trouver une solution d'avenir. Maintenant nous avons le docteur Bruce Tonkin, responsable de .AU.

BRUCE TONKIN : Merci. Prochaine page s'il vous plait. Celle d'après. Voilà.

Voilà les exigences pour .AU. Il faut tout d'abord que le titulaire ait une présence en Australie, donc citoyen ou résident permanent ou ayant une entreprise. Ça peut être une entreprise étrangère, mais il faut avoir une marque déposée australienne. En plus nous avons aussi les noms de base comme .AU direct, par exemple .AU, à ce moment il faudrait une présence australienne. Pour .COM. AU il faut être une personne commerciale enregistrée pour faire des affaires en Australie parce que

nous avons un système d'impôts assez volumineux, il faut un numéro d'impôt, un numéro de TVA et être enregistré auprès du gouvernement pour faire des affaires.

Pour le gouvernement nous avons une organisation séparée qui enregistre les organisations non lucratives et ensuite nous avons les établissements éducatifs et les fournisseurs du gouvernement. Tout cela est appuyé sur des bases de données gouvernementales que nous pouvons vérifier.

Prochaine diapositive.

Les opérateurs de registre doivent valider les informations et les confronter aux bases de données. Encore une fois nous ne vérifions pas ici. C'est là qu'il y a une nuance. On parlait d'identifiants vérifiés avec la couche de mots de passe, etc., pour identifier, nous en fait, nous recueillons l'information, nous la confrontons aux bases de données gouvernementales, nous montrons que les entités ou les personnes existent et cela suffit pour l'enregistrement.

Et ce qu'il faut voir c'est que le nom, l'adresse et l'identifiant sont réels et la plupart des opérateurs en Australie utilisent le registre du gouvernement. C'est gratuit, c'est un service très fiable, vous pouvez le chercher par nom, par nom d'entreprise ou par numéro d'identifiant, ça représente le dossier avec des informations structurées et vous confrontez cela à ce qu'a présenté le titulaire et vous pouvez lancer le nom de domaine.

L'autre service, si vous n'avez pas d'un identifiant pour votre entreprise, si vous êtes un citoyen, c'est un grand pourcentage des titulaires, ils peuvent mettre leur carte d'identité comme un permis de conduire ou un passeport, le gouvernement a un service pour valider l'information. Le seul problème est que cela coûte un certain montant en dollar par vérification. Donc le problème est que si un utilisateur tape des informations, par exemple du permis de conduire, il faut mettre le deuxième prénom, ce qui ne correspond pas à un autre dossier ou parfois il y a deux nombres sur le permis de conduire, le numéro du permis et le numéro d'enregistrement du permis et cela aussi peut causer quelques petites pannes et quelques incohérences, donc refaire le dossier coûte un certain montant à chaque fois, ce qui est assez contrariant pour certains utilisateurs c'est un problème qui pousse certains opérateurs à se défaire de ce système.

La clef ici est que même si les titulaires peuvent utiliser un passeport ou un permis de conduire pour enregistrer leur nom il n'y a pas d'exigence pour l'opérateur de registre de garder les informations, ils valident juste l'information auprès du gouvernement, ils enregistrent le oui ou le non avec la date et l'heure, mais l'idée est de ne pas garder l'information attachée à la personne comme le numéro du permis de conduire.

Le résultat de ce système est que nous n'avons que très peu d'enregistrements malveillants, pour des fins criminelles, et quand c'est le cas, ce sont des entités volées. Donc vous pouvez avoir le meilleur système du monde, mais si l'identité est volée, si vous trouvez un permis de conduire, ça va valider l'information. Même chose si vous trouvez une carte de crédit par terre vous pouvez acheter un café.

Mais ce qu'on voit ici, bien que nous n'ayons pas beaucoup d'enregistrements malveillants nous avons beaucoup d'utilisations malveillantes du DNS, ce sont des sites web compromis, ça n'a rien à voir avec les enregistrements. Mais c'est juste que les organisations ne surveillent pas et n'entretiennent pas bien leur site web et ils se font hameçonner.

Voilà, c'est tout de ma part.

MICKAËL PALAGE: Merci, Bruce. Je passe la parole à un bon ami à moi, boursier technique de CZ.NIC.

JAROMIR TALIR: Le .CZ est un de ces bureaux d'enregistrement qui procède à des vérifications des titulaires de domaine depuis longtemps.

Cette panique mondiale à propos du NIS, nous avons déjà prévu, nous commençons avec la réception des plaintes au niveau des données qui sont incorrectes et nous attendons et nous demandons de plus amples informations. Lorsque nous ne recevons pas de réponse, nous retirons le nom de domaine.

Bien sûr nous ne pouvons pas toujours vérifier les données donc nous avons décidé d'essayer de convaincre les personnes de valider leurs données de façon volontaire.

En fait, il est possible de vérifier à un niveau où vous pouvez rallier les données de contact avec les données déjà existantes, si la personne a

déménagé ou s'il y a un changement de nom. Ce service est reconnu par le gouvernement et une notification est envoyée et nous suivons les exigences de l'EIDAS. Donc cela nous permet de vérifier les titulaires de noms de domaine d'autres pays qui, en 2019, ont commencé à tirer profit de notre raison. Donc ainsi nous avons enregistré et lié toutes les données pour pouvoir faire nos vérifications.

L'année dernière nous avons refait notre système de vérification, nous avons mis en œuvre un portail de services automatiques et donc il y a des méthodes que l'on peut sélectionner pour vérifier son identité.

Alors ce que nous planifions de faire, dans l'avenir, nous voulons intégrer avec tous les registres qui sont en ligne par rapport au registre des adresses physiques, par rapport au registre du commerce, nous pensons aussi utiliser GLIEF pour la vérification des organisations et entités légales et nous allons aussi utiliser le système d'identité numérique européen et de cette manière nous voulons explorer différentes manières pour faire les vérifications du titulaire de nom de domaine et pour d'autres éléments.

Et nous continuons à examiner les problèmes liés aux personnes qui n'ont pas d'identification, nous essayons de trouver des façons de le faire, d'obtenir le soutien du gouvernement pour cela. Il y a aussi des vérifications telles que des exigences obligatoires ou volontaires. Nous essayons d'étudier ces différentes fonctionnalités. Nous voulons peut-être essayer d'obtenir ou de fournir des certificats d'authentification ou de propriété de noms de domaine. Merci.

MICKAËL PALAGE: Merci. Nous allons passer la parole à Timo qui est responsable du développement à .EE.

TIMO VOHMA: Nous sommes une fondation privée à but non lucratif, nous gérons le .EE. Nous avons toujours travaillé sur la vérification de l'identité, nous utilisons les modèles bureaux d'enregistrement, opérateurs de registre. Nous avons des manières de vérifier les contacts de nos titulaires.

Nous avons dû faire face à plusieurs défis. Ce n'est pas seulement un problème en Estonie, car nous avons une structure de vérification d'identification assez robuste. Nous voulons donner la possibilité aux opérateurs de registre de vérifier le contenu. Nous avons utilisé ce que j'appelle l'identification bancaire de l'homme des cavernes, c'est comme ça que je l'appelle. Nous avons les détails qui nous sont envoyés pour chaque candidature et nous avons un système d'authentification. Mais le système est assez onéreux, surtout pour les entités qui nous viennent d'autres pays que l'Union Européenne.

Prochaine diapo.

Maintenant, nous avons une autre solution pour ce problème, nous appelons ça IEID, c'est mieux que ID. C'est une manière d'utiliser les solutions qui nous sont fournies par le gouvernement estonien ou d'autres gouvernements. Nous utilisons des solutions du secteur privé, de banque ID par exemple, ainsi les opérateurs de registre n'ont pas à intégrer ces solutions directement et cela économise beaucoup de

temps et beaucoup de problèmes de gestion, de contacts et d'information de contact.

Donc lorsque les contacts n'ont pas accès à une identification nous fournissons une identité. Nous utilisons un système d'identification, nous avons collaboré avec un fournisseur de service. Il y a beaucoup de ces fournisseurs de service autour du monde qui fournissent ce service. Leur clientèle souvent sont des banques ou des institutions financières. Donc ils savent ce qu'ils font et ils sont très doués.

Donc, nous utilisons des standards ouverts qui s'appellent Identification FIDO, Feed Alliance vérifie ces standards, ils travaillent avec Visa, Mastercard, etc. Si vous n'avez pas entendu parler de FIDO, sachez que c'est la solution pour ce qui est de l'authentification pour les titulaires. Ils sont dirigés vers cette plateforme pour se faire identifier en utilisant cette identité, ils peuvent s'auto-identifier vis-à-vis des opérateurs de registre pour enregistrer leur nom. C'est facile et c'est un système assez facile.

Je sais que je n'ai plus beaucoup de temps. Donc je pense que nous avons trouvé une solution assez simple lorsqu'il s'agit des problèmes d'identification et maintenant nous focalisons sur le fait que nous voulons que ce système soit accessible à tous. Si ce sujet vous intéresse, n'hésitez pas à me contacter, vous avez les liens à l'écran et les adresses mail.

MICKAËL PALAGE: Merci. J'encourage tout le monde à aller revoir la présentation faite par Timo durant la journée de technologie. Maintenant nous allons passer à Jacques, chef de la technologie à CIRA.

JACQUES LATOUR: Je vais parler du processus de vérification à .CA. Maintenant, le processus que nous utilisons pour vérifier les informations du titulaire est basé sur le défi de la présence canadienne. Vous devez être canadien pour ce faire.

Maintenant, s'il y a un rapport d'utilisation malveillante d'un domaine, nous demandons au titulaire de données de nous donner une copie numérique de leur preuve de citoyenneté, soit un passeport, un permis de conduire ou un certificat de naissance. Ils téléchargent la copie de la pièce et nous examinons ces données et nous nous en débarrassons après la vérification, car nous ne voulons pas garder ces informations.

Ensuite il n'y a pas un être humain qui peut détecter la fraude avec tout ce qui se passe dans le monde, il est très difficile de faire cela. Donc si les documents ne sont pas signés, nous ne pouvons pas les utiliser.

Prochaine diapo.

Ce que nous recherchons ce sont des titres justificatifs qui soient numériques, donc des passeports ou certificats de naissance authentifiés. Nous demandons aux titulaires d'utiliser le portail pour nous envoyer ces justificatifs. Par exemple, dans la Colombie-Britannique les personnes doivent utiliser un document qui est émis par le gouvernement et qui est signé et nous pouvons identifier la signature

à travers ce système. Le but est de demander aux titulaires d'envoyer à ce portail que nous utilisons le document. Mais en fait c'est la preuve qu'ils sont canadiens. Ils peuvent ainsi dire : je suis canadien et ce document est signé par l'entité qui l'a émis. Cette information peut donc être vérifiée.

Donc nous pouvons, par ce fait, préserver la vie privée du titulaire.

Maintenant, nous avons les justificatifs numériques, nous savons que le document est signé par cette entité. Mais comment nous faisons confiance, est-ce que le document a été signé par une entité de confiance ?

Nous avons parlé de la confiance numérique lors d'un panel aujourd'hui et en fait, ce que nous essayons de faire c'est de mettre en œuvre un registre de confiance, une infrastructure avec ces registres de confiance pour pouvoir vérifier que ces personnes sont ceux qu'ils prétendent être et qu'ils nous ont fourni les justificatifs qui sont réels. Donc, quand nous avons ces justificatifs signés et reconnus et émis par des entités autorisées à émettre ce genre de justificatifs, nous pouvons ainsi vérifier, identifier, authentifier ce document.

Voilà, c'est tout pour moi.

MICKAËL PALAGE: Nous sommes à l'heure, c'est la fin de cette session, si je pouvais demander à nos collègues d'ICANN Org de dépasser un peu pour que nous puissions répondre aux questions venant de l'audience ?

MICHELLE DESMYTER: Vous avez 5 minutes.

MICKAËL PALAGE: Y a-t-il des questions en ligne ou dans la salle ? Si vous avez une question dans l'audience, venez à la table, prenez un micro et posez votre question. Y a-t-il une personne dans la salle ou en ligne ? Si une question vient plus tard, n'hésitez pas nous les envoyer, nous répondrons, nous parlerons avec les panélistes et nous obtiendrons la réponse.

AVRI DORIA: Je voudrais revenir à la question d'Alan Greenberg dans le chat, il posait une question sur GLIEF, il disait : quels sont les coûts associés avec LEI, avec les identificateurs d'entités juridiques, je ne sais pas si quelqu'un pourrait répondre à la question.

KARLA MCKENNA: Vous parlez de VLEI ou de LEI ?

MICKAËL PALAGE: Peut-être vous pouvez faire les deux, vous pouvez expliquer qu'avec LEI il y a un mécanisme de recouvrement de coûts.

KARLA MCKENNA: Nous avons trente ou quarante entités qui émettent des LEI et nous savons que si chaque entité qui émet un LEI doit soumettre tous les ans

leurs chiffres de recouvrement de coûts. Et donc c'est le montant qu'ils peuvent facturer pour pouvoir faire la validation pour émettre et maintenir le LEI. Donc cela peut aller d'un montant très bas pour certains enregistrements. Il s'agit d'un chiffre de l'ordre de 50 USD et cela peut aller à des centaines de dollars. Cela dépend de l'organisation sur lesquelles les recherches doivent être faites. Il y a des organisations plus importantes, des entreprises plus importantes qui peuvent obtenir des LEI, cela nécessite des recherches plus importantes.

Nous avons certaines entités qui facturent jusqu'à 200 dollars.

AVRI DORIA: Merci pour votre réponse. Je n'ai pas d'autre question.

MICKAËL PALAGE: Pas d'autres questions dans le chat ? Hadia, vous avez votre main levée, je voulais être sûr que vous ne l'aviez pas baissée, car vous étiez frustrée que l'on ne vous réponde pas.

Très bien. Jonathan ?

JONATHAN ZUCK: Excellente présentation, je me demande ce qu'il en est de l'intégration auprès des opérateurs de registre. Parce qu'évidement, dans l'espace gTLD, ils font partie intégrante, il y a beaucoup d'opérateurs de registre par TLD, donc il faudrait intégrer ce type de technologie aussi, s'ils mettaient en œuvre cette vérification ou c'est une boite noire qui est

ensuite rejetée. Qu'en est-il de l'intégration avec les opérateurs de registre ? Je ne sais pas à qui poser la question, mais je suis curieux.

MICKAËL PALAGE: Je laisse Jacques et Jaromir.

JACQUES LATOUR: Pour .CA, par exemple, ce que les opérateurs de registre nous disent c'est : faites en sorte que cela fonctionne, faites une norme, baissez les coûts et ensuite on verra. Il faut commencer quelque part et ensuite on reproduit, il n'y a pas besoin de rebâtir tout depuis le début.

TIMO VOHMAR: Nos opérateurs de registre aiment bien quand on leur dit qu'on s'en occupe, c'est ce qu'ils veulent entendre.

JAROMIR TALIR: Pareil pour nous, pour la plateforme EUID c'est encore nouveau, on ne l'a pas encore imposé aux opérateurs de registre.

JONATHAN ZUCK: Oui, c'est encore un peu hypothétique pour ce qui est des opérateurs. Oui, ils sont pleins d'espoirs, mais ils ne sont pas encore passés à l'acte.

TIMO VOHMAR: Oui, nous sommes en discussion depuis un moment déjà, ils savent ce qui les attend et la prochaine étape sera de simplifier et de rendre moins chère l'intégration.

AVRI DORIA: Oui, il faudra regarder la présentation de la journée Tech parce que plusieurs ccTLD ont parlé du protocole de l'architecture qu'ils sont mis en œuvre, etc. Et c'est quelque chose qui commence enfin à prendre un peu d'ampleur. Et j'espérais justement en avoir quelques impressions dans ce tableau que j'ai écrit, j'essayais d'exprimer qui construit quoi et où.

BRUCE TONKIN : Oui, juste pour contraster un peu, les vérifications des identifications des commerces ont cours depuis 20 ans déjà en Australie et la dernière phase la plus moderne a commencé il y a deux ans, celle de l'intégration.

MICHAEL PALAGE: Nous arrivons à la fin de la prolongation, merci à tout le monde, à l'organisation de l'ICANN, les participants, les panélistes, c'était une discussion très dynamique, merci beaucoup.

[FIN DE LA TRANSCRIPTION]