KOBE – Séance d’échange avec la communauté : le TSG sur l'accès à des données d’enregistrement non publiques
Lundi 11 mars 2019 – 13h30 à 15h00 JST
ICANN64 | Kobe, Japon

RAM MOHAN : Bonjour. Nous allons commencer à vous présenter notre travail du groupe d’études techniques d’accès sur les données d’enregistrement non publiques dans quelques instants. Merci.

Bonjour à tous. Je m’appelle Ram Mohan et je suis coordinateur du groupe d’études techniques sur l’accès aux données d’enregistrement non publiques, donc le TSG-RD tel qu’il s’appelle.

Nous avons environ 90 minutes de prévues pour cette séance et au cours de la séance, nous devrions utiliser 45 de ces 90 minutes pour vous présenter le processus que nous avons mis en place et nous allons vous présenter un modèle technique préliminaire. Ce que nous souhaitons, c’est avoir vos commentaires, votre feedback et votre point de vue là-dessus.

Notre attente, c’est que la séance soit interactive. Ce n’est pas la seule séance puisque nous avons fait des séances avec les gens du EPDP hier. Et demain et par la suite également, nous

rencontrerons d'autres groupes pour vous présenter ce que nous avons fait jusqu'à maintenant.

Ceci étant, je vais vous présenter notre ordre du jour pour cette réunion. Voilà les sujets dont nous allons parler et nous aurons donc suffisamment de temps pour répondre à vos questions. Je sais qu'il y a des personnes ici qui s'occupent également des commentaires qui nous arrivent des participants à distance et nous pourrons également répondre à ces commentaires.

Ceci étant, je vais donc lancer la séance par une petite introduction du groupe technique en lui-même. Pour un petit peu présenter le contexte pour vous expliquer comment nous avons commencé notre travail, je vais passer la parole à Göran.

GÖRAN MARBY : Avant de commencer, j'aimerais remercier les personnes qui sont présentes dans ce groupe pour tout leur travail, pour tout ce qui a été effectué au cours des trois mois passés. De l'extérieur, je dois vous dire que c'est une réelle bénédiction pour moi de voir le travail des volontaires.

Alors pourquoi ce groupe ? Et bien tout d'abord, lorsqu'on parle de quelque chose de juridique avec une solution technique, il y a plusieurs choses. Je vais d'ailleurs répéter certaines choses que vous m'avez déjà entendu dire.

La loi du RGPD est très spécifique par rapport au rôle des personnes qui traitent les données, des entités qui traitent les données, qui ont les données et qui prennent les décisions par rapport à ces données. Ce sont ces entités-là qui sont responsables dans le cadre du RGPD.

Dans notre monde en fait, il s'agit des parties contractantes. L'ICANN en tant qu'entité juridique n'a pas ces données. Donc quand on parle cette hypothèse, il est très difficile d'avoir un modèle unifié d'accès parce qu'en fait, ce sont les parties contractantes en tant qu'entités individuelles qui ont ces responsabilités juridiques.

Alors qu'est-ce que cela veut dire ? Et bien même si on pouvait avoir un politique par rapport à cela... Je vois monsieur Steve Crocker qui arrive. Il travaille avec moi depuis trois mois là-dessus. Bonjour Steve. Je suis très heureux d'avoir pu mentionner ceci.

Donc c'est l'hypothèse de base, que les parties contractantes doivent prendre leurs décisions de manière individuelles. Donc nous essayons de voir différentes solutions, comment diminuer en fait les responsabilités juridiques des parties contractantes dans ce domaine.

Alors je ne sais pas si vous vous souvenez, mais à Barcelone, j'ai reçu une lettre de pratiquement toutes les parties contractantes me semble-t-il qui m'ont dit : « Pourquoi on ne pourrait pas voir s'il y a des solutions potentielles pour diminuer la responsabilité juridique dans le cadre de la création de ce modèle d'accès unifié ? » Parce que sinon, comme vous le savez, il sera très difficile d'avoir un modèle d'accès unifié parce qu'on ne peut pas mettre en application quelque chose au niveau d'ICANN Org quelque chose qui va au-delà de la loi. La loi est supérieure à l'ICANN.

Donc au début de la discussion, nous avons commencé à avoir des conversations avec la Commission européenne sur différentes alternatives, différentes options, on a essayé de réfléchir à l'ICANN et à son rôle. Donc l'idée qui a été mise en place qui est basée sur le RDAP, c'est donc de venir auprès de l'ICANN avec une question, une question qui est sécurisée conformément aux principes du RGPD, une question aux parties contractantes. Et la seule entité qui puisse répondre à cette question, c'est en fait la partie contractante qui passe par l'ICANN.

Apparemment, cela peut sembler relativement simple mais il faut également des connaissances très techniques pour pouvoir mettre en place ce modèle.

Au sein de l'ICANN Org, nous avons ce modèle mais à la place de cette solution, j'ai demandé à Ram de rassembler un groupe de personnes avec d'excellentes compétences au niveau technique pour voir comment un petit peu comment mettre ceci en place.

Alors la question, c'est que se passe-t-il maintenant ? Premièrement, j'aimerais savoir quel est votre point de vue par rapport à la solution qui va vous être présentée. Et par la suite, ce que nous allons faire dans le cadre de ce système, c'est qu'il faut bien considérer le point d'échange, la plaque tournante. De l'autre côté, il faut savoir qui va poser la question, donc les maisons d'accréditation.

Alors qu'est-ce que c'est, ces maisons d'accréditation ? Il y en a plusieurs. Par exemple, il a Europol, il y a aussi certaines de cette entité de la communauté qui essayent de voir comment bâtir ces maisons d'accréditation. Nous avons suggéré l'OMPI par exemple. L'idée, c'est donc d'accréditer ces maisons d'accréditation qui valident les questions, qui valident les personnes qui posent les questions. En fin de compte, les questions arrivent aux parties contractantes. Donc on essaie de bâtir ceci ensemble mais en fin de compte, une fois que tout ceci aura été mis en place, nous devrons nous tourner vers les autorités de protection de données pour savoir si vraiment nous limitons la responsabilité juridique des parties contractantes.

Si la réponse est oui... En fait, la directive européenne est contraignante du point de vue juridique. Donc il faut que les autorités de protection des données prennent la décision et nous répondent. Les autorités de protection des données ne peuvent pas nous dire quelque chose sans ce contexte juridique.

Donc l'idée, c'est que si les choses se passent comme je l'espère, cela veut dire que l'ICANN aura l'opportunité de créer des politiques sur ce modèle d'accès unifié. Alors la question, c'est que pensons-nous de cette protection des données ? L'intention n'est pas de prendre tout ceci en compte, tout le travail de politiques au sein de l'ICANN, mais c'est d'informer l'ensemble de la communauté de l'ICANN par rapport aux possibilités légales pour un modèle d'accès unifié.

Alors, une petite précaution. Si vous allez vers les autorités, que vont-elles dire ? Il faudra déjà avoir fait son travail parce que pour obtenir des directives du point de vue juridique, il faut absolument faire son travail, surtout quand on s'adresse à la Commission européenne. Nous sommes rares parmi ceux qui ont reçu des directives récemment. Et je n'ai pas le droit de nommer des projets qui soient externes à l'ICANN. Donc c'est un des problèmes.

Par rapport à la spécification temporaire, nous avons eu des directives des autorités de protection des données qui nous

disaient qu'on avait le droit de collecter des données. Et il n'y avait pas de spécification au-delà de cela mais on avait le droit de collecter des données.

Par ailleurs, on a des modèles avec des informations qui pouvaient être publiques et d'autres non publiques. Donc cette directive a été très importante pour nous, cela a été la clé parce que sans cela, notre travail aurait été beaucoup plus difficile.

Maintenant, la situation, c'est que nous n'avons pas de directive du point de vue juridique pour la phase deux. Et c'est justement à cette question que nous devons répondre.

Maintenant, je vous donne la parole pour vos questions. Personne ? Je me sens vraiment seul.

ORATEUR NON-IDENTIFIÉ : Une petite question. Donc est-ce que réduire la responsabilité, cela suffit ? Il y a beaucoup de sociétés qui vont investir des milliards, donc est-ce que cela suffit de dire simplement qu'il est possible que la responsabilité sera réduite ? Est-ce qu'on ne pourrait pas avoir une réponse plus précise par rapport à ce que les autorités de protection des données n'acceptent absolument pas ?

GÖRAN MARBY : Cela, j'aimerais bien. Cela dépendra des autorités de protection des données. La loi, le RGPD, c'est quelque chose d'intéressant. Moi, j'ai travaillé dans la réglementation donc le RGPD, c'est du point de vue technique assez intéressant. Alors j'ai un mauvais sens de l'humour donc pour moi, c'est une loi de la maman, des parents.

Vous savez, quand j'étais adolescent, je me disais je peux sortir et me comporter de telle ou telle façon et tout ira bien et en fait, quand je rentrais chez moi, ma maman me disait : « Mais non, tu t'es mal comporté. » Donc la loi, vous savez, tant que vous pouvez l'expliquer, tout va bien. Vous faites ce que vous voulez, vous faites ce que vous pensez qui est autorisé puis finalement, si vous pouvez l'expliquer, tout va bien. Donc c'est un des problèmes de cette loi parce que les parties contractantes doivent d'elles-mêmes prendre les décisions et décider en fonction. Donc c'est très compliqué pour l'ICANN de mettre ceci en application par rapport à toutes les parties contractantes que nous avons.

RUBENS KUHL : Je suis du .br. J'ai un commentaire et une suggestion.

Mon commentaire, c'est qu'une des motivations, certes, est de réduire la responsabilité mais le potentiel pour ce modèle existe

également de réduire le coût opérationnel par rapport au modèle d'accès unifié. Donc il y a des motivations à la fois positives et négatives qui pourraient entrer en jeu.

Alors la suggestion que je souhaite mettre de l'avant, c'est est-ce que l'ICANN ne pourrait pas rendre ce modèle obligatoire ? Le problème, c'est que quand c'est obligatoire, les gens en général résistent. Pourquoi est-ce qu'on fait comme ceci, pourquoi est-ce qu'on fait comme cela ? Par contre, lorsque quelque chose est optionnel, facultatif mais qu'au sein de l'espace des gTLD la couverture est importante, parfois, c'est plus fort que quelque chose qui est obligatoire, justement parce que ce sont les idées qui vont pousser les gens à agir, pas la force parce qu'on leur impose quelque chose.

GÖRAN MARBY : Par rapport à votre deuxième point, à l'ICANN dans nos contrats, nous avons déjà des clauses ; lorsque les lois en fait sont en contradictions avec nos contrats, les gens peuvent suivre la loi plutôt que le contrat. Donc avec tous les pays qui sont concernés, évidemment qu'on est obligé d'avoir ces clauses.

Nous ne pouvons pas forcer les gens à mettre en œuvre une clause qui soit contraire à la législation locale. Parfois, nous avons dit bon, nous allons essayer de mettre ceci en place. Est-

ce que c'est une probabilité à 100 % ? Non. Mais pour moi, il était important d'enquêter par rapport à la possilibité de pouvoir réduire la responsabilité des parties contractantes. Mais il faut en plus que les parties contractantes l'acceptent. Donc justement, il faudra que l'on crée quelque chose qui puisse être acceptable. Et il faudra également que cela corresponde à la loi.

Donc certes, c'est complexe. D'un autre côté, l'ICANN en tant qu'institution a finalement un arrangement assez volontaire. Les contrats que nous avons avec les parties contractantes sont basés sur les politiques qui sont définies par la communauté grâce au processus ascendant. Finalement, à la base, notre modèle est basé sur le consensus. Le consensus, cela veut dire quoi ? Cela veut dire qu'on accepte. Mais je comprends ce que vous voulez dire. Nous ne sommes pas un gouvernement.

ORATEUR NON-IDENTIFIÉ : J'ai quelques questions. Désolée, j'ai oublié l'acronyme. Je ne sais pas exactement si ces questions ont déjà été traitées mais j'ai deux questions en fait.

Le RGPD donne aux utilisateurs finaux un accès plus important à leurs données. Pouvez-vous me dire, si par exemple vous avez quelqu'un qui a son propre site web, si cette personne veut voir ses informations, dans le cadre de ce nouveau, est-ce qu'il y

aura une case qui indiquera à l’utilisateur final si ses informations sont publiques ou privées ? Cela, c’est la première question.

Deuxièmement, il y a quelqu'un d’un bureau d'enregistrement qui disait hier à quelqu'un qui demandait à avoir accès pour les consommateurs qui souhaite vérifier l’authenticité de leurs sites web que malheureusement, était donné que les bureaux d'enregistrement ne pouvaient pas faire la différence entre un particulier et une société qu’en fait, cela ne pouvait pas être possible, de faire la différence. Est-ce que c’est vrai ? Est-ce que c’est vrai que cette distinction entre les particuliers et les sociétés n’est pas possible dans le nouveau système ?

GÖRAN MARBY : Les questions que vous posez sont des questions de politiques, donc qui ont trait aux PDP. Donc il s’agit d’une question de politique et ce n’est ni moi ni personne à cette table qui peut vous répondre parce que nous ne sommes pas impliqués dans les politiques.

Moi, je suis très strict par rapport à cela. C’est vraiment quelque chose de différent. Les questions que vous posez sont relatives au travail sur les politiques. Alors la solution technique a une

cible précise : c'est donc de diminuer la responsabilité juridique des parties contractantes.

Alors bien sûr, votre question est très intelligente parce que les législateurs, les autorités de protection des données, pourraient avoir une opinion par rapport au PDP existant et cela pourrait avoir un impact, certes. Mais nous n'avons pas encore cette réponse.

Par ailleurs, la législation est assez nouvelle. Il y a très peu d'historique juridique dans les tribunaux par rapport cette législation.

Alors par rapport à votre première question, je ne sais pas, je ne connais pas la réponse. Peut-être.

BENEDICT ADDIS : Je m'appelle Benedict Addis et j'ai fait partie du EPDP également. Donc j'ai vraiment une perspective EPDP dans la réponse que je vous donne maintenant et ce que je peux vous dire, c'est que nous avons parlé de l'idée d'avoir cette option de publication. C'est ce à quoi nous avons réfléchi. Et je pense que la réponse, c'est sans doute que oui. Pour l'instant, ce n'est pas possible mais à l'avenir, sans doute. Et c'est quelque chose que les gens nous demandent souvent.

Par rapport à la distinction entre les particuliers et les sociétés, il y a un certain nombre de raisons pour lesquelles c'est difficile. Cela peut sembler relativement simple en apparence mais en fait, c'est extrêmement complexe. Il y a des organismes qui ont le droit à la protection de leurs droits privés dans certains pays par rapport à la loi locale, par exemple je ne sais pas, une clinique des qui fait des avortements. Donc il y a un certain niveau de complexité par rapport à cette question et nous n'avons pas encore dit oui ni non, nous n'avons pas encore répondu par oui ou pas non au niveau du EPPD par rapport à cette question. C'est une question qui aura lieu à la phase suivante. Mais en tout cas, merci pour ces excellentes questions.

RAM MOHAN : Merci Benedict, merci Göran, merci pour ces questions qui nous viennent de la salle. Au fur et à mesure que nous aurons d'autres questions sur les politiques, certainement, vous pouvez nous les poser et nous pourrons en fait les envoyer aux groupes concernés qui ont une démarche spécifique par rapport à ces questions.

En attendant, Göran.

GÖRAN MARBY : Je vais aller dans la salle pour écouter.

RAM MOHAN : Parlons maintenant de ce que nous avons fait. Göran vous a donné un peu l'historique du travail. Le but de ce groupe technique, c'est d'explorer des solutions techniques pour authentifier, autoriser et fournir l'accès pour les tierces parties qui auraient un intérêt légitime à les obtenir. Donc voilà le but.

Il y a une charte qui a été écrite pour le TSG. Tout cela est publié dans la charte. Vous voyez l'URL sur l'écran devant vous. Avec cet URL, vous aurez accès à toutes ces informations.

Nous étions très clairs et Göran l'a dit, nous avons essayé d'adhérer autant que possible à ce que le TSG ne prenne pas de décision ou ne fasse pas de recommandations sur les questions liées aux politiques, par exemple qui a accès à telle chose ou si l'accès doit être appelé un accès, quels sont les accès qui doivent être donnés, quels sont les intérêts légitimes, etc. Il y a une panoplie de questions qui sont présentes. Nous sommes heureux qu'elles soient là ces questions, mais cela ne fait pas partie de notre mission. Nous nous sommes focalisés clairement sur le côté technique des choses.

Qui sont les membres du TSG ? Comme on vous l'a dit, Göran est un sponsor et pour cela, il m'a demandé de former un groupe en octobre de l'année dernière. J'ai passé un peu de temps à

prendre cette décision. Vous voyez, il y a des photos sur l'écran et vous voyez sur ces photos, il y a toutes les personnes qui font partie de ce groupe. Il n'y a que Murray de Facebook qui n'est pas là d'ailleurs. Mais le reste des personnes qui font partie de ce groupe sont là sur cet écran.

Nous avons eu beaucoup de chance car le travail de ces volontaires a été vraiment appuyé par une équipe de l'ICANN de première classe. Vous voyez certains d'entre eux sont là, il y a Elisa, il y a Lianna, il y a John Crain, Gustavo et il y a Francisco Arias qui n'est pas présent. Nous avons eu aussi beaucoup d'aide de la part d'Yvette et d'Erika sur le travail que nous avons fait.

Lorsque nous avons commencé, il était clair que la façon avec laquelle nous pourrions obtenir de vrais résultats, ce serait de travailler avec un consensus, que nous devrions être itératifs dans nos processus, que nos réflexions devraient être techniques. Et c'était vraiment un modèle de participation primaire que nous avons utilisé.

Nous avons donc formulé ces processus pour en arriver à une solution telle que celle dont je vais parler. Nous avons d'abord défini des questions clés, des considérations. Ensuite, nous avons identifié les hypothèses principales. Ensuite, nous avons identifié des cas d'utilisation et les parcours des utilisateurs.

Nous avons défini les exigences des systèmes, qu'elles soient fonctionnelles, opérationnelles ou de gestion, nous avons créé des exigences fonctionnelles, nous avons construit des modèles, nous avons déterminé des considérations de mise en œuvre.

Nous avons toutes ces choses qui nous ont permis, lors de nos réunions face-à-face, d'en arriver à une solution. C'était vraiment un processus itératif. Nous avons mis en place plusieurs modèles, nous les avons étudiés. Nous avons décidé de ce qui était bon ou mauvais et nous avons ainsi choisi une solution que nous avons appelé le modèle technique.

En faisant tout ce travail, en arrivant à ce modèle technique, en observant le modèle déjà existant et en connaissant les exigences, nous nous sommes rendus compte de plusieurs choses. Les considérations qui avaient été prises dans cet espace étaient claires. Ces considérations et observations ne nous concernaient pas puisque nous sommes un groupe technique. Nous ne pouvions pas agir sur ces sujets.

Ce que nous avons fait pour être complet et pour faire du bon travail, nous avons, nous avons pris de note de toutes ces observations et considérations lorsqu'elles ont été soulevées et ces notes seront dans le document final que nous allons publier. Mais ces considérations seront envoyées à d'autres parties de la communauté.

Lorsque nous aurons fini avec cela, nous allons demander le feedback de la communauté en général et nous allons mettre en place une séance pour cela. Nous allons faire cela cette semaine d'ailleurs. Et ensuite, ce groupe technique va se retrouver physiquement ici à Kobe pour faire une révision de tous les feedback que nous avons reçus durant cette réunion et pour voir si nous devons faire certains changements ou autres modifications au modèle auquel nous sommes arrivés.

Nous allons ensuite passer quelques semaines – peut-être trois ou quatre semaines – pour essayer de réitérer un peu le travail que nous devons faire. Donc notre intention, c'est de terminer notre travail d'ici la mi-avril et de publier ce que nous allons considérer notre travail final qui sera publié à la fin avril, qui sera envoyé à vous, la communauté, à Göran, pour ensuite se qualifier pour être l'action 13 de notre charte.

Je parlais tout à l'heure du processus et lorsque vous observez ce que nous avons fait, regarder quelles seront les questions clés et des considérations clés a été la première chose que nous avons faite.

Si vous allez sur la page icann.org/TSG, vous verrez qu'il y a toutes ces catégories qui sont listées et chaque catégorie comprend des questions. Je pense qu'il y a à peu près 17 ou 18 questions qui composent ces catégories. Et cela nous a aidé à

organiser nos réflexions ; on s'est dit qu'est-ce qu'on doit étudier, qu'est-ce qu'on doit faire dans tel ou tel cas.

Une des choses qui a été logique pour nous lors de notre travail, on s'est rendu compte qu'on devait être très clairs sur les hypothèses que nous formulions parce que si nous n'avions pas défini ces hypothèses, le travail fondamental que nous avons fait n'aurait pas été complet.

Nous avons continué après ce processus et nous avons fait une liste des hypothèses clés. Nous les avons détaillées dans le processus. Et nous avons commencé au mois de novembre avec sept hypothèses. Et maintenant, je pense que nous en avons quelques unes de plus ; c'est un bon signe. Cela veut dire que nous avons pris conscience d'autres problèmes.

Autre chose que je voulais souligner, c'est que lorsque nous parlons d'hypothèses dans le document et comme dans les diapositives à l'écran, ce que vous devez voir, c'est que nous soulignons les choses qui doivent être faites, qui sont les bonnes choses à faire. Ce que nous faisons, c'est simplement de documenter ces hypothèses ou ces considérations puisque ce sont des commentaires qui ont été faits ou ce sont des questions qui existent dans l'espace. La fondation de notre travail est basée sur les hypothèses qui existent et qui sont vraies. Clairement, certaines de ces hypothèses ne sont pas vraies,

doivent évoluer, doivent changer, mais elles ont de toute façon un impact sur le modèle en lui-même. Moi, j'aimerais bien être dans le public et être à votre place et voir comment ces choses vont évoluer, au niveau technique si vous voulez.

Un des éléments importants dans tout cela, c'est que notre mission est basée sur les éléments techniques. Si vous observez les hypothèses, si vous voyez des questions qui ont à voir avec les politiques et si vous avez des questions sur nos hypothèses, sachez que nous avons une déclaration ici.

Amenez-nous vos questions mais sachez que nous ne sommes pas en position de fournir des réponses autoritaires au sujet des ces hypothèses, qu'elles soient appropriées ou pas. Ce que vous devez savoir, c'est que ce sont nos hypothèses. Il est possible que nous ayons manqué certaines des hypothèses et peut-être que ces hypothèses que nous avons formulées sont complètement fausses.

Sachant cela, je vais passer la parole à Steve et je vais lui demander de nous parler de ces hypothèses.

STEVE CROCKER : Voilà, vous avez image conceptuelle des requêtes pour les données non publiques par rapport à la passerelle (gateway) de

l'ICANN lorsqu'il s'agit de l'accès aux données de telle ou telle requête et des processus d'autorisation et d'authentification.

Il y a 12 hypothèses sur ce sujet. J'ai fait référence à six de ces hypothèses entre parenthèses d'ailleurs comme vous les verrez sur la prochaine diapositive. Le mode de base RDAP est le mécanisme que nous allons utiliser, donc l'accès Port 43 sera obsolète. L'accès aux données non publiques de gTLD fera partie de cet accès. Les requêtes des sources non identifiées seront contrôlées par le service de protection d'ICANN.

Cette diapositive vous montre les 12 hypothèses. Celles qui sont en haut sont celles dont je vous ai parlées. Celles du bas, ce sont des hypothèses variées qui discutent des questions d'évolution et d'autres questions. Donc il doit y avoir un processus qui doit se préoccuper des changements des règlementations et de l'évolution du modèle et des pratiques en général. Il faut mettre en place un pilote et les choix de politiques doivent être faits. Il faut voir aussi le côté pratique des mises en œuvre des politiques.

Il faudra lire le rapport pour obtenir d'autres détails sur cela. À vous, Ram.

RAM MOHAN : Donc, après avoir formulé ces hypothèses, nous en sommes arrivés à définir des cas d'utilisation. Tout à l'heure, je vous ai parlé du processus que nous avons suivi. Les cas d'utilisation, cela fait partie aussi du travail que nous avons fait.

Andy, vous voulez bien nous parler de cela ?

ANDY NEWTON : Oui. Les cas d'utilisation que nous avons étudiés sont listés ci-dessus. Nous avons demandé aux utilisateurs autorisés qui avaient besoin d'accès à certaines informations telles que les forces de l'ordre par exemple – les forces de l'ordre, c'est un acteur vers lequel nous nous sommes retournés très souvent, qui nous a aidé dans nos recherches, les gens aussi qui travaillent pour la propriété intellectuelle. Eux ont besoin d'accéder à ces données. Nous avons aussi vu que les utilisateurs qui recevaient les autorisations en ligne devaient recevoir cette autorisation rapidement lorsque c'était possible.

Nous avons aussi un autre cas dans lequel il y avait un besoin pour certains utilisateurs d'avoir accès à des données qui leurs étaient associées. Nous avons eu besoin d'avoir du soutien pour ces utilisateurs qui ne pouvaient pas avoir accès à certaines données.

Ensuite, nous avons parlé des utilisateurs qui sont les sujets de ces données et comment pouvaient-ils eux-mêmes avoir accès à ces données.

De là, nous en sommes arrivés à mettre en place des exigences. Tout d'abord, nous avons commencé à observer les différents éléments du système et nous avons élargi le sujet un peu. En général, nous avons parlé des standards des normes de l'internet, nous avons de support de l'IPv6 qui doit être distribué. On doit donc pouvoir soutenir un modèle de distribution de l'IPv6. Nous devons aussi donner du support pour le TSL et d'autres protocoles de sécurité appropriés.

Une des choses que nous avons décidé tout de suite, c'était d'avoir un portail web pour les personnes qui ont des requêtes rapides, qui ont besoin d'avoir l'accès rapide et une fois. Et nous avons mis en place des exigences et nous allons mettre en place un portail qui sera géré par l'ICANN.

Nous avons parlé aussi de l'authentification et de l'autorisation, à voir si cela va être délégué à des agents qualifiés, peut-être nommés par l'ICANN. Nous avons aussi parlé de la façon avec laquelle nous allons procéder. Nous avons parlé d'un gateway RDAP de l'ICANN qui passerait par les serveurs RDAP. Il y aura dont ainsi des requêtes multiples qui seraient gérées par des politiques multiples. Et tout cela doit avoir l'appui des parties

contractuelles. Lorsque nous aurons une requête qui ne sera pas autorisée, nous devons savoir aussi comment on va pouvoir rediriger cette requête.

Il y a après les problèmes des serveurs RDAP par les parties contractuelles. Ils doivent pouvoir répondre aux requêtes du gateway RDAP de l'ICANN.

Je vais vous parler des exigences en général. Nous avons des requêtes de login et d'auditing. Nous devons parler de la rétention des données. Nous devons aussi essayer de réconcilier des requêtes de toutes les parties pour pouvoir faire des audits et nous préoccuper des abus qui sont faits sur le système. Nous avons aussi des requêtes de performance. Nous devons être sûrs d'avoir des accords de service parce que sans cela, nous ne saurons jamais quelle est la partie du système qui ne fonctionne pas.

Ensuite, nous avons parlé des exigences de sécurité pour les informations et on a vu qu'il devait y avoir une évaluation des exigences. On doit avoir un moyen de faire des audits et de fournir les informations de ces audits aux personnes qui les demandent.

Ensuite, nous devons avoir un moyen de faire des rapports. Tout cela doit être gouverné par un programme de gestion pour nous

assurer que toutes les techniques d'entreposage cryptées sont faites.

Je pense que c'est tout. Scott, vous voulez parler du modèle en lui-même ?

SCOTT HOLLENBECK : Merci Andy. Bon, le titre de la diapositive dit ceci : « Le modèle est basé sur deux standards et protocoles. OAuth 2.0 et OpenID Connect ».

Avant de parler de cette diapositive qui a plein de termes techniques, je voudrais vous montrer une photo. Vous voyez ce diagramme qui correspond à une évolution de celui que Steve vous a montré. Il comprend plus de détails. Vous voyez les interactions entre les différents facteurs.

Si vous êtes familiers avec les services d'authentification unique, quand vous devez vous identifier par exemple sur Twitter, sur votre adresse Gmail ou sur identifiant Facebook, conceptuellement, vous pouvez comprendre ce modèle. Bien sûr, il y a beaucoup plus de détails mais le flux est similaire.

Nous allons revenir en arrière en ensuite, nous reviendrons à ce diagramme. Il y a des pré-exigences pour que ce système puisse fonctionner. Tout d'abord, ces fournisseurs de service doivent

exister. Il doit y avoir des processus qui les amènent à exister. Il y a du travail d'élaboration de logiciels qui doit être fait pour que ces services soient opérationnels.

Les demandeurs, *requestors*, c'est un terme que nous avons pris du EPDP pour identifier les gens qui requièrent des informations sur les données. Ces fournisseurs d'identification sont des nouveaux acteurs. Ils doivent associer les attributs des identifiants avec l'accréditation.

Cette solution marche en dehors de la boîte aujourd'hui en utilisant des services qui sont fournis par des compagnies comme Google, Yahoo, etc. Ces fournisseurs ne connaissent rien sur le RDAP, donc ils n'ont aucune association avec cela. Cela, c'est à venir.

Donc une fois qu'on a les prérequis, le processus se met en route et le demandeur envoie une demande RDAP par un service d'accès en utilisant une application client. Donc le service d'accès reçoit la requête mais étant donné que le service ne sait pas qui demande, on va demander au client d'aller s'adresser à un fournisseur d'identité.

Ensuite, la personne verra un formulaire web qui lui demandera d'envoyer son identité ou alors ce sera peut-être un certificat de client si c'est quelque chose qui a été négocié à l'avance.

Donc disons que les informations d'identification sont validées et ensuite, le client verra une demande à sélectionner différents morceaux d'identité – ce sont les attributs dont on a parlé – et d'approuver comme quoi ces informations seront partagées les autres parties, en fait avec la partie sous-jacente, le service qui contrôle l'accès à ces informations protégées.

Donc le demandeur répond, remplit tous les formulaires, envoie le formulaire. Et ensuite, le fournisseur d'identité fournit un code d'autorisation au client. Ensuite, il y a redirection http au service d'accès, ce qui lance le processus de mise en place d'une requête RDAP.

Le service d'accès prend ce code d'utilisation et l'utilise pour extraire des ensembles de données qu'on appelle des tickets ou des jetons d'identité, qui sont renvoyés au client. Alors ces jetons contiennent des informations sur l'identité associée au demandeur et qui en fait détermine l'autorisation.

Donc il y a une requête RDAP qui est envoyée avec ces informations de jetons à la passerelle, au gateway ICANN. Et lorsque ceci est reçu, la requête RDAP est traitée. Donc la requête est reçue avec les jetons et ensuite, les informations sont envoyées à une partie tierce qui autorise et qui vérifie. Donc tout ceci est traité par l'entité d'autorisation, s'assure que tout est valide et ensuite, il correspond la requête aux attributs pour

s'assurer que tout va bien. Et ensuite, il y a des résultats de vérification qui sont envoyés par la passerelle. Donc la passerelle, ce sera soit oui, tout va bien ou alors non, la personne n'est pas autorisée à demander ces informations.

S'il y a autorisation, la passerelle, le gateway, envoie les requêtes RDAP au serveur RDAP, donc soit un bureau d'enregistrement ou un opérateur de registre suivant le cas, pour en fait retirer toutes les données non publiques. Les réponses seront filtrées, traitées pour envoyer une réponse RDAP au client qui ensuite affichera les résultats et les enverra au demandeur.

Voilà encore une fois une photo, donc c'est le même flux de données.

RAM MOHAN : Merci Scott. Mais est-ce que vous pourriez nous parler des services d'autorisation ? En fait, on a divisé les deux entités et donc je pense qu'il serait utile, on a eu des questions hier par rapport à l'objectif est-ce que les différentes entités sont ensemble, comment fonctionne la distribution. Donc ce serait bien d'en parler un petit peu.

Par ailleurs, nous avons également parlé ou délibéré sur un autre sujet, la question du fournisseur d'identité. Quel est son rôle ?

SCOTT HOLLENBECK : Oui, merci Ram, pas de problème. Je ne sais pas si vous connaissez le WHOIS. J'imagine que ceux qui sont dans cette salle vous le connaissez, vous savez comment cela fonctionne. Vous savez qu'il y a deux acteurs dans ce modèle : il y a le client et les serveurs RDAP bureaux d'enregistrement et opérateurs de registre.

Et en fait, ce modèle ne fonctionne pas vraiment bien lorsqu'ils faut prendre des décisions en termes d'identification, d'authentification et de contrôle de l'accès. Donc voilà pourquoi ces services entrent en compte. OpenID Connect et OAuth 2.0 sont faits pour avoir les moyens d'identifier les clients pour les authentifier et pour que les décisions d'accès soient basées sur les identités.

Mais cela veut dire qu'il faut ajouter d'autres acteurs. Premièrement, ce service d'accès RDAP de l'ICANN dans notre petit groupe, nous parlions du service d'enregistrement fiduciaire. C'est un petit peu comme un agent, un courtier

finalement qui reçoit les requêtes et qui décide de qui peut être impliqué et comment traiter la requête.

Mais une des premières choses que le serveur doit faire lorsqu'il reçoit une requête, doit d'abord savoir à qui il parle. Et il le fait par le fournisseur d'authentification, le fournisseur d'identité.

Alors voilà comment fonctionne le protocole. Ces services peuvent être effectués par une entité qui parfois est définie comme fournisseur d'identité ou alors on peut diviser les deux fonctions en plusieurs acteurs. Le modèle que nous avons décrit en fait donne l'option pour les deux options. En fin de compte, je crois que ce sera le politiques qui détermineront comment la division des services sera mise en place et qui effectuera telle ou telle fonction.

Mais comme vous le voyez, il y a une interaction. Donc vous avez le fournisseur d'authentification qui reçoit la requête du service RDAP, il y a interaction avec le client. Vous avez l'interface web dont j'ai parlé tout à l'heure. Voilà là où le client fournit sa vérification d'identité. Ensuite, il y a la fonction d'authentification. Et le service RDAP n'a pas besoin d'être exposé à ces informations. Il a simplement une attestation du fournisseur qui lui dit si oui ou non le client est authentifié et identifié.

Mais ensuite, il y a le service d'autorisation. Une fois que le RDAP sait que la personne est identifiée et authentifiée, il faut maintenant décider si oui ou non le demandeur a le niveau d'accès qui correspond à ce qu'il demande. Donc encore une fois, cela, c'est une fonction qui peut être divisée et donnée à une partie tierce. C'est ce que nous essayons de définir dans le cadre de notre modèle. Donc la requête est envoyée, les comparaisons sont effectuées par rapport à certaines politiques qui ne sont pas encore mises en place. Donc soit c'est oui, soit c'est non. Le service ensuite agit suivant la réponse. Voilà.

Est-ce que c'est ce que vous vouliez, Ram ?

RAM MOHAN : Oui, très bien. Merci Scott.

Encore autre chose. Il y a eu une question qui nous est arrivée pour savoir si ce service d'accès RDAP de l'ICANN dans le cadre de notre modèle veut dire que les données qui sont là dans les différentes sources, est-ce que l'ICANN aura une copie de ces données dans ce modèle ou pas ? Il serait bien de répondre à cette question.

SCOTT HOLLENBECK : Oui. Alors en ce qui concerne les données dans ce modèle, les données restent dans les sources qui font autorité. Alors, qu'est-ce que cela veut dire, faire autorité ? Je sais que c'est compliqué. Par exemple dans le WHOIS détaillé, les opérateurs de registre sont un petit peu la source d'autorité pour ainsi dire pour les données.

Donc selon nous, faire autorité, cela veut dire que l'entité qui a la relation avec la personne concernée, l'entité concernée, ce qu'il faut savoir, c'est où la donnée est collectée, où est-elle produite. Parfois, il y a une séparation entre les fonctions des bureaux d'enregistrement et les opérateurs de registre. Les bureaux d'enregistrement, eux, gardent les données pour lesquelles ils ont autorité. C'est un petit peu différent du côté des opérateurs de registre.

Dans le cadre du RDAP, du modèle que je vous ai décrit, l'ICANN ne garde pas les données. Il n'y a aucun enregistrement qui est fait. Il y a uniquement des logs d'accès. Les données ne sont pas conservées. C'est uniquement une transition qui passe par l'ICANN.

RAM MOHAN : Merci beaucoup. Vous n'arrêtez pas de pousser cela vers moi, je vois. Je voulais rester un petit peu là-dessus parce que c'est un

petit peu le cœur de ce que nous cherchons à faire dans notre groupe.

Une autre question qui a été soulevée, Scott, c'est donc ce service d'accès RDAP de L'ICANN. Dans la question, c'était de savoir si dans notre modèle, on avait imaginé que tout ceci serait centralisé. Est-ce qu'on s'imagine que c'est simplement quelque chose qui est sur un site web ? Est-ce qu'il y aura des modèles automatisés ? Et par ailleurs, si vous êtes non authentifié et peut-être même non autorisé, si une demande de ce type nous arrive, une demande de données restreintes ou non publiques, s'il s'agit d'un domaine qui n'est pas un domaine gTLD, quel est notre rôle ? Comment cela marche ? Il serait important d'avoir la réponse, me semble-t-il.

SCOTT HOLLENBECK : Oui. Alors le service d'accès RDAP, ce que nous envisageons, c'est effectivement une interface web avec deux parties. Nous avons besoin d'un accès automatisé en ligne mais nous avons également besoin d'un accès asynchrone. Donc s'il y a quelqu'un qui n'a pas nécessairement le droit mais qui a peut-être quand même un objectif tout à fait légitime pour demander des informations, il pourra peut-être faire l'objet d'une révision et on pourra peut-être lui faire une réponse d'une manière ou d'une autre.

Mais ce service d'accès RDAP pourrait être mis en œuvre exactement comme n'importe quel autre service web. Il ne s'agira peut-être pas d'un serveur unique, il y a une question d'équilibre de la charge. Donc on verra quelle est la meilleure pratique à suivre.

Mais en ce qui concerne les fonctions d'identification et d'authentification, cela peut être centralisé mais cela peut également être distribué. Et le modèle que nous essayons de promouvoir, c'est un modèle dans lequel ces fonctions ne sont pas centralisées. Elles sont distribuées. Ces fonctions serait effectuées par des entités qui sont en lien avec le demandeur parce que les demandeurs sont connus, donc ils peuvent émettre les identifications et prendre des décisions sur la base des relations qui existent.

En ce qui concerne les données publiques, vous verrez qu'une chose que nous avons ici, c'est qu'on s'attend à ce que les parties contractantes aient des interfaces publiques pour les données publiques. Donc les clients pourront envoyer leurs requêtes directement aux bureaux d'enregistrement ou aux opérateurs de registre et ils recevront ce que les politiques détermineront comme des données publiques.

ORATEUR NON-IDENTIFIÉ : Dans notre document, nous avons parlé des différentes combinaisons, de divisions ou de combinaisons des fournisseurs d'identité et des fournisseurs d'identification. Donc nous avons un modèle acteur. Nous avons différentes combinaisons qui ont été définies dans le document. Je crois qu'il y a quatre possibilités.

Pour revenir aux utilisateurs non autorisés ou non authentifiés, d'une manière générale ce que nous avons demandé, c'est que la passerelle RDAP de l'ICANN fournisse un serveur qui puisse rediriger avec http la source qui existe dans le fichier bootstrap http. Donc ce n'est pas uniquement du point de vue gTLD ICANN mais le RDAP utilise d'autres contacts, les espaces RIR et les ccTLD également.

RAM MOHAN : Merci. Merci Scott.

Ceci étant, je vais maintenant passer la parole à Gavin pour la partie considérations.

GAVIN BROWN : Merci Ram. Ram a mentionné au début mais je vais quand même le répéter un petit peu, nous avons eu différentes discussions et nous avons identifié certaines choses qui à notre avis n'avaient

pas été bien analysées avant le début de notre travail. Et puis cela faisait partie de notre mandat également parce qu'on se focalise surtout sur une solution technique et il est quand même très intéressant de s'impliquer dans les politiques.

Donc je vais vous parler des grands points. Vous avez les diapositives à l'écran.

Nous avons déjà parlé de la rétention des données brièvement. Il a déjà été dit que nous n'envisageons pas cette passerelle d'accès comme une passerelle qui enregistrerait des données d'enregistrement. Il n'y a rien qui soit stocké, c'est simplement une transition vers les parties contractantes.

Mais il y aura certains éléments de données qui sont entreposés quand même, certains logs. Et certes, il y a des risques qui existent par rapport à ces logs. Donc dans le domaine du travail sur les politiques, les règles de rétention de données devront être appliquées à ces enregistrements ou à ces logs. Donc il faudra en parler.

Il y a différentes choses qui devront exister dans le système pour pouvoir s'assurer – justement, on parlera tout à l'heure de la transparence. Il est important de pouvoir auditer le système pour s'assurer que tout se passe bien. Donc le logs, cela fait vraiment partie de ces capacités.

Et il faudra également pouvoir réduire le risque de divulgation. Le fait que quelqu'un ait présenté une requête, cela veut dire déjà à la base qu'il y a certaines informations qui sont divulguées. Donc avoir une politique pour réduire le risque de la divulgation, à mon avis, c'est quelque chose de très important.

On a parlé également tout à l'heure des conventions de service. De toute évidence, il y a un certain nombre de parties qui sont impliquées. Le modèle que nous avons décrit comprend un certain nombre d'entités séparées qui chacune compte sur le fonctionnement des autres pour qu'elles puissent faire leur travail dans le cadre de ce système. Et l'utilisateur final également compte sur la disponible du système pour que ses besoins soient satisfaits. Donc il faudra qu'il y ait des conventions de service qui soient définies et mises en place pour garantir la disponibilité et la fiabilité du système.

Nous recommandons également à ICANN Org d'assurer la transparence dans le domaine de ces conventions de service, peut-être avoir une page où le demandeur peut voir quel est le statut du système de manière assez rapide et simple.

L'ICANN doit pouvoir également revoir l'impact potentiel de la responsabilité de s'occuper d'un système tel que celui-ci, et puis le rôle des parties contractantes. Les points trois et quatre peuvent être considérés ensemble.

Certes, il y a des risques juridiques et il y a des risques au niveau opérationnel qui pourraient être très importants. Encore une fois, cela dépendra du développement de politiques et de la mise en place du système. Mais il y a un certain nombre de risques à prendre en compte, le risque de sécurité des informations, nous en avons déjà parlé. Et également nous avons considéré qu'il était important de signaler à l'ICANN et à la communauté que certaines révisions, certaines évaluations devaient être effectuées pour justement être sûr de bien traiter ces risques.

Selon nous, il a été important de signaler la question de la réduction de la responsabilité juridique des parties contractantes. Nous sommes geek, nous ne sommes pas avocats donc nous ne savons pas si le système que nous proposons réduit réellement cette responsabilité juridique. Donc pour nous, il était essentiel d'encourager les parties contractantes à nous donner leur propre point de vue. Et je pense qu'elles le feront.

En ce qui concerne la transparence, brièvement, pour nous, c'est une partie cruciale par rapport à la confiance en ce système. Si l'ICANN souhaite réellement mettre en place ce système, il faut réellement être transparent par rapport à l'utilisation du système. Nous n'allons pas donner de détails par rapport à la

divulgation ou la publication d'informations spécifiques mais comment est-ce que le système va être utilisé. C'est vraiment la clé pour comprendre, pour s'assurer qu'il y a réellement confiance en l'intégrité du système. Donc ce que nous avons proposé, c'est un rapport de transparence qui soit publié régulièrement et communiqué à la communauté.

Enfin, nous avons reconnu que le demandeur pourra de temps à autre être en désaccord par rapport au résultat de sa demande. Alors il nous faudra mettre en place un mécanisme pour traiter des plaintes, des plaintes sur les processus, des plaintes sur le système ; tout doit pouvoir être collecté et on doit pouvoir y répondre. Il doit y avoir un processus de traitement de ces plaintes qui devra également inclure l'effacement de certaines demandes. Cela fait partie du RGPD parce que certaines personnes concernées pourront demander à l'ICANN, que ce soit justifié ou non, d'effacer certaines données les concernant. Voilà. Ram.

RAM MOHAN : Merci Gavin.

On va passer à la diapositive suivante, merci beaucoup. C'est la conclusion de nos explications sur les commentaires que nous avions pour la réunion d'aujourd'hui. Nous sommes sur la bonne

voie, nous avons reçu les informations de la communauté. Nous les avons rassemblées. Nous avons jusqu’à mercredi cette semaine pour... Non, excusez-moi, nous allons le faire encore un peu plus longtemps. Nous voulons incorporer tous ces commentaires afin de mettre en place ce modèle technique. Nous planifions avoir plusieurs téléconférences et des réunions en face-à-face d’ici la mi-avril pour pouvoir finaliser notre travail. Nous voulons publier ce modèle technique final à la fin d’avril. Ensuite, bien sûr, ce groupe se séparera et nous aurons complété notre travail.

Maintenant, nous sommes là pour répondre à vos questions. Je vois qu’il y a déjà quelqu'un au micro pour poser une question. Il y a des micros dans la salle et je ferai de mon mieux pour modérer vos interventions.

RUBENS KUHL : Je me demande si le groupe a considéré un scénario dans lequel l’ICANN pourrait utiliser OAuth ou OpenID. Là, les parties contractantes seraient contactées directement. Cela éviterait la circulation des données dans le système de l’ICANN parce que c’est cela qui pose un problème. Même si ce n’est pas une question de proxy en cache, si les proxy sont compromis, cela pose un problème.

Il y a eu une possibilité de centraliser le flux de données. Ce système n'a pas été choisi. Y a-t-il une raison derrière cela ?

ANDY NEWTON : La raison pour laquelle nous n'avons pas fait cela, c'est que nous devions avoir un mécanisme pour distribuer les politiques à toutes les parties contractantes. C'était une tâche importante pour toutes les parties contractantes parce qu'il fallait faire des mises à jour de toutes les politiques. Donc il était plus facile pour ICANN Org de s'en préoccuper. Donc c'est pour cela que nous avons choisi cette façon de faire. C'est un modèle plus simplifié, plutôt qu'avoir accès directement aux parties contractantes.

Quand il s'agit des conventions, je ne pense pas qu'elles soient changées.

RUBENS KUHL : À l'ICANN, le flux des données ne devrait pas être centralisé. Il n'y a pas de besoin pour qu'une décision ait un impact sur une autre.

ANDY NEWTON : Lorsqu'il s'agit des conventions d'accord, il y a donc un impact sur tous les services que l'ICANN entreprend. Je pense que la

question de la convention ne change pas... Quelque soit le type de système, cela ne fait pas de différence.

GAVIN BROWN : Avoir un accès unique adresse certaines des préoccupations que nous avons reçues des forces de l'ordre. Il y avait trop d'informations qu'ils demandaient qui devaient passer par des parties contractantes. Steve en avait parlé d'ailleurs. Je pense que c'est pour cela, lorsque nous avons discuté de cela, on avait reçu des informations de la part des forces de l'ordre sur ces questions de transparence. Il y avait donc des préoccupations sur ce sujet – une personne spécifique dans les forces de l'ordre qui avait besoin de telle ou telle information sur telle ou telle personne qui était connue d'un bureau d'enregistrement, etc.

BENEDICT ADDIS : Nous avons une considération que nous avons signalée pour vous en ce moment. Nous voulons parler du fait que toutes les requêtes passent par l'ICANN ou alors il faudrait qu'il y ait plus de divulgation aux parties contractantes ou moins de divulgation. Il va y avoir besoin d'une discussion sur l'élaboration de ces systèmes, est-ce que les requêtes vont être limitées ou pas vis-à-vis des parties contractantes pour savoir

vraiment qui fait la demande et pour pouvoir éviter comme cela la responsabilité. Mais cela va bien au-delà de notre travail.

Il y a un autre avantage. Au niveau de la transparence, lorsque les services sont centralisés, cela permet à la connexion d'être plus transparente. Cela, c'est une bonne chose.

KLAUS STOLL : Un commentaire pour vous et une suggestion. Pour votre élément numéro six au niveau de la transparence, vous devriez peut-être mentionner la recherche académique parce que beaucoup de personnes seraient très intéressées. Cela va au-delà des statistiques. Ce serait bon de le mentionner je pense.

RAM MOHAN : Merci beaucoup. Nous allons en prendre note et nous allons y réfléchir durant nos discussions.

VITTORIO BERTOLA : Ma question était similaire à celle qui a été posée. Je me demandais pourquoi vous voulez que tout cela soit décentralisé, surtout quand il s'agit d'un choix technique. Donc c'est une décision technique. Est-ce que c'est technique ou politique ? D'une façon technique, si je dois construire quelque chose comme cela, je pense que quelque chose de décentralisé

fonctionnerait mieux, quelque chose de décentralisé vers les parties contractantes. On peut discuter de ces propositions si vous voulez.

Mais d'autre autre côté, quand vous parlez des politiques, vous voulez vous assurer que vous avez toutes les données pour être conforme par rapport aux politiques. Mais dans votre présentation, vous avez dit que vous ne savez pas ce qui fonctionnera le mieux par rapport aux politiques ou pas. Donc voilà, je suis perdu. On essaie de résoudre un problème technique avec la meilleure solution technique ou alors vous avez des exigences politiques qui vous font obstacle ? Il faut vraiment discuter de cela.

GAVIN BROWN : Oui, c'est vrai que dans certaines de ces réponses, il y a un petit peu des questions politiques. Donc il faut faire baisser la complexité technique du système, que les parties contractantes fassent des mises à jour des politiques et comprennent bien le langage des politiques. Cela est compliqué. C'est une chose à faire qui serait terriblement compliquée et technique. On essaie de simplifier le système.

Et comme je l'ai dit tout à l'heure – et on a mis cela dans le document d'ailleurs –, nous voulons que les parties

contractantes utilisent seulement un TLS et nous faisons donc du contrôle d'accès en utilisant un jeton que le client reçoit de la part des parties contractantes et cela élève la barre pour ce que les parties contractantes doivent faire.

ALEX DEACON : J'ai une question qui est liée à la question de Ruben. Il s'agit des exigences du système par rapport à l'identification des informations. C'est clair que cela a à voir avec la politique plus qu'avec la technologie. Mais si la décision a déjà été prise que le modèle numéro deux sera celui qui sera choisi, ce modèle décrit l'ICANN en tant que la seule entité qui pourra décider. Dans ce cas-là, pouvez-vous nous donner un peu de contexte ? Pourquoi est-ce que ces exigences, bonnes ou pas, ont été mises en place ? Comment avez-vous décidé de cela ?

ANDY NEWTON : Les nouvelles exigences du système doivent pouvoir permettre de faire cela, d'avoir des identités ou attributs de la personne qui fait la demande et doivent pouvoir supporter la demande vis-à-vis de parties contractantes. Et cela relève des politiques, bien sûr. Là, il s'agit d'une caractéristique du système dans laquelle la politique doit être en place et le système ne peut pas soutenir cela.

ALEX DEACON : Si la politique décide que cela passe par le proxy de l'ICANN... Attendez, le système le supportera ou pas ?

ANDY NEWTON : Oui, c'est pour cela que nous avons les quatre modèles différents. Nous ne savons pas encore quel modèle sera correct et celui qu'on va utiliser. C'est pour cela qu'on les a décrit de la façon dont on l'a fait.

NEAL MCPHERSON : Je parle des données historiques. Le processus est décrit comme un processus qui n'est pas en temps réel. On a parlé des plaintes... Est-ce qu'il y a une date butoir ? Quand on parle des données, est-ce qu'on parle de données en temps réel ? Il y a beaucoup de requêtes que l'on reçoit qui sont basées sur le fait de qui est le propriétaire du nom de domaine.

RAM MOHAN : Je ne vous ai pas entendu. Pouvez-vous vous rapprocher du micro parce qu'on n'a pas bien entendu votre question.

NEAL MCPHERSON : Quand il s'agit du délai, vous savez, une requête peut prendre du temps, comment est-ce que vous établissez la chronologie sur le fait que vous allez délivrer certaines données ou pas ? Est-ce que cela va être en temps réel ? On a beaucoup de requêtes par exemple pour les données historiques. Comment est-ce que cela fonctionne par rapport à votre processus ? Si on vous dit : « J'ai besoin de données qui date de six mois. », comment vous allez faire ?

ANDY NEWTON : Je travaille pour ARIN et nous avons quelque chose qui s'appelle WHOWAS, donc qui était, au passé, quand on nous demande des choses qui datent d'il y a six mois. On a développé un service qui s'appelle WHOWAS. Et cela nous complique un peu la vie et on n'est pas très sûrs si cela correspond à notre mission de travail. Nous avons discuté de cela mais nous nous sommes dit : « On va mettre cela de côté pour l'instant. » Est-ce que cela répond à votre question ?

RAM MOHAN : Prochaine question.

GREGORY MOUNIER : Greg Mounier d'Europol. J'ai une question sur une autre caractéristique qui est toujours utilisée par les investigateurs lorsqu'ils font des recherches, la recherche inverse. Il faut pouvoir identifier tous les domaines qui ont été enregistrés avec le nom du titulaire, l'adresse, etc. Et techniquement, cela était possible, cela a été élaboré mais pour une raison ou pour une autre, je n'ai pas toujours compris, le TSG n'a pas fini de l'élaborer. Qu'est-ce que ça va prendre pour que vous puissiez décider à inclure cela dans l'ampleur de votre travail ? Qu'avez-vous décidé ?

ANDY NEWTON : Oui, ce n'est pas inclus parce que la recherche inverse ne fait pas partie de notre travail en ce moment. Il y a donc une version préliminaire qui a été faite par l'IETF et on va en discuter à Prague dans deux semaines. Cela n'a jamais fait partie de la base du travail du RDAP.

Ce projet comprend les éléments qui nous permettent d'obtenir les données de telle ou telle partie. Mais c'est pour cela que ce n'est pas couvert par le projet.

GREGORY MOUNIER : Ce serait bon de le faire, au moins de noter qu'on l'a considéré mais qu'on ne l'a pas encore fait.

RAM MOHAN : Merci. Restez au micro, on va vous en reparler.

Il est 14:46. Le 11 mars 2011 à 14:46 heure locale, un séisme de magnitude 9.0 a frappé la côte pacifique du nord-est de l'île japonaise Honshu. Le séisme connu comme le grand séisme de l'est du Japon a généré un violent tsunami avec des vagues atteignant jusqu'à 40 mètres qui ont pénétré jusqu'à 10 kilomètres à l'intérieur des terres. Ce fut le séisme le plus fort jamais enregistré au Japon et le quatrième séisme le plus violent au monde.

Environ 20 000 personnes sont mortes et près de 500 000 personnes ont été forcées d'évacuer les lieux. En souvenir de tous ceux qui ont perdu leur vie ou qui ont été affectés par le violent séisme qui a frappé la côte est du Japon, nous allons maintenant observer une minute de silence.

Merci. Voulez-vous répondre et faire le suivi de la question ?

ANDY NEWTON : Oui. Attendez, je ne me souviens plus de la question.

GREGOY MOUNIER : C'était juste une déclaration. Ce serait dommage si techniquement ce n'est pas possible si la politique dit que ce l'est.

ANDY NEWTON : Oui. Dans l'avenir, je pense qu'on va pouvoir l'utiliser. C'est plutôt une question de politique. Il y a quand même des détails techniques à régler mais bon, dans l'avenir, si la communauté décide que le besoin se fait sentir, ce sera fait.

SÉVERINE WATERBLEY : Bonjour. Je m'appelle Séverine Waterbley de la Belgique et je suis membre au GAC. Si je vous comprends bien, ICANN sera le processeur du RGPD. Et les services d'autorisation seront les processeurs. Donc est-ce qu'il y a une relation contractuelle entre les opérateurs de registre et les fournisseurs de service pour nous donner une autorisation ou une authentification ?

RAM MOHAN : C'est une très bonne question mais nous ne sommes pas qualifiés pour vous répondre là-dessus. Par contre, ce qu'on va faire pour nous assurer que cette question n'est pas perdue, c'est enregistré, nous allons en prendre note et nous allons

passer cela aux personnes qui se préoccupent de ce sujet à ICANN Org.

BENEDICT ADDIS : Je vais mettre ma casquette EPDP. Nous avons beaucoup parlé sur la nature exacte de l'accord juridique entre l'ICANN et les parties contractantes. Et je sais que le service juridique de l'ICANN a fourni son accord par rapport à cette question. Donc voilà. Encore une fois, dans 40 minutes, nous pourrons parler de ces questions avec la réunion du EPDP dans cette même salle.

TIM CHEN : Merci pour le travail que vous avez effectué. Je crois que cela représente un réel service étant donné le niveau technique de cet enjeu. Je sais que vous êtes tous bénévoles, donc merci.

Alors deux questions techniques. Tout d'abord, il y avait une note en bas d'une diapositive sur les considérations qui parlait des requêtes à usage multiple. J'aimerais bien savoir ce que cela veut dire. C'était dans une section du début, il y avait 13 considérations, voilà. Requêtes à usage multiple, qu'est-ce que cela veut dire ?

RAM MOHAN : Oui. Alors cela, c'était au début dans notre travail. Ce que les gens prenaient en compte, c'est la demande de données qui peut avoir différentes formes. Cela peut être une partie qui est autorisée à un accès à un élément de données une seule fois. Et dans d'autres cas, cela peut être une autorisation qui est plus longue mais également plus longue pour une catégorie de requête ou alors qui donne accès uniquement à certains éléments de données.

Donc ce qui n'était pas clair pour nous à ce moment de nos discussions, qu'il faille restreindre le modèle et qu'on traite uniquement une requête une fois par élément de données ou une fois par sujet, est-ce que cela devait être éphémère, est-ce que cela devait être persistant ou répétitif ; donc c'était cela, la question par rapport aux requêtes multiples.

TIM CHEN : Très bien. Le service bootstrap a été mentionné hier dans la séance que vous avez organisée avec les parties contractantes et vous l'avez rementionné aujourd'hui. J'ai essayé de regarder le RFC là-dessus et je crois que nous avons clarifié avec la question de Greg que ce n'est pas quelque chose... Hier, on parlait d'atteinte transversale de toutes les parties contractantes. Je ne sais pas si c'est cela mais le service

bootstrap, l'objectif, c'est de voir quelles sont les sources faisant autorité auxquelles il faudrait revenir.

Donc un petit commentaire par rapport au bootstrap, Scott l'a mentionné, est-ce que ce service traitera des requêtes d'informations en dehors de simplement les noms de domaine gTLD, ces données-là ? Est-ce que vous pourriez nous donner des détails là-dessus ?

SCOTT HOLLENBECK : Oui. Alors il y a plusieurs choses qui sont possibles. Nous avons un petit peu rigolé du fait de savoir si : « Ah, ce serait bien si internic.net nous fournissait des services utiles. Ce serait pas mal. » Mais au-delà de cela, comment est-ce que cela évoluera au fil du temps ? Et bien cela dépendra de la coordination et de la mise en œuvre des politiques. Mais en théorie, ce que vous proposez est tout à fait possible.

ANDY NEWTON : Par rapport à cela, j'aimerais ajouter quelque chose. Il est tout à fait probable qu'il y aura des personnes qui seront des clients qui ne souhaitent pas passer par le processus bootstrap eux-mêmes. Ils vont utiliser Kurl ou Bash et ils vont avoir une source de bootstrap qu'ils vont choisir et je pense que ce sera l'ICANN

probablement. Et dans ce cas, ce serait bien que l'ICANN soit un serveur bootstrap avec l'IANA.

RAM MOHAN : Merci.

ORATEUR NON-IDENTIFIÉ : Une petite observation. Je crois que la seule partie qui a été exclue finalement de ce modèle et du EPDP, c'est en fait l'utilisateur final. Je sais que vous avez des cas d'utilisation qui vous permettent de vérifier vos propres données. Mais ce modèle, en tout cas c'est mon point de vue, vous savez, c'est le canarie dans la mine qui est sacrifié, l'utilisateur final. Moi, je n'appartiens à aucun groupe, je suis simplement une utilisatrice finale et il est finalement malheureux qu'on se retrouve dans cette situation. Je pense qu'li faut lutter dans ce sens. On est toujours exclus, on a toujours le pire des résultats pour nous. Et les parties trouvent des mécanismes pour extraire les données qu'elles souhaitent avec des restrictions, grâce à des moyens juridiques, des autorisations. Mais nous sommes les seuls qui finalement sommes exclus et cela, c'est malheureux. Pour moi, c'est quelque chose contre quoi il faut vraiment lutter, et ce n'est que le début.

RAM MOHAN : Merci. Mais c'est une question assez étrange à nous présenter à nous parce que si vous revenez en arrière, si vous écoutez les enregistrements, si vous lisez les transcriptions, vous verrez que dans nos discussions, nous avons passé beaucoup de temps à justement prendre en compte le point de vue de l'utilisateur final qui présente une requête. Et même s'il y a des cas d'utilisation, vous avez cinq cas d'utilisation qui sont dans notre résumé mais en fait, il y a eu beaucoup de discussions sur l'utilisateur final. Et d'ailleurs, le principe dont parlait Andy, *keep it simple*, que les choses soient simple, ne pas avoir tout un tas de services pour que les utilisateurs finaux ne soient pas forcés à s'adresser à différents services pour avoir les informations, c'était justement notre objectif, de nous assurer que l'expérience de l'utilisateurs final soit prioritaire.

En tout cas de mon point de vue, je pense que les utilisateurs finaux ont vraiment été pris en considération pas nous. Mais certes, dans le cadre du processus général, je suis d'accord. Tous, nous devons vraiment considérer les besoins et les exigences des utilisateurs finaux.

Je vois que Steve a la main levée.

STEVE CROCKER : J'aimerais avoir des détails par rapport à votre question. C'est quoi le problème en fait ? Un titulaire de nom de domaine peut se rendre dans son compte avec le bureau d'enregistrement et trouver toutes informations et les vérifier. Il y a un accès direct. Donc je ne comprends pas vraiment quel est le problème dont on parle, qu'est-ce qui est significatif en termes de soutien de l'utilisateur final.

RAM MOHAN : Et Benedict vient de me dire que peut-être vous parlez de la personne concernée plutôt que de l'utilisateur final.

ORATEUR NON-IDENTIFIÉ : Oui, tout à fait.

RAM MOHAN : Donc il s'agit du cas d'utilisation numéro cinq.

ORATEUR NON-IDENTIFIÉ : Avant, je ne connaissais pas le WHOIS. Maintenant que je sais que le WHOIS existe, j'aurais pu l'utiliser, j'aurais voulu l'utiliser. La femme du GAC française qui a posé sa question essayait justement de promouvoir l'accès des utilisateurs finaux aux informations des sociétés. Cela, c'est une chose qui est très

importante pour nous. Et je crois que la solution aurait pu être – pour nous, cela aurait été le centre de tout ceci – de développer l'utilisation du WHOIS pour nous comme protection et non pas de l'éliminer.

BENEDICT ADDIS : Bon, maintenant que les termes sont clairs et qu'on n'est pas perdus, encore une fois, je vais m'exprimer au nom du EPDP. Je serais très triste de voir un système tel que celui-ci se transformer en club privé avec des gens qui sont passés par les différents niveaux d'approbation.

Mais je crois que le modèle est suffisamment flexible – et encore une fois, si la communauté décide qu'on l'utilise de cette manière. Et je pense que les utilisateurs finaux pourront justement avoir accès à ce qu'ils ont besoin de trouver.

ORATEUR NON-IDENTIFIÉ : C'est un commentaire qui est en fait lié à ce dont on parle. Donc dans votre rapport au 4.1, l'utilisateur, son cheminement en fait, je ne comprends pas vraiment comment vous le décrivez. Pourtant, j'utilise le WHOIS depuis très longtemps.

Le deuxième point, je l'ai lu plusieurs fois et je crois qu'on pourrait apporter certaines améliorations à ce cheminement de

l'utilisateur pour vraiment le mettre dans le contexte de l'utilisateur du WHOIS ou du RDS. Je ne sais pas ce qu'on décidera à la fin en termes de nom du service mais parlons de l'utilisateur, qui est-il, quel est son cheminement, le définir de manière claire. Mettez-vous vraiment à la place de la personne qui souhaite trouver des informations au sein du RDS.

RAM MOHAM : Merci beaucoup pour votre commentaire, c'est très utile.

Nous en sommes pratiquement à la fin de notre réunion. Ce que j'aimerais faire, c'est faire passer le micro aux différents membres du groupe d'études techniques pour des petits commentaires de conclusion. Je vais commencer par Scott.

SCOTT HOLLENBECK : Merci. Vous savez, il s'agit là d'une consultation. Nous avons proposé quelque chose, nous pensons que cela peut fonctionner mais nous sommes très intéressés par vos commentaires, par ce que vous avez à dire, donc n'hésitez pas.

ANDY NEWTON : Je souhaite faire écho au commentaire de Scott. Ce qui nous intéresse, c'est votre point de vue donc envoyez vos commentaires. Merci. Nous en parlerons ensemble.

BENEDICT ADDIS : Et bien, c'est une équipe extraordinaire. C'est tout ce que j'ai à dire, merci à tous, merci d'être venus nous écouter.

JORGE CANCIO : Je voudrais simplement dire merci pour vos commentaires. Nous apprécions beaucoup.

JODY KOLKER : Je n'ai rien à ajouter. Merci.

GAVIN BROWN : Il y a une petite chose que j'aimerais ajouter sur la base d'un commentaire fait précédemment, l'utilisation des données d'enregistrement en ce qui concerne la protection des consommateurs.

Je crois qu'une des choses extraordinaires par rapport au RDAP, c'est que les données d'enregistrement deviennent beaucoup plus accessibles par rapport au Port 43. Si vous utilisez une application avec Java et si vous par exemple vous créez une application pour un téléphone mobile, en principe, les données Port 43, c'est très difficile, très compliqué d'y accéder. Donc les données sont fournies de manière adjacente.

Je crois que l'adoption – et certes, cela n'est pas directement lié au travail du TSG – mais je crois que nous avons là le potentiel d'activer un certain nombre d'avantages pour les consommateurs qui souhaitent justement avoir davantage confiance dans les identificateurs qu'ils utilisent parce que cela permettra aux informations clés des noms de domaine, des autres ressources que le RDAP rend disponibles d'être justement disponibles beaucoup plus facilement pour l'utilisateur final. Moi, ce que j'imagine, c'est une extension de navigateur où on peut cliquer sur la barre de l'adresse et qui vous permet immédiatement d'avoir les données affichées sur le navigateur sans devoir passer par un système Port 43 compliqué. Cela peut être très utile, on peut avoir par exemple le système de cache de sécurité qui vraiment garantit l'intégrité du système.

TOMOFUMI OKUBO : Merci d'être restés jusqu'à la fin de la séance. Tout le monde n'est pas resté jusqu'à la fin.

STEVE CROCKER : Même chose par rapport à ce qui a été dit. Merci. Diana ? Eliza ?

JOHN CRAIN : Juste une dernière chose. Vraiment, je souhaite remercier cette équipe. En tant qu’ingénieurs, on n’aime pas avoir à bâtir un système sans exigence et c’est justement ce que nous avons dû faire et je trouve que le travaille qui a été effectué est absolument fantastique. Ces gens-là sont des bénévoles, comme vous, et ils ont dû bâtir quelque chose que j’espère est agnostique aux politiques. Mais je pense qu’il survivra et qu’au cours des années à venir, cela sera très utile. Vous avez vraiment fait un travail extraordinaire face à un enjeu difficile.

RAM MOHAN : La séance est terminée. Je vous remercie tous d’y avoir participé.

[FIN DE LA TRANSCRIPTION]