Conseil de la radiodiffusion et des télécommunications canadiennes
Canadian Radio-television and Telecommunications Commission

Décision de Conformité et Enquêtes et de Télécom CRTC 2021-267

Version PDF

Ottawa, le 5 août 2021

Dossier public : 8638-M75-202008953

Mitel Networks Corporation – Demande au Conseil d'ordonner à l'Autorité canadienne de gouvernance des jetons sécurisés de permettre à tous les fournisseurs de services de télécommunication de recevoir un certificat relatif aux normes STIR/SHAKEN

Le Conseil détermine que le refus de l'accès aux certificats de téléphonie sécurisée à tous les fournisseurs de services de télécommunication (FST) qui n'ont pas un accès direct aux ressources de numérotation n'est ni nécessaire ni approprié, et que cet accès ne devrait être refusé que s'il y a lieu de croire qu'on ne peut pas faire confiance à un FST pour maintenir l'intégrité des normes STIR/SHAKEN. Par conséquent, le Conseil s'attend à ce que l'Autorité canadienne de gouvernance des jetons sécurisés crée, en collaboration avec les FST actuellement inadmissibles et dans les 60 jours suivant la date de la présente décision, des exigences d'admissibilité qui reflètent les conclusions du Conseil dans la présente décision.

Introduction

1. Dans la décision de Conformité et Enquêtes et de Télécom 2018-32, le Conseil a déterminé que les fournisseurs de services de télécommunication (FST) devraient mettre en œuvre les normes STIR/SHAKEN[1] sur la partie de voix sur protocole Internet (IP) de leurs réseaux afin de réduire la mystification de l'identité de l'appelant. Dans la décision de Conformité et Enquêtes et de Télécom 2019-402-2, le Conseil a fixé la date de mise en œuvre au 30 juin 2021. Dans la décision de Conformité et Enquêtes et de Télécom 2021-123, le Conseil a imposé à tous les FST l'obligation de mettre en œuvre les normes STIR/SHAKEN à titre de condition d'offre et de prestation de services de télécommunication en vertu des articles 24 et 24.1 de la *Loi sur les télécommunications* (*Loi*). La date d'entrée en vigueur de cette obligation a été fixée au 30 novembre 2021.

[1] STIR signifie Secure Telephony Identity Revisited (nouvelle approche relative à la sécurité de l'identité de l'appelant). SHAKEN signifie Signature-based Handling of Asserted information using toKENs (traitement de l'information fournie en fonction de la signature au moyen de jetons). Ces normes sont un ensemble de protocoles et de procédures conçus pour lutter contre la mystification de l'identité de l'appelant par l'authentification et la vérification de l'information d'identification de l'appelant.

2. Dans la décision de Conformité et Enquêtes et de Télécom 2019-403, le Conseil a approuvé l'établissement de l'Autorité canadienne de gouvernance des jetons sécurisés (ACGJS) en tant qu'autorité de gouvernance dans le cadre de la mise en œuvre des normes STIR/SHAKEN. Il incombe à l'ACGJS de gérer les certificats de sécurité de l'identité de l'appelant qu'utilisent les FST pour valider numériquement les authentifications des appels. Selon le modèle défini par l'Alliance for Telecommunications Industry Solutions (ATIS)[2], le cadre de gouvernance comprend également un administrateur des politiques, lequel est choisi par l'autorité de gouvernance et est chargé d'appliquer ses règles, et une autorité de certification, qui délivre des certificats de sécurité de l'identité de l'appelant.

3. L'ACGJS a établi des critères pour que les FST puissent devenir actionnaires de l'ACGJS et obtenir des certificats de sécurité de l'identité de l'appelant[3]. Selon ces critères, seuls les FST qui ont un accès direct aux ressources de numérotation canadiennes de l'Administrateur de la numérotation canadienne (ANC) [FST admissibles] ont accès aux certificats de sécurité de l'identité de l'appelant.

4. Par conséquent, les FST qui obtiennent des numéros auprès d'un fournisseur de services de numéros de téléphone (FSNT) plutôt qu'auprès de l'ANC (FST inadmissibles) ne peuvent pas authentifier, selon les normes STIR/SHAKEN, les appels provenant de leurs réseaux. Les appels provenant de FST inadmissibles ne seraient authentifiés que lorsqu'ils atteignent un FST admissible qui, n'ayant pas de relation directe avec l'appelant, ne pourrait pas attribuer à ces appels le niveau d'authentification le plus élevé.

5. L'ATIS définit trois niveaux d'attestation qui peuvent être attribués aux appels[4]. Avec une attestation complète (niveau A), l'appelant est authentifié et est autorisé à utiliser le numéro de l'appelant. Avec l'attestation partielle (niveau B), l'origine de l'appel est authentifiée, mais pas l'autorisation de l'appelant à utiliser le numéro de l'appelant. Avec l'attestation de passerelle (niveau C), un FST peut authentifier l'endroit dans son réseau qui a reçu l'appel, mais il ne peut pas en authentifier la source. Un appel provenant d'un FST inadmissible ne recevrait probablement qu'une attestation de niveau B ou de niveau C.

6. L'ACGJS et le Groupe de travail Réseau du Comité directeur du CRTC sur l'interconnexion (CDCI) étudient actuellement des moyens de s'assurer que les appels provenant de FST inadmissibles sont correctement authentifiés.

7. L'une des solutions proposées consiste à utiliser la norme du certificat de délégué[5] élaborée par l'ATIS. Avec cette solution, un FST inadmissible serait en mesure

---

[2] Voir ATIS-1000080 (en anglais seulement).

[3] Ces critères sont définis dans le guide des politiques de l'ASGJS (en anglais seulement).

[4] Voir ATIS-1000074 (en anglais seulement).

[5] Voir ATIS-1000092 (en anglais seulement).

d’obtenir un certificat de délégué, valable pour un numéro de téléphone précis, auprès du FSNT duquel il a acheté ce numéro[6].

Demande

8. Le 21 décembre 2020, Mitel Networks Corporation (Mitel) a déposé une demande dans laquelle elle demandait au Conseil d’ordonner à l’ACGJS de permettre à tous les FST d’être en mesure de recevoir des certificats de sécurité de l’identité de l’appelant directement auprès de l’ACGJS.

9. Mitel est un revendeur de services de télécommunication et n’a pas d’accès direct aux ressources de numérotation. Par conséquent, Mitel n’a pas de droit d’accès aux certificats de sécurité de l’identité de l’appelant.

10. Mitel a fait remarquer que le Conseil a exigé de tous les FST qu’ils mettent en œuvre les normes STIR/SHAKEN, mais que les conditions d’admissibilité de l’ACGJS empêchent Mitel et d’autres FST inadmissibles de se conformer efficacement, ou de se conformer tout court, à cette condition, ce qui nuit à la mise en œuvre efficace des normes STIR/SHAKEN.

11. En ce qui concerne la norme proposée pour les certificats de délégué, Mitel a relevé trois problèmes principaux. Tout d’abord, la norme telle qu’elle est actuellement définie entraînerait l’évolution constante de milliers de certificats de délégué provenant de plusieurs FSNT. Deuxièmement, il n’y a pas de calendrier imposé pour la mise en œuvre des certificats de délégué par les FSNT, de sorte que l’on ne sait pas combien de FSNT mettraient en œuvre le soutien pour les certificats de délégué, ni quand ils le feront ou à quel coût. Troisièmement, l’utilisation de certificats de délégué réduirait les options pour des services de terminaison d’appel rentables, de haute qualité et hautement disponibles, car les FST inadmissibles seraient tenus d’envoyer tous leurs appels d’origine aux entreprises qui soutiennent les relations de délégation.

12. Mitel a indiqué comprendre que l’autorité de certification actuelle promeut activement la solution de l’autorité déléguée comme source de revenus pour les FST.

13. Mitel a souligné qu’à ce jour, aucun travail important n’a été effectué pour trouver d’autres solutions et aucune norme n’a été publiée. Par conséquent, Mitel estime que les FST inadmissibles seront nettement désavantagés par rapport aux FST admissibles, puisqu’ils n’auront le choix qu’entre un accès limité et coûteux aux certificats de délégué ou l’attribution d’un faible niveau d’authentification aux appels provenant de leurs réseaux.

---

[6] Cette norme de certificat de délégué peut être utilisée par les FST inadmissibles et par d’autres entités qui ne sont pas des FST et qui achètent des numéros de téléphone en gros auprès de FSNT, comme les grandes entreprises et les centres d’appels.

14. Mitel a fait valoir que le fait de permettre à tous les FST canadiens de devenir membres de l'ACGJS améliorerait la gouvernance parce que ses décisions refléteraient l'ensemble de l'industrie, et que l'inclusion de FST supplémentaires répartirait plus uniformément le coût de la gouvernance.

15. Mitel a fait remarquer que la décision de l'ACGJS sur les critères d'admissibilité a sans doute été prise dans le but de concevoir un modèle similaire à celui des États-Unis, étant donné la nature intégrée du réseau téléphonique nord-américain. Aux États-Unis, cependant, le critère d'admissibilité a été étendu, et Mitel ne voit aucune raison de ne pas l'étendre pour les FST canadiens.

16. Le Conseil a reçu des interventions de la part de Bell Canada; du Canadian Voice Peering Project; de Distributel Communications Limited (Distributel); du chapitre canadien de l'Internet Society (ISCC); ainsi qu'une intervention conjointe de Microsoft Corporation, RingCentral Inc. et 8X8 inc. (Microsoft et autres); de M. Marc Nanni; des Opérateurs des réseaux concurrentiels Canadiens; de Rogers Communications Canada Inc. (RCCI); de Saskatchewan Telecommunications (SaskTel); de Shaw Communications Inc. (Shaw); de TekSavvy Solutions Inc. (TekSavvy); et de TELUS Communications Inc. (TCI).

Le Conseil devrait-il demander à l'ACGJS de permettre à tous les FST d'être en mesure de recevoir des certificats de sécurité de l'identité de l'appelant directement auprès de l'ACGJS?

Positions des parties

Microsoft et autres

17. Microsoft et autres ont réaffirmé les arguments de Mitel et ont également fait remarquer que l'ACGJS n'a pas fourni de raisons techniques ou stratégiques d'exclure certains fournisseurs. Microsoft et autres ont expliqué que, d'un point de vue technique, rien n'empêche les FST inadmissibles d'authentifier et de valider les appels provenant de leurs réseaux. Microsoft et autres estiment qu'en refusant aux FST inadmissibles l'accès aux certificats de sécurité de l'identité de l'appelant, les principes de neutralité concurrentielle et de promotion de la concurrence qui sous-tendent les Instructions de 2006 et de 2019 sont bafoués.

18. Se fondant sur leur expérience du déploiement des normes STIR/SHAKEN aux États-Unis, Microsoft et autres ont fait valoir que la suppression de la condition d'admissibilité de l'accès direct aux numéros de téléphone pour l'accès aux certificats de sécurité de l'identité de l'appelant dans ce pays a donné lieu à un cadre plus transparent, participatif et concurrentiel, car différents types de FST sont autorisés à participer aux activités de gouvernance.

19. Microsoft et autres ont également proposé d'étendre l'accès aux certificats de sécurité de l'identité de l'appelant aux FST qui i) sont inscrits auprès du Conseil en tant que fournisseurs autorisés de services téléphoniques locaux; ii) sont autorisés par le Conseil à fournir des services de télécommunication internationale de base en

provenance ou à destination du Canada; et iii) attribuent des numéros de téléphone à des abonnés au Canada, qu'ils soient obtenus directement ou par des intermédiaires.

ISCC

20. En ce qui concerne la concurrence loyale, l'ISCC a fait remarquer que les FST qui raccordent les appels pourraient traiter les appels provenant de FST inadmissibles avec méfiance comparativement à ceux provenant de FST admissibles, car ils ne disposeraient que d'une authentification de niveau B ou C. L'ISCC estimait que cette situation risque d'inciter les clients à confier leurs activités à un FST qui peut fournir une authentification de niveau A, ce qui se traduirait par un système de télécommunication à deux vitesses au Canada : des FST pouvant authentifier les appels et d'autres ne le pouvant pas.

21. L'ISCC a fait remarquer que, parce que les petits FST sont généralement interconnectés par IP à des entreprises en amont, ils sont mieux placés pour mettre en œuvre les normes STIR/SHAKEN; pourtant, la politique de délivrance des certificats de l'ACGJS les exclut de ce processus.

TekSavvy

22. TekSavvy, un FST admissible, a appuyé la demande de Mitel, indiquant que la solution du certificat de délégué est insuffisante pour répondre aux préoccupations des revendeurs de services téléphoniques.

TCI et SaskTel

23. TCI ne s'est pas opposée à la proposition selon laquelle les FST n'ayant pas d'accès direct aux numéros de téléphone devraient avoir accès aux certificats de sécurité de l'identité de l'appelant. Elle a toutefois estimé qu'un examen supplémentaire par le Conseil de tout FST ayant un tel accès est nécessaire afin de prévenir une exploitation abusive des normes STIR/SHAKEN. TCI a précisé que le FST de l'appelant est le mieux placé pour en authentifier l'identité et qu'il doit se porter garant des authentifications qu'il fournit, et que la solution du certificat de délégué présente des lacunes à cet égard. Elle a fait valoir que pour exploiter le plein potentiel des normes STIR/SHAKEN, tous les FST doivent être responsables de leurs propres certificats et aucun FST ne devrait authentifier les appels d'un autre FST. À cet égard, TCI a appuyé la position de Mitel selon laquelle les FST devraient pouvoir obtenir leurs propres certificats, sous réserve de conditions qui garantiraient l'intégrité du système.

24. Cependant, TCI s'est fermement opposée à la suggestion voulant que l'ACGJS agisse par intérêt personnel. Elle a affirmé que la nécessité de prendre des décisions rapides expliquait le nombre restreint de membres au départ, même si un nombre accru de membres aurait permis de mieux répartir le fardeau financier.

25. SaskTel a reconnu un certain mérite à la demande de Mitel, mais a souhaité que la demande soit mise en suspens et a proposé que le Conseil demande aux parties de résoudre les questions pendantes telles que la gouvernance, les exigences

d’exploitation, les normes et les sanctions, les mécanismes de mise en application et les conséquences de l’autorisation du trafic non approuvé.

26. Ni TCI ni SaskTel se sont opposées à ce que les FST inadmissibles aient accès à terme aux certificats de sécurité de l’identité de l’appelant. Elles ont toutefois précisé que cet accès devrait se faire dans le contexte de leur participation au cadre général d’application et d’exploitation des normes STIR/SHAKEN, qui doit encore être élaboré par l’ACGJS et approuvé par le Conseil.

Shaw, Bell Canada et RCCI

27. Shaw, Bell Canada et RCCI se sont opposées à la demande de Mitel. Tous les FST qui n’ont pas appuyé la demande de Mitel (FST opposés) invoquent essentiellement les mêmes arguments pour étayer leurs positions.

28. Les FST opposés ont fait valoir que la demande de Mitel était prématurée et ont invité Mitel à participer plus activement au processus de développement des normes STIR/SHAKEN. Tout comme Mitel, ils ont souligné que les normes, mécanismes et politiques en vue d’intégrer les FST inadmissibles sont en préparation, mais ils ont estimé qu’il s’agit d’une situation normale dans l’élaboration des normes STIR/SHAKEN. Ils ont fait valoir que le fait d’approuver la demande de Mitel empêcherait l’ACGJS d’établir le cadre qui s’impose et perturberait l’application ordonnée des normes STIR/SHAKEN. Ils ont affirmé que les efforts devraient porter sur l’établissement de bonnes bases sur lesquelles établir des capacités supplémentaires, telles que l’octroi aux revendeurs d’un accès direct aux certificats de sécurité de l’identité de l’appelant.

29. Les FST opposés ont insisté sur le fait qu’il est essentiel de mettre en œuvre un processus approprié afin d’intégrer tous les types de FST dans le cadre des normes STIR/SHAKEN. Pour que le cadre des normes STIR/SHAKEN atteigne ses objectifs, seules les entités à qui l’on peut faire confiance pour respecter les règles et directives des normes STIR/SHAKEN peuvent être autorisées à authentifier des appels.

30. RCCI et TCI ont fait remarquer le risque d’exploitation abusive du système de normes STIR/SHAKEN par des FST inadmissibles. Bien qu’elle ne se soit pas opposée à la demande de Mitel, TCI a fait remarquer que certains FST pourraient être incités à fournir une authentification de niveau A même s’ils ne peuvent pas vérifier que l’appelant a le droit d’utiliser l’identité de l’appelant présentée, parce que les clients pourraient autrement craindre que leurs appels ne soient pas pris en charge; cette situation poserait un risque sérieux pour l’intégrité du cadre des normes STIR/SHAKEN. TCI et RCCI ont toutes deux argué que ce risque d’exploitation abusive pourrait provenir de FST inadmissibles, et qu’un FST qui abuserait du système de cette manière pourrait facilement réapparaître sous un nouveau nom. Elles ont soutenu qu’un tel risque est sérieux, particulièrement dans un environnement dans lequel des réseaux virtuels infonuagiques peuvent être exploités par des FST qui n’ont aucune installation au Canada, contrairement aux FST actuellement admissibles qui ne peuvent pas facilement changer d’identité pour éviter de rendre des comptes.

31. RCCI a rappelé l'observation du Conseil, dans la décision de Conformité et Enquêtes et de Télécom 2018-32, selon laquelle les appels mystifiés proviennent principalement des services de voix sur protocole Internet (VoIP). RCCI a fait remarquer que l'ensemble de l'industrie doit déployer les normes STIR/SHAKEN pour perturber de tels appels, et que l'assouplissement des critères d'admissibilité compromettrait la sécurité des normes STIR/SHAKEN, qui vise à rétablir la confiance des Canadiens dans les renseignements sur l'identité de l'appelant. Elle a précisé que les fraudeurs auraient alors la capacité d'inonder le réseau téléphonique public commuté canadien d'appels importuns ou frauduleux ayant des numéros de téléphone falsifiés avec une authentification selon les normes STIR/SHAKEN.

32. D'après les FST opposés, Mitel exagère le préjudice que la politique d'accès actuelle causerait aux FST inadmissibles. Ils ont expliqué que, lorsque les normes STIR/SHAKEN seront appliquées, une infime partie des appels seulement, y compris ceux qui proviennent de FST ayant accès aux certificats de sécurité de l'identité de l'appelant, recevra une authentification de niveau A, et un nombre infime des téléphones des clients sera apte à afficher des renseignements liés aux normes STIR/SHAKEN.

33. En ce qui concerne les préoccupations de Mitel au sujet de la disponibilité et du coût des certificats de délégué, Shaw a précisé que, compte tenu du grand nombre de FST n'ayant pas d'accès direct aux numéros de téléphone, l'industrie ne fera pas abstraction de leurs besoins. RCCI a ajouté qu'il y aura suffisamment de concurrence entre les fournisseurs de certificats de délégué pour garantir des prix abordables. RCCI et Shaw ont souligné que les FST admissibles ont déjà beaucoup investi dans la mise en application des normes STIR/SHAKEN, et que tous les FST devraient s'attendre à devoir assumer une partie des coûts connexes, notamment par l'acquisition et l'administration de certificats de délégué.

34. RCCI a proposé que Mitel pourrait prendre les mesures nécessaires pour se qualifier en tant qu'entreprise de services locaux concurrente (ESLC), ce qui lui permettrait de recevoir des certificats de sécurité de l'identité de l'appelant.

Distributel

35. Distributel n'a pas pris position sur la demande de Mitel, mais a demandé que le Conseil émette sa conclusion le plus rapidement possible, puisque celle-ci se répercutera sur la manière dont les FST appliquent les normes STIR/SHAKEN.

Réplique de Mitel

36. Mitel s'est opposée à la suggestion de RCCI selon laquelle le fait de permettre aux FST sans installations canadiennes d'avoir un accès direct aux certificats de sécurité de l'identité de l'appelant irait à l'encontre des mesures de sécurité des normes STIR/SHAKEN. Mitel a fait remarquer qu'un FST qui donne des attestations inappropriées peut voir son certificat révoqué ou peut être sanctionné; de plus, un grand fournisseur peut tout aussi bien authentifier incorrectement les appels qu'un fournisseur de services VoIP locaux. En outre, Mitel a fait remarquer que plusieurs

FST inadmissibles mettent en jeu davantage de capitalisation boursière et de revenus commerciaux s'ils enfreignent les règles du CRTC que bien des FST admissibles.

37. Mitel a également fait valoir qu'il était inapproprié de juger de la fiabilité d'un FST selon le type de service qu'il fournit, comme l'a suggéré RCCI. Mitel était d'accord avec TCI que plus il y a de FST qui participent directement au cadre de normes STIR/SHAKEN, mieux le système fonctionnera. Une participation accrue facilitera le dépistage des appels en cas de comportements malveillants. Les politiques d'exclusion augmenteront la probabilité d'appels importuns, ce qui minera la confiance du public dans le système.

38. Mitel a indiqué qu'elle n'était pas opposée à l'imposition de conditions à la participation directe des FST au cadre de normes STIR/SHAKEN, pourvu que ces conditions soient appliquées de manière uniforme à tous les FST. Mitel a appuyé les trois conditions de participation directe qui ont été proposées par Microsoft et autres.

39. Mitel a rejeté la suggestion de RCCI selon laquelle, étant donné que Mitel a la possibilité de devenir une ESLC et d'avoir ainsi accès aux certificats de sécurité de l'identité de l'appelant, une conclusion du Conseil ne serait pas nécessaire.

40. Mitel a également rejeté l'argument des FST opposés selon lequel la demande est prématurée. Elle a indiqué qu'elle a essayé de discuter de cette question avec l'ACGJS et qu'elle a entretenu une correspondance à ce sujet, mais en vain. En outre, attendre que l'ACGJS ait élaboré de nouvelles politiques serait préjudiciable aux FST inadmissibles.

Résultats de l'analyse du Conseil

41. Le Conseil fait remarquer que, compte tenu des tentatives infructueuses de Mitel et d'autres entreprises pour résoudre le problème par le biais de discussions avec le CDCI et l'ACGJS, il semble peu probable que l'industrie s'entende sur une solution. Étant donné le degré élevé de coopération requis au sein de l'industrie pour l'application efficace des normes STIR/SHAKEN, le Conseil estime qu'il serait prudent d'établir des directives et de faciliter une résolution rapide de la question.

42. Le Conseil fait remarquer que les FST sont encouragés à adopter la solution des certificats de délégué, ou une solution de rechange, car les entreprises de services locaux auront besoin d'authentifier les appels sortants d'entités telles que les entreprises et les grandes organisations. Toutefois, à moins que le Conseil ne donne de directives précises à l'industrie concernant le développement de solutions incluant des FST inadmissibles, il est peu probable que de telles solutions soient suffisamment avancées pour garantir l'équité concurrentielle au moment où elles seront nécessaires.

43. Le Conseil estime que la politique de l'ACGJS en matière d'accès aux certificats de sécurité de l'identité de l'appelant pourrait mener à certaines contraintes empêchant les FST inadmissibles de se conformer à l'exigence du Conseil selon laquelle tous les FST doivent mettre en œuvre les normes STIR/SHAKEN, nonobstant le fait que les FST ne sont pas tous tenus de les mettre en œuvre de la même manière. Cependant,

les solutions de remplacement pour la mise en œuvre des normes STIR/SHAKEN sans accès direct aux certificats pourraient comporter d'importantes lacunes. Ces solutions ne sont pas encore disponibles, et leurs coûts sont inconnus. Dans tous les cas, le Conseil estime qu'une politique qui empêche toute une catégorie de FST d'accéder directement aux certificats de sécurité de l'identité de l'appelant, simplement en vertu du type de FST, pourrait entraîner un avantage concurrentiel pour les FST n'ayant pas cet accès. Le Conseil fait également remarquer que l'ACGJS n'a pas fourni de justification pour sa politique d'accès.

44. En ce qui concerne l'observation selon laquelle les appels mystifiés proviennent principalement de services VoIP[7], et le fait que de nombreux FST inadmissibles offrent de tels services, le Conseil conclut qu'il n'est pas approprié de juger de la fiabilité d'un FST selon le type de service ou de technologie qu'il fournit.

45. Quelle que soit l'origine des appels mystifiés, le Conseil est d'avis que toute taille ou tout type de FST peut authentifier incorrectement les appels. Par ailleurs, étant donné que la mystification de l'identité de l'appelant est plus courante sur les réseaux téléphoniques sur IP, les normes STIR/SHAKEN ont été créées pour traiter ce problème. Elles ne s'appliquent en fait qu'aux appels sur IP. Le Conseil fait remarquer que le fait de permettre à tous les FST d'authentifier les appels avec un certificat de sécurité de l'identité de l'appelant rendrait le FST de l'appelant directement garant des authentifications.

46. De plus, le Conseil fait remarquer que le petit nombre de circuits à fréquences vocales et d'interconnexion sur IP actuellement dans les réseaux de télécommunication canadiens constitue un obstacle important à un déploiement efficace des normes STIR/SHAKEN. Ainsi, la fourniture d'un accès aux certificats de sécurité de l'identité de l'appelant pour les FST qui peuvent générer du trafic IP sur le réseau téléphonique serait bénéfique au déploiement des normes STIR/SHAKEN, dans la mesure où les FST démontrent qu'ils respectent le cadre de ces normes.

47. En ce qui concerne les comparaisons entre la mise en œuvre des normes STIR/SHAKEN aux États-Unis et au Canada, le Conseil estime que, bien que la comparaison puisse être instructive, elle n'est pas directement applicable étant donné les différents cadres réglementaires des deux pays.

48. Le Conseil estime que les critères d'admissibilité actuels de l'ACGJS en matière d'accès aux certificats de sécurité de l'identité de l'appelant pourraient conférer un avantage concurrentiel aux FST qui ont un accès direct aux ressources de numérotation de l'ANC, et un désavantage concurrentiel correspondant aux FST qui n'ont pas cet accès, ce qui n'a pas été justifié au dossier de la présente instance.

49. Néanmoins, le Conseil estime que les conditions d'admissibilité pour l'accès aux certificats de sécurité de l'identité de l'appelant pourraient être appropriées, dans la

---

[7] Voir la décision de Conformité et Enquêtes et de Télécom 2018-32.

mesure où elles sont i) nécessaires pour maintenir l'intégrité des normes STIR/SHAKEN; et ii) particulièrement conçues pour atteindre cet objectif. Toutefois, compte tenu du peu de renseignements concernant cette question dans le dossier de la présente instance, le Conseil n'est pas en mesure d'aborder de tels critères pour le moment.

50. Le Conseil estime que la capacité d'authentifier entièrement les appels sortants deviendra une nécessité concurrentielle lorsque le traitement des appels authentifiés, c'est-à-dire par affichage et filtrage, sera plus avancé et plus largement disponible. Toutefois, comme la mise en œuvre des normes STIR/SHAKEN en est encore à ses débuts, le Conseil estime qu'il n'est pas urgent d'étendre l'accès aux certificats de sécurité de l'identité de l'appelant à tous les FST à compter de la date de la présente décision. Par conséquent, le Conseil estime qu'il serait approprié d'accorder 60 jours pour l'élaboration de conditions d'admissibilité qui permettraient à tous les FST d'obtenir l'accès aux certificats de sécurité de l'identité de l'appelant, sauf dans les cas où il est raisonnable d'estimer qu'on ne peut faire confiance au FST pour maintenir l'intégrité des normes STIR/SHAKEN.

Conclusion

51. Compte tenu de tout ce qui précède, le Conseil conclut que la politique actuelle consistant à refuser l'accès aux certificats de sécurité de l'identité de l'appelant à tous les FST qui n'ont pas un accès direct aux ressources de numérotation n'est ni nécessaire ni appropriée. Toute condition d'admissibilité pour l'accès aux certificats de sécurité de l'identité de l'appelant doit être spécifiquement adaptée afin que l'accès aux certificats de sécurité de l'identité de l'appelant ne soit refusé que lorsqu'il est raisonnable d'estimer que l'on ne peut pas faire confiance au FST pour maintenir l'intégrité des normes STIR/SHAKEN.

52. En outre, le Conseil s'attend à ce que l'ACGJS :

    i) élabore des conditions d'admissibilité qui empêchent l'accès aux certificats de sécurité de l'identité de l'appelant uniquement aux FST auxquels on ne peut faire confiance pour maintenir l'intégrité des normes STIR/SHAKEN, et ce, dans un délai de 60 jours;

    ii) collabore avec les FST inadmissibles à l'élaboration de nouveaux critères d'admissibilité pour l'accès aux certificats de sécurité de l'identité de l'appelant.

Instructions

53. Les Instructions de 2006[8] précisent que le Conseil, dans l'exercice des pouvoirs et fonctions que lui confère la *Loi*, doit mettre en œuvre les objectifs de la politique énoncés à l'article 7 de la *Loi*, conformément aux considérations qui y sont énoncées. Les Instructions de 2019[9] précisent que le Conseil doit préciser la manière dont ses décisions promeuvent la concurrence, l'abordabilité, les intérêts des consommateurs et l'innovation, le cas échéant.

54. Le Conseil estime que ses conclusions dans la présente décision, à savoir que les conditions d'admissibilité actuelles pour que les FST puissent avoir accès aux certificats de sécurité de l'identité de l'appelant ne sont pas appropriées, et que ces conditions d'admissibilité doivent être spécifiquement adaptées pour exclure uniquement les FST auxquels on ne peut pas faire confiance pour maintenir l'intégrité des normes STIR/SHAKEN, assureront une application neutre des normes STIR/SHAKEN sur le plan concurrentiel et favoriseront ainsi la concurrence. De plus, la décision du Conseil favorisera les intérêts des consommateurs, car elle assurera une application plus efficace des normes STIR/SHAKEN pour la protection des Canadiens contre le préjudice causé par les appels importuns. Par conséquent, le Conseil estime que sa décision favorise l'atteinte des objectifs de la politique énoncés aux alinéas 7a), 7c), 7f), 7g), 7h) et 7i) de la *Loi*[10].

Secrétaire général

Documents connexes

- *Mise en œuvre des normes STIR/SHAKEN pour les appels vocaux sur protocole Internet*, Décision de Conformité et Enquêtes et de Télécom CRTC 2021-123, 6 avril 2021

---

[8] *Décret donnant au CRTC des instructions relativement à la mise en œuvre de la politique canadienne de télécommunication*, DORS/2006-355, 14 décembre 2006

[9] *Décret donnant au CRTC des instructions relativement à la mise en œuvre de la politique canadienne de télécommunication pour promouvoir la concurrence, l'abordabilité, les intérêts des consommateurs et l'innovation*, DORS/2019-227, 17 juin 2019

[10] Les objectifs cités de la politique sont les suivants : 7a) favoriser le développement ordonné des télécommunications partout au Canada en un système qui contribue à sauvegarder, enrichir et renforcer la structure sociale et économique du Canada et de ses régions; 7c) accroître l'efficacité et la compétitivité, sur les plans national et international, des télécommunications canadiennes; 7f) favoriser le libre jeu du marché en ce qui concerne la fourniture de services de télécommunication et assurer l'efficacité de la réglementation, dans le cas où celle-ci est nécessaire; 7g) stimuler la recherche et le développement au Canada dans le domaine des télécommunications ainsi que l'innovation en ce qui touche la fourniture de services dans ce domaine; 7h) satisfaire les exigences économiques et sociales des usagers des services de télécommunication; 7i) contribuer à la protection de la vie privée des personnes.

- *Établissement de l'Autorité canadienne de gouvernance des jetons sécurisés*, Décision de Conformité et Enquêtes et de Télécom CRTC 2019-403, 9 décembre 2019

- *Groupe de travail Réseau du CDCI – État d'avancement de la mise en œuvre des mesures d'authentification et de vérification de l'identité de l'appelant par les fournisseurs de services de télécommunication*, Décision de Conformité et de Télécom CRTC 2019-402, 9 décembre 2019; modifiée par les Décisions de Conformité et de Télécom CRTC 2019-402-1, 13 décembre 2019; et 2019-402-2, 15 septembre 2020

- *Mesures pour réduire la mystification de l'identité de l'appelant et déterminer l'origine des appels importuns*, Décision de Conformité et Enquêtes et de Télécom CRTC 2018-32, 25 janvier 2018; modifiée par les Décisions de Conformité et Enquêtes et de Télécom CRTC 2018-32-1, 24 octobre 2018; et 2018-32-2, 18 décembre 2018