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

Décision de télécom CRTC 2022-264

Version PDF

Ottawa, le 26 septembre 2022

Dossier public : 8621-C12-01/08

Modification des Lignes directrices canadiennes relatives à l'échange de données et migration vers le protocole de Transport Layer Security 1.3

Sommaire

Le Conseil **approuve** le rapport de consensus BPRE096b concernant le formulaire d'identification de la tâche du Groupe de travail Plan de travail et les Lignes directrices canadiennes relatives à l'échange de données mises à jour, et **ordonne** aux fournisseurs de services de télécommunication de passer à l'utilisation du protocole Transport Layer Security 1.3 pour l'échange de données sur des liaisons Application Statement 2 au plus tard le **30 juin 2023**.

Introduction

Contexte

1. Les fournisseurs de services de télécommunication (FST) utilisent actuellement l'échange électronique de fichiers comme mécanisme permettant d'assurer l'efficacité des transferts de clients et de sécuriser l'échange de diverses données utilisées à l'appui d'autres services tarifés et services faisant l'objet d'une abstention de la réglementation, tel que le service de fichiers d'échange d'inscriptions ordinaires, les registres d'appels sans frais, les demandes de service local, les annulations de service et les demandes d'entreprise intercirconscription de base. À l'exception de certains échanges de fichiers à faible volume, les échanges bilatéraux de fichiers entre les FST utilisent des liaisons Application Statement 2 (AS2) comme mécanisme standard. Le protocole AS2 est compatible avec diverses plateformes d'entreprise à entreprise et de la communauté des fournisseurs d'infrastructure de télécommunication.

2. Le 16 octobre 2017, le Groupe de travail Plan de travail (GTPT) a présenté le rapport BPRE096a concernant le formulaire d'identification de la tâche (FIT), intitulé *Readiness of Canadian Carriers to Implement Enhanced Transport Layer Security via AS2* (état de préparation des entreprises canadiennes relativement à la mise en œuvre du protocole amélioré Transport Layer Security par l'intermédiaire du protocole AS2) [en anglais seulement]. Dans le rapport, le GTPT a souligné l'objectif du protocole Transport Layer Security (TLS) sur des liaisons AS2 de transfert électronique de fichiers entre FST, ainsi que la raison d'être de l'augmentation du niveau de sécurité du protocole TLS. Le GTPT a conclu que la norme TLS 1.3 n'était pas encore à un stade d'achèvement permettant une mise en

œuvre aux fins d'utilisation au Canada, et qu'une telle mise en œuvre ne serait pas possible avant un à trois ans.

3. Le Conseil a approuvé le rapport BPRE096a du FIT dans la décision *Groupe de travail Plan de travail du CDCI – Rapport de consensus BPRE096a concernant l'état de préparation des entreprises canadiennes relativement à la mise en œuvre du protocole Transport Layer Security par l'intermédiaire du protocole Applicability Statement 2*, Décision de télécom CRTC 2018-62, 15 février 2018 (décision de télécom 2018-62). Dans cette décision, le Conseil a avisé les entreprises et d'autres intervenants de se préparer à mettre en œuvre les améliorations en matière de sécurité à venir prévues dans la version 1.3 de la norme TLS et de prévoir un budget pour leur mise en œuvre.

Rapport

4. Le 14 juin 2022, le Comité directeur du CRTC sur l'interconnexion (CDCI) a transmis au Conseil, pour approbation, le rapport de consensus BPRE096b du FIT du GTPT (Rapport) en vue de modifier la version 5 des Lignes directrices canadiennes relatives à l'échange de données (BPGLDI50) [Lignes directrices]. Les modifications aux Lignes directrices visent à renforcer la sécurité de la transmission des données entre les FST en adoptant la plus récente spécification TLS de l'Internet Engineering Task Force (IETF) utilisée dans l'environnement AS2.

5. Le GTPT a fait remarquer qu'outre les renseignements fournis dans le rapport BPRE096a du FIT, la norme TLS 1.3 de l'IETF s'était maintenant stabilisée et est soutenue par les fournisseurs d'infrastructure de télécommunication. De plus, les fournisseurs cessent de soutenir la norme TLS 1.2. Ainsi, l'industrie des télécommunications doit passer à la norme TLS 1.3 afin de continuer à bénéficier du soutien des fournisseurs pour ses plateformes. Par ailleurs, la mise à niveau à la norme TLS 1.3 assurera une protection accrue des renseignements échangés sur les liaisons AS2. Le GTPT a mis à jour les Lignes directrices afin d'y intégrer l'utilisation de la norme TLS 1.3 pour la transmission de données sur des liaisons AS2.

6. Le GTPT a fait remarquer que les méthodes élaborées pour le déploiement de la norme TLS 1.2 en 2015 et en 2016 pourraient être utilisées, voire améliorées, pour le déploiement obligatoire anticipé de la norme TLS 1.3 prévu en 2023.

7. Le GTPT a demandé que le Conseil publie sa décision sur le Rapport et la version 5 proposée des Lignes directrices au plus tard le 30 septembre 2022. Sous réserve de l'approbation par le Conseil, sans modification du Rapport et des Lignes directrices, d'ici le 30 septembre 2022, le GTPT a demandé à ce que le Conseil exige des FST qu'ils mettent en œuvre la norme TLS 1.3 selon le calendrier suivant :

    - Préparation volontaire, à compter du 1er octobre 2022 : Les FST peuvent volontairement commencer la communication des données de

configuration, des plans de déploiement et des dates liés à la norme TLS 1.3 avec des pairs utilisant le protocole AS2.

- Période de déploiement, à compter du 1er janvier 2023 : Les FST doivent rendre les renseignements sur la configuration disponibles pour les pairs utilisant le protocole AS2. Le déploiement de la norme TLS 1.3 commence et aura lieu à des dates convenues mutuellement.
- Période de déploiement, se terminant le 30 juin 2023 : Les FST doivent avoir terminé l'activation de la norme TLS 1.3 sur leurs liaisons AS2.

8. Le GTPT a également fait remarquer qu'il avait l'intention de continuer à planifier le déploiement de la norme TLS 1.3 et de faciliter les communications connexes entre les FST au cours de ses réunions plénières mensuelles ou d'autres réunions spéciales, selon les besoins.

Analyse du Conseil

9. Depuis 2015, le GTPT a pris un certain nombre de mesures pour renforcer la sécurité des renseignements échangés au moyen de la norme TLS 1.2 sur des liaisons AS2. La migration vers la norme TLS 1.3 est nécessaire, car la sécurité de la technologie TLS 1.2 a été compromise au fil des ans, et la norme TLS 1.3 comprend des mesures améliorées en matière de chiffrement et d'algorithme qui actualisent et renforcent la sécurité de chiffrement.

10. Le Conseil fait remarquer que dans la décision de télécom 2018-62, dans laquelle il a approuvé le rapport BPRE096a du FIT, il a également abordé la nécessité éventuelle de passer à la norme TLS 1.3 dans le cadre de l'utilisation des liaisons AS2. Le Conseil a fait remarquer que, comme l'a indiqué le GTPT dans le rapport BPRE096a, la norme TLS 1.3 n'était pas, à ce moment-là, à un stade d'achèvement permettant son utilisation dans un environnement de production. Cependant, le GTPT et le Conseil envisageaient qu'à un moment donné, les FST devraient passer à la norme TLS 1.3 et que celle-ci serait intégrée dans les Lignes directrices. Par conséquent, dans sa décision, le Conseil a avisé les entreprises et d'autres intervenants de se préparer à mettre en œuvre les améliorations futures en matière de sécurité prévues dans la version 1.3 de la norme TLS et de prévoir un budget pour leur mise en œuvre.

11. Pour soutenir cette activité, le GTPT a mis à jour les Lignes directrices pour y inclure la norme TLS 1.3 et élaboré un calendrier de migration, tel que mentionné ci-dessus, qui s'inspire de l'expérience que l'industrie des télécommunications a acquise lors de la migration vers la norme TLS 1.2. Le GTPT a indiqué que l'une des exigences d'une migration réussie est le passage de tous les FST à la nouvelle norme TLS 1.3 d'ici une date définie. Le Conseil estime que tous les FST devraient être tenus de passer à la norme TLS 1.3 d'ici une certaine date, et que cette date devrait être le 30 juin 2023, comme le propose le GTPT.

Conclusion

12. Compte tenu de ce qui précède, le Conseil **approuve** le Rapport et les Lignes directrices mises à jour et **ordonne** aux FST de passer à l'utilisation du protocole TLS 1.3 pour l'échange de données sur des liaisons AS2 au plus tard le **30 juin 2023**.

Instructions

13. Conformément au sous-alinéa 1b)(i) des Instructions de 2006[1], le Conseil estime que l'approbation du Rapport et des Lignes directrices, ainsi que l'obligation d'utiliser la norme TLS 1.3 pour l'échange de données sur des liaisons AS2, feront progresser l'objectif de la politique énoncé aux alinéas 7a) et 7f) de la *Loi sur les télécommunications*[2].

14. Conformément aux Instructions de 2019[3], le Conseil estime que sa conclusion peut promouvoir la concurrence, l'abordabilité et les intérêts des consommateurs en fournissant un environnement sécurisé pour l'échange de renseignements sur les clients entre les entreprises, ce qui facilite la transition sans heurts des clients entre différents concurrents, faisant ainsi la promotion du choix des clients sur le marché des télécommunications.

Secrétaire général

---

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

[2] Les objectifs de la politique cités 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; et 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.

[3] *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