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

Décision de télécom CRTC 2016-150

Version PDF

Ottawa, le 26 avril 2016

Numéro de dossier : 8621-C12-01/08

Groupe de travail Plan de travail du CDCI – Rapport de consensus BPRE093b concernant des lignes directrices modifiées canadiennes relatives à l'échange de données

1. Le 1er février 2016, le Groupe de travail Plan de travail (GTPT) du Comité directeur du CRTC sur l'interconnexion (CDCI) a soumis à l'approbation du Conseil le rapport de consensus suivant :

    - *Canadian Data Interchange Guidelines* (Version 4.0) [BPRE093b]

2. On peut consulter ce rapport de consensus sur le site Web du Conseil, à l'adresse www.crtc.gc.ca, dans la section « Rapports » de la page du GTPT, qui se trouve sous la rubrique du CDCI.

3. Dans le rapport, le GTPT a indiqué qu'il avait examiné les aspects liés à la sécurité du protocole AS2[1], qu'utilisent les fournisseurs de services de télécommunication canadiens pour échanger des fichiers de données, et qu'il avait obtenu un consensus sur plusieurs éléments, comme suit :

    - révoquer l'utilisation de certificats autosignés et exiger de toutes les entreprises qu'elles mettent en œuvre des certificats numériques fournis par des autorités de certification[2], d'ici le 27 juin 2016;

    - utiliser le protocole Transport Layer Security (TLS) au lieu du protocole Secure Sockets Layer (SSL)[3] et exiger de toutes les entreprises qu'elles mettent en œuvre la version 1.2 du protocole TLS, d'ici le 27 juin 2016;

[1] Les protocoles AS1 et AS2 (Applicability Statement 1 et Applicability Statement 2) sont des normes techniques pour la transmission sécuritaire et fiable de données sur Internet. AS1 est similaire au courriel; AS2 permet le transfert direct de données.

[2] Le rôle de l'autorité de certification consiste à garantir que la personne à laquelle le certificat est accordé est bien la personne que celle-ci prétend être.

[3] TLS et SSL sont des protocoles de cryptage offrant une protection des communications sur un réseau informatique.

- utiliser l'algorithme de cryptage à 256 bits Advanced Encryption Standard (AES) au lieu de l'algorithme de cryptage Triple Data Encryption Standard[4] et exiger de toutes les entreprises qu'elles mettent en œuvre l'algorithme de cryptage de 256 bits AES, d'ici le 27 juin 2016;

- enlever le protocole AS1 en tant qu'option qu'utilisent les fournisseurs de services de télécommunication canadiens pour échanger des fichiers de données.

4. Le GTPT a précisé qu'il a mis à jour les Lignes directrices canadiennes relatives à l'échange de données (Lignes directrices)[5] pour faire état de ces modifications, ainsi que des conclusions que le Conseil a tirées dans la décision de télécom 2015-435[6]. Le GTPT a demandé au Conseil d'approuver ses modifications proposées et l'adoption des Lignes directrices connexes mises à jour.

Résultats de l'analyse du Conseil

5. Le Conseil a examiné les modifications que le GTPT a proposées aux Lignes directrices énoncées au paragraphe 3 ci-dessus, et il estime que ces modifications amélioreront la sécurité des données échangées entre les fournisseurs de services de télécommunication. Puisque les Lignes directrices modifiées proposées par le GTPT font état de ces modifications, ainsi que des conclusions que le Conseil a tirées dans la décision de télécom 2015-435, le Conseil **approuve** le rapport de consensus du GTPT et l'adoption des Lignes directrices modifiées (version 4.0).

Secrétaire générale

Documents connexes

- *Groupe de travail Plan de travail du CDCI – Calendrier de transition concernant l'échange sécurisé de fichiers de données entre les fournisseurs de services de télécommunication et les fournisseurs de logiciels (rapport BPRE093a)*, Décision de télécom CRTC 2015-435, 23 septembre 2015

- *Groupe de travail Plan de travail du CDCI – Rapport de non-consensus BPRE071a – Norme minimale relative à l'échange de données sur les demandes et les confirmations de service local*, Décision de télécom CRTC 2010-118, 26 février 2010

---

[4] Ces algorithmes de cryptage sont des normes utilisées par l'industrie canadienne des télécommunications pour crypter des fichiers de données transmis par l'usage du protocole AS2 afin de protéger les données de l'entreprise et du client.

[5] La version actuelle des Lignes directrices (version 3.3, datée du 1er septembre 2010) a été publiée par le GTPT pour faire état des conclusions que le Conseil a tirées dans la décision de télécom 2010-118.

[6] Dans cette décision, le Conseil a approuvé un calendrier pour mettre à niveau la norme de sécurité SHA-1 (Secure Hash Algorithm-1 [algorithme de hachage sécurisé-1]) dans le processus du protocole AS2.