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

Décision de télécom CRTC 2015-435

Version PDF

Ottawa, le 23 septembre 2015

Numéro de dossier : 8621-C12-01/08

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)

Contexte

1. Le protocole AS2 (Applicability Statement 2) est une norme technique pour la transmission de données sur Internet qu'utilisent les fournisseurs de services de télécommunication (FST) canadiens pour échanger des fichiers de données[1].

2. Avec le protocole AS2, on utilise des certificats numériques pour garantir l'échange sécurisé au niveau requis des fichiers de données. Ces certificats sont généralement obtenus auprès d'une autorité de certification reconnue[2]. Un certificat numérique comprend une signature numérique, qui témoigne du fait que le message a été créé par un expéditeur connu et qu'il n'a subi aucune modification au cours de sa transmission.

3. Les signatures numériques sont attribuées aux certificats au moyen d'algorithmes mathématiques sécurisés mis au point par la National Security Agency des États-Unis. La version actuelle des Lignes directrices canadiennes relatives à l'échange de données, qui ont été modifiées par le Groupe de travail Plan de travail (GTPT) du Comité directeur du CRTC sur l'interconnexion (CDCI) conformément aux conclusions du Conseil dans la décision *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, précise qu'il faut utiliser l'algorithme nommé SHA-1 (Secure Hash Algorithm-1 [algorithme de hachage sécurisé-1]) pour vérifier les certificats numériques. Toutefois, en raison de préoccupations liées à la sécurité, l'algorithme SHA-1 sera progressivement éliminé

[1] Dans la décision de télécom 2010-118, le Conseil a déterminé, entre autres choses, que le 1er janvier 2011, le protocole AS2 devenait la norme minimale d'échange de données pour les demandes de service local (DSL) et les confirmations de service local entre les entreprises de services locaux (ESL), sauf en ce qui concerne les ESL dont le volume opérationnel est inférieur à 25 DSL par mois, sur une période de trois mois, avec n'importe lequel des partenaires commerciaux.
[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.

par de nombreux fournisseurs de logiciels d'ici le début de 2016 en vue de le remplacer généralement par l'algorithme SHA-2.

Rapport

4. Le 12 août 2015, le GTPT a soumis à l'approbation du Conseil le rapport suivant :

    - *Canadian Data Interchange Guidelines* (Version 4.0) [BPRE093a]

5. On peut consulter ce rapport 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.

6. Dans son rapport, le GTPT a soumis à l'approbation du Conseil un calendrier de transition de l'algorithme SHA-1 à l'algorithme SHA-2 afin de continuer à garantir l'échange sécurisé des fichiers de données entre les FST. Ce calendrier comprend trois dates repères, avec un délai de trois mois entre chacune de ces dates, visant i) à définir une période de chevauchement au cours de laquelle aucune technologie des FST ou des fournisseurs de logiciels ne serait rendue incompatible et ii) à accorder suffisamment de temps à tous les FST, de même qu'à leurs partenaires commerciaux, pour installer et mettre à l'essai le logiciel à l'interne.

7. Plus précisément, le GTPT a proposé que :

    - d'ici le 16 novembre 2015 – tous les FST devront accepter, sur demande, les fichiers envoyés avec l'algorithme SHA-2;

    - d'ici le 28 mars 2016 – tous les FST devront être prêts à envoyer, sur demande, des fichiers en utilisant l'algorithme SHA-2;

    - d'ici le 27 juin 2016 – les FST devront cesser d'utiliser l'algorithme SHA-1.

Point ne faisant pas l'objet d'un consensus

8. Les participants du GTPT s'entendent sur la nécessité de réaliser dès que possible la transition des certificats signés avec un algorithme SHA-1 vers les certificats signés avec un algorithme SHA-2. Ils n'ont toutefois pas réussi à obtenir un consensus en ce qui a trait à la première date repère.

9. Même si la Société TELUS Communications (STC) a appuyé cette initiative, elle a déclaré qu'elle n'était pas en mesure de respecter la première date repère (16 novembre 2015) et qu'elle ne parviendrait à accepter, sur demande, les fichiers envoyés avec l'algorithme SHA-2 qu'au cours du premier trimestre de 2016.

10. Le GTPT a donc demandé au Conseil d'examiner le point ne faisant pas l'objet d'un consensus concernant les dates repères proposées pour la transition vers l'algorithme SHA-2.

11. Cependant, après le dépôt du rapport du GTPT, la STC a procédé à une évaluation interne des activités requises pour réaliser la transition vers l'algorithme SHA-2 et a confirmé au Conseil qu'elle serait finalement en mesure de respecter les trois dates repères proposées par le GTPT (soit le 16 novembre 2015, le 28 mars 2016 et le 27 juin 2016).

Résultats de l'analyse du Conseil

12. Étant donné que la STC a confirmé au Conseil qu'elle est maintenant en mesure de respecter les trois dates repères proposées susmentionnées, le point ne faisant pas l'objet d'un consensus est donc réglé. Par conséquent, le rapport peut être effectivement traité comme un rapport de consensus.

13. Le Conseil a examiné le rapport du GTPT et le calendrier de transition de l'algorithme SHA-1 à l'algorithme SHA-2 proposé et conclut que tous deux sont raisonnables. Par conséquent, le Conseil **approuve** le rapport et **ordonne** aux FST de respecter le calendrier de transition de l'algorithme SHA-1 à l'algorithme SHA-2 énoncé ci-dessus au paragraphe 7.

Secrétaire général