



Telecom Decision CRTC 2022-264

PDF version

Ottawa, 26 September 2022

Public record: 8621-C12-01/08

Changes to the Canadian Data Interchange Guideline and migration to Transport Layer Security 1.3

Summary

The Commission **approves** the Business Process Working Group's consensus Task Identification Form (TIF) report BPRE096b and the updated Canadian Data Interchange Guideline and **directs** telecommunications service providers to migrate to the use of Transport Layer Security 1.3 for exchanging data over Application Statement 2 links by **30 June 2023**.

Introduction

Background

1. Telecommunications service providers (TSPs) currently use electronic file exchange as a mechanism to support efficient customer transfers and to secure the exchange of various records used in support of other tariffed and forborne services, such as basic listing interchange file service, toll-free call records, local service requests, service cancellations, and primary interexchange carrier requests. Except for some low-volume file exchanges, bilateral file exchanges between TSPs use Application Statement 2 (AS2) links as the standard mechanism. AS2 is supported by various business-to-business platforms and the telecommunications infrastructure vendor community.
2. On 16 October 2017, the Business Process Working Group (BPWG) submitted Task Identification Form (TIF) Report BPRE096a entitled *Readiness of Canadian Carriers to Implement Enhanced Transport Layer Security via AS2*. In the report, the BPWG outlined the purpose of Transport Layer Security (TLS) on AS2 electronic inter-TSP file transfer links and the rationale to increase the security level of TLS. The BPWG concluded that the TLS 1.3 standard was not yet at a completion state that could be implemented for use in Canada, and that this implementation time frame would not occur for another one to three years.
3. The Commission approved TIF report BPRE096a in *CISC Business Process Working Group – Consensus report BPRE096a regarding readiness of Canadian carriers to implement enhanced Transport Layer Security via Applicability Statement 2*, Telecom Decision CRTC 2018-62, 15 February 2018 (Telecom Decision 2018-62). In that

decision, the Commission notified carriers and others to be prepared to implement the future security enhancements contained in TLS 1.3 and to budget for this activity.

The report

4. On 14 June 2022, the CRTC Interconnection Steering Committee (CISC) forwarded to the Commission, for its approval, BPWG consensus TIF report BPRE096b (the report) for changes to the Canadian Data Interchange Guideline – Version 5 (BPGLDI50) [the Guideline]. The changes to the Guideline are to enhance the security of data transmission between TSPs by moving to the latest Internet Engineering Task Force (IETF) TLS specification that is used in the AS2 environment.
5. The BPWG noted that further to the information provided in TIF report BPRE096a, the IETF TLS 1.3 standard has now stabilized and is being supported by telecommunications infrastructure vendors. Additionally, the vendors are discontinuing support for TLS 1.2. Thus, the telecommunications industry must migrate to TLS 1.3 in order to continue to receive vendor support for its platforms. The TLS 1.3 upgrade will also provide increased protection of information exchanged over AS2 links. The BPWG updated the Guideline to include the use of TLS 1.3 for the transmission of data over AS2 links.
6. The BPWG noted that the methods developed for the rollout of TLS 1.2 in 2015 and 2016 could be used and perhaps enhanced for the anticipated mandatory TLS 1.3 rollout in 2023.
7. The BPWG requested that the Commission issue its decision on the report and the proposed Version 5 of the Guideline by 30 September 2022. Pending Commission approval of the report and the Guideline without changes by 30 September 2022, the BPWG requested that the Commission mandate that TSPs implement TLS 1.3 per the following schedule:
 - Voluntary preparation, starting 1 October 2022: TSPs may voluntarily begin communication of TLS 1.3 configuration data, rollout plans, and dates with other AS2 peers.
 - Deployment window, starting 1 January 2023: TSPs must have configuration information available for other AS2 peers. Rollout of TLS 1.3 begins and will occur on mutually agreeable dates.
 - Deployment window, ending 30 June 2023: TSPs must have completed activation of TLS 1.3 on their AS2 links.
8. The BPWG also noted that it intends to continue to plan the rollout of TLS 1.3 and facilitate related communications between TSPs at its monthly plenary meetings or at other special meetings, as required.

Commission's analysis

9. Since 2015, the BPWG has taken a number of measures to strengthen the security of exchanged information by using TLS 1.2 over AS2 links. The migration to TLS 1.3 is necessary because TLS 1.2 security has been compromised over the years, and TLS 1.3 includes improved encryption and algorithm measures that update and strengthen encryption security.
10. The Commission notes that in Telecom Decision 2018-62, in which it approved TIF report BPRE096a, it also discussed the eventual need to migrate to TLS 1.3 as part of the use of AS2 links. The Commission noted that, as discussed by the BPWG in BPRE096a, at that time the TLS 1.3 standard was not in a state of standard completion permitting its use in a production environment. However, both the BPWG and the Commission envisioned that at some point TSPs would need to migrate to the TLS 1.3 standard, and that it would be incorporated into the Guideline. As a result, the Commission, in its decision, notified carriers and others to be prepared to implement the future security enhancements contained in the TLS 1.3 standard and to budget for this activity.
11. To support this activity, the BPWG has updated the Guideline to include TLS 1.3 and developed a migration timeline, as noted above, that builds on the telecommunications industry's previous experience in migrating to TLS 1.2. The BPWG indicated that one of the requirements for a successful migration is for all TSPs to move to the new TLS 1.3 standard by a set date. The Commission considers that all TSPs should be required to migrate to TLS 1.3 by a certain date, and that this date should be 30 June 2023, as proposed by the BPWG.

Conclusion

12. In light of the above, the Commission **approves** the report and the updated Guideline and **directs** TSPs to migrate to the use of TLS 1.3 for exchanging data over AS2 links by **30 June 2023**.

Policy Directions

13. In accordance with subparagraph 1(b)(i) of the 2006 Policy Direction,¹ the Commission considers that approval of the report and the Guideline, as well as mandating the use of the TLS 1.3 standard for data exchange over AS2 links, will advance the policy objective set out in paragraphs 7(a) and 7(f) of the *Telecommunications Act*.²

¹ *Order issuing a Direction to the CRTC on Implementing the Canadian Telecommunications Policy Objectives*, SOR/2006-355, 14 December 2006

² The cited policy objectives are 7(a) to facilitate the orderly development throughout Canada of a telecommunications system that serves to safeguard, enrich and strengthen the social and economic fabric of Canada and its regions and 7(f) to foster increased reliance on market forces for the provision of telecommunications services and to ensure that regulation, where required, is efficient and effective.

14. In accordance with the 2019 Policy Direction,³ the Commission considers that its decision can promote competition, affordability, and consumer interests by providing a secure environment for the exchange of customer information between carriers, which assists the seamless transition of customers between different competitors, thereby promoting customer choice in the telecommunications marketplace.

Secretary General

³ *Order Issuing a Direction to the CRTC on Implementing the Canadian Telecommunications Policy Objectives to Promote Competition, Affordability, Consumer Interests and Innovation*, SOR/2019-227, 17 June 2019