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

Telecom Decision CRTC 2018-62

PDF version

Ottawa, 15 February 2018

Public record: 8621-C12-01/08

CISC Business Process Working Group – Consensus report BPRE096a regarding readiness of Canadian carriers to implement enhanced Transport Layer Security via Applicability Statement 2

Background

1. In 2015 and 2016, the CRTC Interconnection Steering Committee (CISC) Business Process Working Group (BPWG) undertook efforts to strengthen the security of the electronic file transfer protocol Applicability Statement 2 (AS2), which is used for the exchange of records[1] over the Internet between telecommunications service providers (TSPs) operating in Canada. The project identified specific items of file transfer cryptography currently in use, and defined a path forward to upgrade and enhance security related to the digital certificates[2] used within AS2.

2. As a result of these efforts, the BPWG submitted a series of reports, which the Commission approved in various decisions.[3] In those decisions, the Commission approved the BPWG's recommendations, which resulted in a new and updated Canadian Data Interchange Guideline (CDIG), which contains industry guidelines for the electronic exchange of business data among TSPs.

3. However, during the implementation of upgrades to file exchange security, some AS2 incompatibilities between TSPs were highlighted. These were due to differences in their specific implementation of cipher suites[4] in the Transport Layer Security (TLS) 1.2 standard (TLS 1.2).[5]

---

[1] These include local service order information, directory listings, long distance service requests and records, and billing and collections data.

[2] Digital certificates are electronic credentials that are used to certify the online identities of individuals, organizations, and computers. Certificates are issued and certified by a certification authority such as Entrust.

[3] See Telecom Decisions 2015-435, 2016-150, and 2017-31.

[4] A cipher suite is a combination of authentication and encryption algorithms used to negotiate the security settings for a network connection that uses the Secure Socket Layer (SSL) / Transport Layer Security (TLS) network protocols.

[5] The transport layer used with AS2 involves Hypertext Transfer Protocol (HTTP) combined with SSL or TLS for security – this is known as HTTPS. TLS is newer than SSL. In Telecom Decision 2016-150, the Commission approved the use of TLS 1.2 rather than SSL.

4. To address incompatibilities, the BPWG recommended, and the Commission approved in Telecom Decision 2017-31, an amended CDIG that required TSPs to use the "mandatory to implement" (MTI) cipher suite contained within the Internet Engineering Task Force (IETF) TLS 1.2 standard.

5. The BPWG members also agreed to continue to address opportunities to enhance cipher security while continuing to operate within TLS 1.2. The BPWG indicated that although the TLS 1.3 standard (TLS 1.3) was still under development, there appeared to be consensus on the revised MTI cipher suite element in that standard. Accordingly, the BPWG investigated the implementation possibilities related to the draft TLS 1.3. The BPWG also agreed that standardization with respect to an upcoming MTI cipher suite would "future-proof" the activities of the BPWG should an upgrade to TLS 1.3 occur.

The report

6. On 16 October 2017, the Commission received a consensus report entitled *Readiness of Canadian Carriers to Implement Enhanced Transport Layer Security via AS2* (BPRE096a) [the report][6] from the BPWG. In the report, the BPWG provided an update on TLS 1.3 with regard to AS2 file exchange security issues.

7. The BPWG stated that the majority of its members did not support the identified MTI cipher suite in TLS 1.3, nor did they have formal plans or dates when their existing AS2 vendors could provide such support.

8. The BPWG noted that a review of TLS 1.3 revealed that the structure of the TLS 1.3 cipher suite is different than the structure of cipher suites contained within TLS 1.2. It concluded that a future-proof approach using known MTI cipher suites contained within TLS 1.3 would not be feasible.

9. The BPWG indicated that the closure of the IETF's TLS 1.3 standardization process is imminent. It stated that several open-source software vendors are already claiming that they support TLS 1.3, and that some popular Internet browsers (e.g. Google Chrome and Mozilla Firefox) include TLS 1.3 support in their test/development mode.

10. The BPWG concluded that the eventual standardization and widespread adoption of TLS 1.3 will likely occur within the next one to three years, which is consistent with most carriers' information technology planning and budgeting windows of one to three years before implementation. The BPWG decided, therefore, to take a proactive course of action that would involve reminding carriers that they will eventually have to comply with and implement TLS 1.3.

---

[6] The report can be found under the "Reports" section of the BPWG page, which is available in the CISC section of the Commission's website at www.crtc.gc.ca.

11. Accordingly, the BPWG requested that the Commission approve the report and inform Canadian TSPs of

    - the telecommunications industry's plans to implement TLS 1.3 (when it is a fully approved standard by the IETF) as a mandatory component of the AS2 process within the CDIG; and

    - the need to plan and budget for the associated software expenditures.

Commission's analysis and determinations

12. In Telecom Decision 2015-435, the Commission approved an upgrade of the requirements for the exchange of data between TSPs, and an upgrade schedule spread over a one-year period. In that case, BPWG members upgraded to a standard that was first published in 2001 from a standard that was issued in 1993. In Telecom Decision 2016-150, the Commission approved further security upgrades, including moving to TLS 1.2, which was issued in 2008. The Commission considers it reasonable to assume that TLS 1.3 will be implemented similarly over several years.

13. The BPWG's proactive approach to reviewing upcoming security upgrades is laudable and is in the interest of consumers, whose information will be better protected. The Commission considers that approval of the report and a reminder to carriers that TLS 1.3 will eventually be included in the CDIG will (i) result in carriers taking into account that they may incur upgrade costs for which they must budget, and (ii) likely lead to TSPs adopting TLS 1.3 earlier than would normally do.

14. Accordingly, Commission **approves** the report. The Commission hereby notifies carriers to be prepared to implement the future security enhancements contained in TLS 1.3 and to budget for this activity.

Secretary General

Related documents

- *CISC Business Process Working Group – Consensus report BPRE093c regarding revised Canadian Data Interchange Guidelines*, Telecom Decision CRTC 2017-31, 2 February 2017

- *CISC Business Process Working Group – Consensus report BPRE093b regarding revised Canadian Data Interchange Guidelines,* Telecom Decision CRTC 2016-150, 26 April 2016

- *CISC Business Process Working Group – Upgrade schedule for the secure exchange of data files between telecommunications service providers and software vendors (report BPRE093a),* Telecom Decision CRTC 2015-435, 23 September 2015