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

Telecom Decision CRTC 2015-435

PDF version

Ottawa, 23 September 2015

File number: 8621-C12-01/08

CISC Business Process Working Group – Upgrade schedule for the secure exchange of data files between telecommunications service providers and software vendors (report BPRE093a)

Background

1. AS2 (Applicability Statement 2) is a technical standard for transmitting data over the Internet, and is used by Canadian telecommunications service providers (TSPs) to exchange data files.[1]

2. With AS2, digital certificates are used to enable the required security when data files are exchanged. These certificates are typically obtained from a recognized Certificate Authority.[2] A digital certificate includes a digital signature, which demonstrates that the message was created by a known sender and that it was not altered in transit.

3. Digital signatures are applied to the certificates using secure mathematical algorithms designed by the U.S. National Security Agency. The current version of the Canadian Data Interchange Guidelines, which were amended by the CRTC Interconnection Steering Committee (CISC) Business Process Working Group (BPWG) pursuant to the Commission's determinations in *CISC Business Process Working Group – Non-consensus report BPRE071a – Minimum requirement for the exchange of local service request and local service confirmation data*, Telecom Decision CRTC 2010-118, 26 February 2010, specifies that an algorithm referred to as SHA-1 (Secure Hash Algorithm - 1) is to be used for the verification of digital certificates. However, due to security concerns, SHA-1 is being phased out by many software vendors by early 2016 and will generally be replaced by SHA-2 (Secure Hash Algorithm - 2).

[1] In Telecom Decision 2010-118, the Commission determined, among other things, that as of 1 January 2011, AS2 is the minimum requirement for the exchange of local service request (LSR) and local service confirmation data between local exchange carriers (LECs), except for LECs whose trading volume has not reached 25 LSRs per month with any one trading partner in a three-month period.
[2] The role of the Certificate Authority is to guarantee that the individual to whom the certificate is granted is, in fact, who they claim to be.

Report

4. On 12 August 2015, the BPWG submitted the following report for the Commission's approval:

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

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

6. In the report, the BPWG proposed, for the Commission's approval, a schedule for upgrading from SHA-1 to SHA-2 to ensure the continued secure exchange of data files between TSPs. This schedule includes three milestone dates, with three months allowed between each, to (i) ensure an overlapping period during which no TSP's or software vendor's technology would be rendered incompatible, and (ii) provide sufficient time for each TSP, and its trading partners, to install and test the software internally.

7. Specifically, the BPWG proposed that

    - by 16 November 2015 – all TSPs must accept files sent using SHA-2, if requested;

    - by 28 March 2016 – all TSPs must be ready to send files using SHA-2, if requested; and

    - by 27 June 2016 – TSPs must no longer use SHA-1.

Non-consensus issue

8. There was consensus between the BPWG participants on the need to migrate as soon as possible from digital certificates signed with the SHA-1 algorithm to certificates signed with SHA-2. However, consensus could not be reached on the first milestone date.

9. While TELUS Communications Company (TCC) supported the initiative, it stated that it was not able to commit, at the time, to the first milestone date (16 November 2015), and that it would be some time in the first quarter of 2016 before it could comply with this milestone.

10. The BPWG therefore requested that the Commission address the non-consensus issue regarding the proposed milestone dates for migration to SHA-2.

11. However, subsequent to the BPWG report, TCC conducted an internal assessment of the activities required to complete the migration to SHA-2 and confirmed to the Commission that it would be able to meet the three milestone dates proposed by the BPWG (i.e. 16 November 2015, 28 March 2016, and 27 June 2016).

Commission's analysis and determinations

12. Since TCC has confirmed to the Commission that it is able to meet the three milestone dates mentioned above, the non-consensus issue has been resolved, and the report can be effectively treated as a consensus report.

13. The Commission has reviewed the BPWG's report and the proposed SHA-1 to SHA-2 upgrade schedule, and finds both to be reasonable. The Commission therefore **approves** the report, and **directs** TSPs to abide by the SHA-1 to SHA-2 upgrade schedule set out in paragraph 7 above.

Secretary General