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

Telecom Decision CRTC 2016-150

PDF version

Ottawa, 26 April 2016

File number: 8621-C12-01/08

CISC Business Process Working Group – Consensus report BPRE093b regarding revised Canadian Data Interchange Guidelines

1. On 1 February 2016, the CRTC Interconnection Steering Committee (CISC) Business Process Working Group (BPWG) submitted the following consensus report for the Commission's approval:

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

2. This consensus 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.

3. In the report, the BPWG indicated that it had reviewed the security-related aspects of AS2,[1] which is used to exchange data files between Canadian telecommunications service providers, and had reached consensus on several items, as follows:

    - disallow the use of self-signed certificates, and require all companies to implement digital certificates provided by certificate authorities,[2] by 27 June 2016;
    - use Transport Layer Security (TLS) rather than Secure Sockets Layer (SSL),[3] and require all companies to implement TLS Version 1.2, by 27 June 2016;
    - use the Advanced Encryption Standard (AES) 256-bit encryption algorithm rather than the Triple Data Encryption Standard encryption algorithm,[4] and require all companies to implement the AES 256-bit encryption algorithm, by 27 June 2016; and

[1] AS1 and AS2 (Applicability Statement 1 and Applicability Statement 2) are technical standards for the secure and reliable transport of data over the Internet. AS1 is similar to email; AS2 provides for direct data transfer.

[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.

[3] TLS and SSL are encryption protocols that provide communications security over a computer network.

[4] These encryption algorithms are standards used by the Canadian telecommunications industry to encrypt data files transmitted through the use of AS2 to safeguard company and customer data.

- remove AS1 as an option to exchange data files between Canadian telecommunications service providers.

4. The BPWG submitted that it has updated the Canadian Data Interchange Guidelines (the Guidelines)[5] to reflect these revisions, as well as the Commission's determinations set out in Telecom Decision 2015-435.[6] The BPWG requested that the Commission approve its proposed revisions and the adoption of the associated updated Guidelines.

Commission's analysis and determinations

5. The Commission has reviewed the BPWG's proposed revisions to the Guidelines set out in paragraph 3 above, and considers that these revisions will enhance the security of data exchanged between telecommunications service providers. Since the BPWG's proposed revised Guidelines reflect these revisions, as well as the Commission's determinations set out in Telecom Decision 2015-435, the Commission **approves** the BPWG's consensus report and the adoption of the revised Guidelines (Version 4.0).

Secretary General

Related documents

- *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

- *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

[5] The current version of the Guidelines (Version 3.3, dated 1 September 2010) was issued by the BPWG to reflect the Commission's determinations set out in Telecom Decision 2010-118.

[6] In that decision, the Commission approved a schedule for upgrading the Secure Hash Algorithm (SHA) security standard in the AS2 process.