Legal update, Canada: PIPEDA's Secure Electronic Signature Regulations have been published[1]

BARBARA MCISAAC QC AND HOWARD R. FOHR

The use of electronic against paper documents became more clearly defined under the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (PIPEDA), with the recent introduction of the *Secure Electronic Signature Regulations*. These regulations facilitate the use of electronic signatures as an alternative to paper-based records. Part 2 of PIPEDA provides for the use of electronic alternatives where federal laws contemplate the use of paper to record or communicate information or transactions.[2] On February 1, 2005, this framework was substantially augmented with the registration of the *Secure Electronic Signature Regulations*, SOR/2005-30 (SES Regs).

Section 33 of PIPEDA states that a federal department, agency, body, etc. may use electronic means to create or otherwise deal with documents whenever a federal law does not specify the manner of doing so. However, Part 2 of PIPEDA requires a secure electronic signature for certain types of electronic alternatives to paper, such as sworn statements (section 44), statements declaring truth (section 45), witnessed signatures (section 46), originals (section 42), documents under seal (section 39) and documents as evidence or proof (section 36).

A secure electronic signature is defined in section 31 of PIPEDA as an *"an electronic signature that results from the application of a technology or process prescribed by regulations made under subsection 48(1)."* Section 48 of PIPEDA describes the minimum characteristics of the technology that would satisfy the Act's requirements,[3] and authorized the Governor in Council, upon the recommendation of the Treasury Board, to make regulations prescribing the required technologies. As such, the SES Regs were required in order to complete the definition of secure electronic signature and thereby enable the use of electronic alternatives for the documents referenced above once the other requirements of these provisions have been met.

The SES Regs describe the technology or processes to create a digital signature that meets the characteristics of a secure electronic signature. Only digital signature certificates[4] that are deemed to be sufficiently trustworthy will qualify. These certificates must be issued by a certification authority[5] which: (a) the President of the Treasury Board has verified as having the capacity to issue certificates in a secure and reliable manner and which fulfil the requirements of section 48 of PIPEDA, and (b) are listed on the website of the Treasury Board Secretariat.

We have been advised that the process for recognition as a certification authority by the federal government is through cross-certification with the government's Canadian Federal PKI

Only digital signature certificates that are deemed to be sufficiently trustworthy will qualify

[1] This article was first published in the Internet and E-Commerce Law in Canada, Volume 6, Number 2, April 2005.
[2] PIPEDA, section 32.
[3] For instance, whereby (a) the electronic signature is unique to the person, (b) the use of the technology to associate the person's electronic signature to an electronic document is under the sole control of the person, (c) the technology can be used to identify the person, and (d) the electronic signature can be linked with an electronic document so that it can be used to determine whether the electronic document has been changed since the attachment of the electronic signature to the electronic document.
[4] Defined in section 1 of the SES Regs as *"an electronic document that (a) identifies the certification authority that issued it and is digitally signed by that certification authority; (b) identifies, or can be used to identify, the person; and (c) contains the person's public key."*
[5] Defined in section 1 of the SES Regs as *"a person or entity that issues digital signature certificates and that has been listed as such on the website of the Treasury Board Secretariat."*

Bridge (CFPB) Certification Authority, operated by the Communications Security Establishment. Public Works and Government Services Canada explains that "Cross-certification is the process undertaken by Certification Authorities to establish a trust relationship. When two Certification Authorities are cross-certified, they agree to trust and rely upon each other's public key certificates and keys as if they had issued them themselves. The two Certification Authorities exchange cross-certificates, enabling their respective users to interact securely."[6] A Government of Canada department or agency must sponsor a Certification Authority outside the federal government wishing to cross-certify with the CFPB.[7]

The SES Regs go on to establish a rebuttable presumption where a document contains a secure electronic signature. Where an electronic document contains a digital signature certificate issued by a certification authority recognized by the Treasury Board, then that data is presumed, in the absence of evidence to the contrary, to have been signed by the person who is identified by the digital signature certificate.

Since the enactment of PIPEDA, the electronic documents section of PIPEDA (Part 2) has been overshadowed by the personal information protection provisions of the Act (Part 1). However, with the coming into force of the SES Regs and the increased use of electronic alternatives to paper-based means of communication, Part 2 of PIPEDA should not be overlooked. ■

Barbara McIsaac QC, is a senior member of the McCarthy Tétrault LLP Litigation Group in Ottawa. She practices mainly in the areas of public and administrative law and commercial litigation. She is one of Canada's leading experts in privacy law and a co-author, with Rick Shields and Kris Klein, of *The Law of Privacy* in Canada (Carswell), the foremost Canadian privacy law text.

Howard Fohr is an associate in the McCarthy Tétrault Litigation Group in Ottawa. He carries on a general litigation practice and also assists in the firm's privacy practice. Ms McIsaac and Mr Fohr may be contacted via

http://www.mccarthy.ca

[6] See http://www.solutions.gc.ca/pki-icp/crosscert/crosscert_e.asp.

[7] We have been advised that Industry Canada, Public Works and Government Services Canada, Foreign Affairs Canada, the Communications Security Establishment, the Canada Revenue Agency and the Royal Canadian Mounted Police operate Certification Authorities capable of issuing digital certificates for secure electronic signatures.