ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

The Evolution of Electronic Signatures in the United States and Canada

Technology, Privacy, and eCommerce

Electronic signatures have been around for many years. In fact, one would be surprised to know that the validity of an electronic signature was first dealt with in 1867 by US courts which recognized the validity of a signature transmitted via telegraph.

Digitalization imposes, and almost automatically requires, the use of electronic signatures. An overview of the North American legal framework illustrates certain technicalities and misconceptions related to e-signatures.

E-signature vs. digital signature

The terms “electronic signature” and “digital signature” are often used interchangeably. However, they are different concepts and have distinct sets of features and functions.

Essentially, an electronic signature consists of affixing a tag to a document (whose support is electronic, i.e. PDF) to express consent. More specifically, attaching a code to a message guarantees the integrity of the document and the authentication of the sender. It is important to note that “electronic signature” is a generic term that includes several electronic processes, including a digital signature which is based on asymmetric cryptography. In other words, an electronic signature is merely a legal concept. It is a lasting representation and captures someone’s intent.

On the other hand, a digital signature is simply an encryption technology within the electronic signature. It works with an electronic signature and not as an electronic signature. A digital signature is “a signature that is specifically based on asymmetric cryptography, coupled with a one-way hash function.” Thus, a digital signature supports an electronic signature and provides a higher degree of certainty for the recipient.

Legal framework

Many jurisdictions have adopted legislation related to electronic signatures. To that end, the main purpose has been to provide for the authenticity of the person using the signature, the capture of intent and the integrity of a message or document on which the signature is affixed.

The North American legal framework that covers e-signatures has been guided by the UNCITRAL Model Law on Electronic Commerce (MLEC), and the UNCITRAL Model Law on Electronic Signatures (MLES). A technology-neutral approach is taken, “which avoids favouring the use of any specific technology or process. This means in practice that legislation based on this Model Law may recognize both digital signatures based on cryptography (such as public key infrastructure or PKI) and electronic signatures using other technologies.”

In other words, an electronically signed document is perfectly admissible in evidence and has the same effect as if it were on paper. This legislative approach is considered as a “minimalist” approach considering that there is no particular type of technology adopted to replace a manuscript signature in the digital environment.

In Canada and the United States, any form of electronic symbol or message can qualify as a signature. The main emphasis is on how intention is communicated.

United States

In 2000, the US Congress adopted the Electronic Signatures in Global and National Commerce Act (E-SIGN). It is a federal statute which preempts state law in case of conflict between the two. Of interest, E-SIGN does not apply to states which have enacted the Uniform Electronic Transactions Act (UETA).

Uniform Electronic Transactions Act (UETA)

Section 5 of the UETA provides that the act “applies only to transactions between parties each of which has agreed to conduct transactions by electronic means.” It does not create a new system of legal rules for the electronic marketplace, but rather ensures that electronic transactions are equivalent to and as enforceable as paper-based transactions.

The UETA defines an electronic signature as “an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record.”

Essentially, the UETA ensures that contracts and transactions are enforceable and valid notwithstanding the fact that an electronic process is applied.

E-SIGN

As mentioned above, E-SIGN bestows an equivalent legal status to electronic signatures and electronic documents. Similar to the UETA, due to its technology-neutral approach, the parties are free to decide which electronic process they want to apply to their electronic transaction.

It is important to note that E-SIGN requires consent from customers. Moreover, prior to consenting, the consumer “must be provided with a clear and conspicuous statement” outlining their rights.

E-SIGN specifies that a state statute, regulation or other rule of law may preempt the federal law, but only by adopting the UETA or by passing a law that is consistent with E-SIGN and essentially technologically neutral.

E-SIGN came into effect after the UETA and the reason behind this federal intervention is based on the inconsistency of the states when it came to defining which method could create an authentic electronic signature. In other words, a federal law was necessary because state electronic signature and electronic commerce statutes lacked uniformity.

Canada

Federal

In 2000, the *Personal Information Protection and Electronic Documents Act (PIPEDA)* came into effect. It is a federal statute which, like its American counterpart, provides for functional equivalency between electronic and paper documents.

Essentially, PIPEDA provides for “the use of electronic alternatives … where federal laws contemplate the use of paper to record or communicate information or transactions.”

Of interest, PIPEDA provides for the use of electronic signatures, the ability to provide electronic documents when an original document is required and the use of electronic documents to satisfy a requirement under federal law for a document to be in writing.

Compared to E-SIGN, the Canadian federal legislator went a step further and envisioned a situation where a “secure electronic signature” would be required. That is, an electronic signature resulting from the application of a prescribed technology or process. Following this tangent, in 2005, the Secure Electronic Signature Regulations were adopted. It provided that the term “secure electronic signature” refers to a digital signature that results from asymmetric cryptography.

Provincial

The primary focus of the provincial legislations is to provide a single, media-neutral definition of an electronic signature. However, Quebec’s legislation is slightly different. In fact, the Act to establish a legal framework for information technology (the “Act”) has a more extensive framework.

An electronic signature affixed to a document will benefit from a presumption of integrity. That is, it will not require any proof of authenticity if the “integrity of the document is ensured and the link between the signature and the document was established at the time of signing and has since been maintained.”

Moreover, the Act goes into some detail and sets out very strict rules about certificates and biometrics and establishes a harmonization committee to create technical standards for Quebec.

The Act is somewhat similar to the federal *Secure Electronic Signature Regulations* because it defines standards and regulates the choice (not to the same extent obviously) of technologies.

Cryptography

Cryptographic techniques ensure the integrity and confidentiality of messages exchanged and they also ensure that none of the parties to the transaction can deny their participation in the exchange of information.

The main type of cryptography is public-key cryptography. Essentially, this technology uses two keys which are intrinsically linked to each other and they are necessary to decrypt a given message.

In simple terms, there are three main steps in digital signature technology. First, a message or document is encrypted using a hash function. A hash function is used to determine whether the document has been altered and it assures integrity. It is a one-way encryption. In other words, there is no way to decrypt the hash. It is only possible to validate it. For example, if a password is “cat” and the resulting hash is “Tr121as” it is impossible to decrypt “Tr121as” to “cat” and recover the password. Second, in order to prove that the message was in fact sent by the legitimate sender, the encrypted message is sealed by the sender’s private key. Finally, upon reception of the message, the recipient decrypts the message using the sender’s public key and evaluates the hash to verify if the underlying message/document was compromised.

Here’s the step-by-step:

1. The sender sends a message/document which is converted by a mathematical function called a “hash function.” The latter generates an abstract called a “hash” or “digest.”
2. A digest is specifically linked to each message/document, like a fingerprint. The digest is then encrypted using the private key of the sender and attached to the message. The product of this process corresponds to the digital signature.
3. The recipient validates the identity of the sender of the message by decrypting the digital signature with the public key of the sender to obtain the digest. Subsequently, the message/document passes through the hash function a second time and if both codes are identical (digest sent versus digest received) then the sender is authenticated and the message/document is upright. If along the way, the message was changed (by someone malicious) then the digest would have been different, and the validation process of the digest would have failed.

In short, the North American landscape is ripe (and has been for a while) for disruption. Electronic signature solutions are increasingly evolved and equal to ink in the eyes of the law. In fact, many electronic signature solutions go beyond the legislative and statutory requirements. In a world where digitization is the main focus, electronic signatures provide a great opportunity for speed, efficiency and reliability.

Amir Tajkarimi is legal counsel at National Bank of Canada and cofounder of legal tech start-up Lexop.com. The opinions expressed in this article are solely those of the author and do not necessarily represent the viewpoint of the National Bank of Canada.

Further Reading

1 TREVOR v. WOOD, 36 N.Y. 307 (1867).

2 STEPHEN MASON, ELECTRONIC SIGNATURES IN LAW, (3d ed. 2012), at 189. See also the infographic provided by Silanis Technology available at [www.silanis.com/blog/business-solutions/the-difference-between-e-signatures-and-digital-signatures] (last visited Oct. 3, 2014).

3 MASON, supra note 3, at 189; See also JONATHAN E. STERN, The Electronic Signatures in Global and National Commerce Act, 16 BERKELEY TECH. L.J. 391 (2001); See also LALANCETTE & MAALAOUI, La signature électronique, LA REVUE JURIDIQUE DES ÉTUDIANTS ET ÉTUDIANTES DE L'UNIVERSITÉ LAVAL, (2002) 16 R.J.E.U.L.

4 MASON, supra note 3, at 189 ("For the sake of clarity, the term 'electronic signature' is used to denote the generic concept of a signature that is brought about by the use of a computer or computer-like device, and includes a digital signature as one form of electronic signature.").

5 MASON, supra note 3, at 153-160.

6 UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE (1996).

7 "The Model Law on Electronic Signatures (MLES) aims to enable and facilitate the use of electronic signatures by establishing criteria of technical reliability for the equivalence between electronic and hand-written signatures. Thus, the MLES may assist States in establishing a modern, harmonized and fair legislative framework to address effectively the legal treatment of electronic signatures and give certainty to their status." UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES (2001).

8 UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES (2001).

9 For a more detailed discussion, see MASON, supra note 2, at 156.

10 15 U.S.C. §§ 7001-7003.

11 Congress enacted the Electronic Signatures in Global and National Commerce Act (E-SIGN) that also establishes the validity of electronic records and signatures. It governs in the absence of a state law or where states have made modifications to UETA that are inconsistent with E-SIGN. By adopting the official version of UETA, states have the authority to modify, limit or supersede some E-SIGN provisions, including its consumer protection provisions.

12 The Uniform Electronic Transactions Act (UETA) was developed by the National Conference of Commissioners on Uniform State Laws to provide a legal framework for the use of electronic signatures and records in government or business transactions. UETA makes electronic records and signatures as legal as paper and manually signed signatures. Available at [www.ncsl.org/research/telecommunications-and-information-technology/uniform-electronic-transactions-acts.aspx]. There are 3 states that have not adopted the UETA, but have statutes pertaining to electronic transactions: New York, Illinois and Washington.

13 With respect to handwritten signatures and paper-based documents.

14 E-SIGN defines "transaction" to mean the sale, lease, exchange, licensing, or other disposition of personal or real property and services between two or more persons.

15 15 U.S.C. § 7001 SEC. 101. (c).

16 15 U.S.C. § 7002 SEC. 102. (a).

17 Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5).

18 PIPEDA is inapplicable to contracts which are governed by provincial jurisdiction.

19 PIPEDA supra note 41, s. 32.

20 Id., s. 43.

21 Id., s. 42.

22 Id., s. 41.

23 Id., s. 31.

24 Secure Electronic Signature Regulations, SOR/2005-30.

25 PARLIAMENT OF CANADA: LIBRARY OF PARLIAMENT RESEARCH PUBLICATIONS, The Development of Laws on Electronic Documents and E-Commerce Transactions.

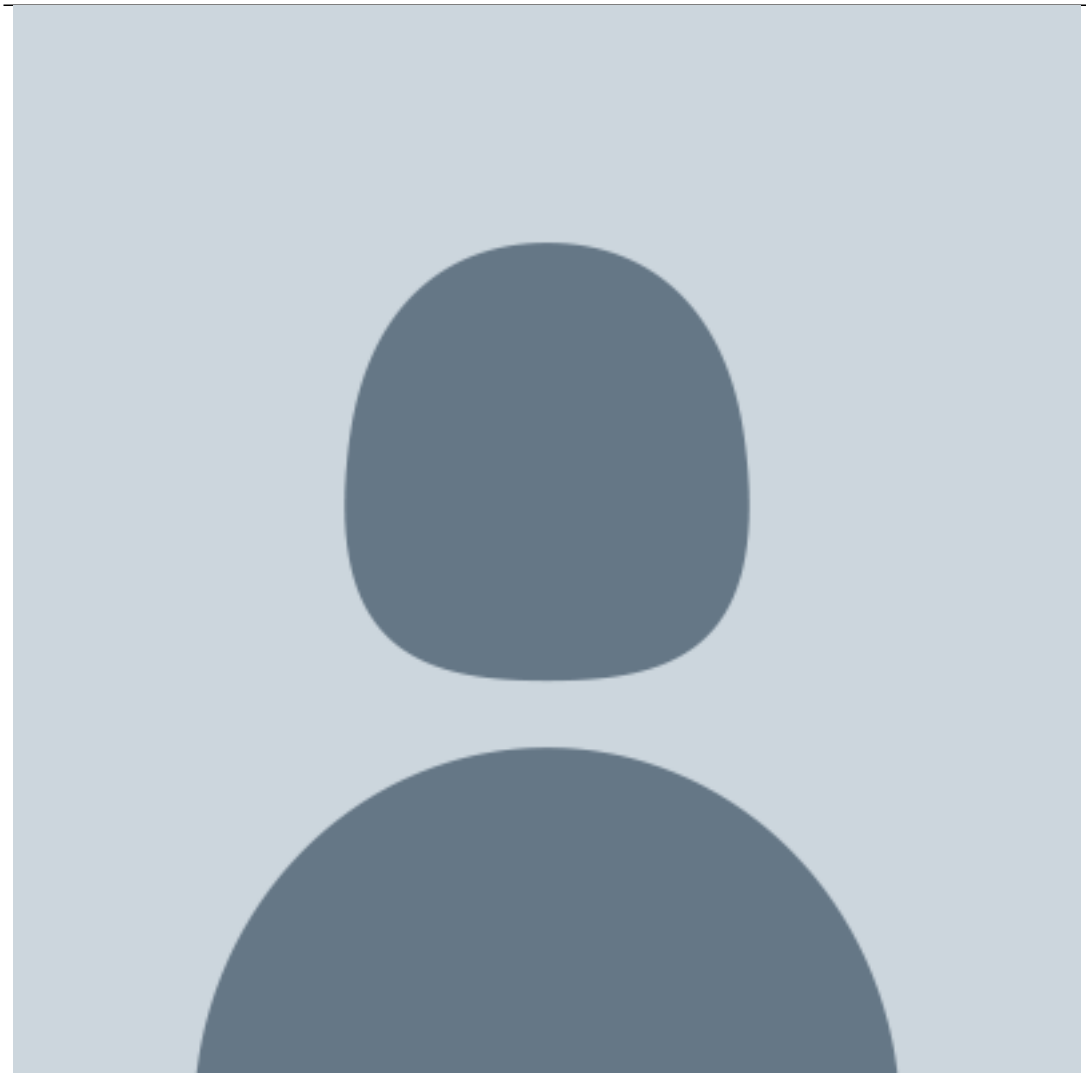
26 The following are the provincial (including the territories of Yukon and Nunavut) legislations: British Columbia: Electronic Transactions Act, SBC 2001, Ch. 10; Alberta: Electronic Transactions Act, S.A. 2001, c. E-5.5; Saskatchewan: Electronic Information and Documents Act, 2000, S.S. 2000, c. E-7.22; Manitoba: Electronic Commerce and Information Act, C.C.S.M., c. E55; Ontario: Electronic Commerce Act, 2000, S.O. 2000, c. 17; Quebec: An Act to establish a legal framework for information technology, R.S.Q., C-1.1; Nova Scotia: Electronic Commerce Act, S.N.S. 2000, c. 26; New Brunswick: Electronic Transactions Act, S.N.B. 2001, c. E-5.5; Prince Edward Island: Electronic Commerce Act, S.P.E.I. 2001, c. 31; Newfoundland and Labrador: Electronic Commerce Act, S.N.L. 2001, c. E-5.2; Yukon: Electronic Commerce Act, R.S.Y. 2002, Ch. 66; Nunavut: Electronic Commerce Act, S.Nu. 2004, c. 7.

27 An Act to establish a legal framework for information technology, R.S.Q., C-1.1. s. 39.

28 Id., ss. 42-68.

29 MASON, supra note 3, at 259; LALANCETTE & MAALAOUI, supra note 4, at 9; CGI Whitepaper, Public Key Encryption and Digital Signature: How do they work?.

Amir Tajkarimi



Banque Nationale