

UECA and Electronic Signatures

by [Peter F. M. Jones](#)

Draft legislation proposed by the Uniform Law Commissioners of Canada, entitled the Uniform Electronic Commerce Act ("UECA"), adopts common law principles to govern signature requirements. Section 1 (b) of UECA defines "electronic signature" as "information in electronic form that a person has created or adopted in order to sign a document and that is in, attached to or associated with the document." The words "created or adopted" clearly refer to the intention of a party signing a document. If such intent exists, and if signature is attached to or associated with the document, the electronic information is a signature for all purposes covered by the Act.

The Explanatory Notes available on the University of Alberta host site give an insight into the considerations that led the drafting group responsible for UECA to take this approach. The objective was to make the definition neutral as between technology that provides information in electronic form that can be adopted as a signature. Another consideration was to keep the legal concept close to the existing law, which does not set any technical standard for the production of a valid signature.

Although it is possible to digitize handwriting so that it is displayed as an image, an electronic signature does not need to "look like" a handwritten signature. A handwritten signature had to be appended to or incorporated in a document, a feature that is no longer a requirement for an electronic signature. The electronic signature may be "associated with" the document, by an algorithm generated by the program that creates an email.

Unlike the UN Model Law on Electronic Commerce, UECA does not demand that an electronic signature meet a test of appropriate reliability. The reasoning is that the law of manual signatures accepts a rudimentary mark as a signature and does not demand a threshold level of reliability failing which a signature is rejected. Attribution of a mark to an individual is required by independent evidence. A person who wishes to rely on any signature takes the risk that proof of attribution is not persuasive, a situation that does not change for an electronic signatures.

The issues of reliability are addressed in another section of UECA. Section 10 (2) enables a For the purposes of subsection (1), the an authority responsible for the legal requirement of a signature may regulations addressing the need for reliable identification of the person signing the document, and the association of the electronic signature with the document allegedly signed.

The Australian State of Victoria has included standards of reliability in its draft legislation governing electronic commerce. Requirements for a signature are satisfied by an electronic signature if having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.

Undoubtedly the drafters of the Victoria legislation considered that a statutory standard of reliability will encourage methods of signature to evolve to a more secure state. The consideration that appealed to the drafters of UECA was that imposing standards will impose a more sophisticated level of electronic signatures than most businesses can master. Rather than discourage use of electronic commerce the choice was to accept a traditional view. One can argue that the traditional view developed in a more static society enabled the external evidence of association of a mark with a person to be presented more easily. That association will be more difficult to prove today, and so in the long run it is better to impose a higher standard as a condition of participation in electronic commerce.

The State of Arizona has enacted laws take the basic approach of the UECA but also provide for secure electronic signatures. A signature is a secure electronic signature if, through the application of a security procedure, it can be demonstrated that the electronic signature at the time the signature was made was all of the following:

1. unique to the person using it.
2. capable of verification.
3. under the sole control of the person using it.
4. linked to the electronic record to which it relates in such a manner that if the record were changed the electronic signature would be invalidated.

The differences between these various laws are just significant enough to require consideration of the country or state in which the electronic transactions will take place. Fortunately the differences are not so great as to make generalizations of little use. Actual court decisions in concrete situations are necessary to decide if further uniformity in the laws is desirable.

June 13, 2000