Implementation of electronic signatures: a discussion on regulatory issues

Raj GURURAJAN
Department of Information Systems
University of Southern Queensland
Toowoomba QLD 4350

ABSTRACT

To address and facilitate the growth of activities in the area of e- and m-commerce, United Nations produced a document called the UNCITRAL Model Law. Article 13 of the Model Law describes the concept of ‘attribution of data messages’, a principal component in ensuring authenticity and reliability of an electronic message. The purpose behind such prescription is to ensure harmony among trading partners as the implementation of regulatory framework in many countries is not uniform and bound by various jurisdictional issues. While conducting transactions across borders, including state and national, trading parties should be aware of various consequences of ‘transmission of electronic messages’ as there may be profound implications to the parties when things go wrong due to technical problems.

When organizations trade on the Internet, especially to conduct transactions at international level, the concept of electronic signatures is an integral part of transactions negotiated through a data message. However, it appears that organizations have not yet comprehended the full impact of various legislative procedures associated with the implementation of electronic signatures as the enforcement of various issues with respect to this electronic signature varies depending upon the context and situation. While the electronic signature helps to identify a person who has been involved in a transaction electronically, due to various technical issues, it is difficult to interpret who is the sender, how to authenticate the signature, how the data message is transmitted, and the validity of enforceable issues.

This paper investigates aspects of United Nation’s Model Law, Article 13, which deals with electronic signatures. The discussion provided includes how electronic signatures are interpreted in the context of a data message, the difficulties encountered in implementing Article 13 in specific contexts due to regulatory frameworks and potential legal consequences. The scope of this paper is currently restricted to ‘discussion’ only.

Introduction

In today’s world, technological advancements have often been cited as the major reason for a paradigm shift towards globalization. Small businesses are becoming increasingly conversant with international regulations due to the advancements in the domain of electronic commerce as these businesses can participate in international activities using Information Technology (IT). While technology facilitates international transactions, there has to be some kind of harmony between trading countries in terms of regulations in order to understand ‘transactions’ between partners in a uniform manner. Without such harmonious regulations, it may not be possible for businesses to get involved in international transactions as the regulatory framework between countries can differ from each other. For example, what is legal in one country may not be legal in another country. Hence, the United Nations created a set of Laws, called UNCITRAL “Model Law” to provide uniform understanding of various
issues of international trade. Due to the rapid growth of electronic as well as mobile commerce, these laws were revised to incorporate a number of new amendments in order to facilitate electronic transactions. Among these, the electronic signatures are important because these laws govern aspects associated with computer-mediated transactions.

Businesses involved in international transactions should be aware of these electronic signature regulations to understand how signature elements in an electronic message are constituted and implemented. If businesses don’t understand the concept behind electronic signatures, then any relative ignorance will lead into potential problems when trading in international domains as the enforcement is not uniform. The purpose of this paper is to provide an overview of different regulations comprising the electronic signatures and how these regulations influence businesses involved in cross-border transactions.

**Electronic Signatures**

When the functions of traditional signatures are transformed into an electronic form, we realize electronic signatures. According to Kuechler (2003) a traditional signature identifies a person; it provides certainty as to the personal involvement of that person in the act of signing; it associates a person with the content of a document; it might attest to the intent of a party to be bound by the content of a signed contract; it might endorse the intent of a person to certify the authorship of a text; it might endorse the intent of a person to associate with the content of a document written by someone else; it might reveal details such as time and date of the correspondence. Signatures play a number of roles in identifying characteristics of a document. It should be noted that in addition to written signatures, a number of other forms of signatures are also available (Deise et al., 2000). These are stamps, perforation, etc. The purpose of these signatures is to provide various levels of certainty. For example, in some countries, there exists a general requirement that contracts for the sale of goods above a certain amount should be signed in order to be enforceable. In addition to these forms, there are occasions when these forms of signatures need to be witnessed by neutral bodies and the evidence of such witness is provided by traditional handwritten signatures. In essence signatures satisfy the authentication requirements for a document (Stowe, 2000). The term electronic signature refers to certain functional aspects of a traditional signature and NOT a scanned form of a signature. Electronic signatures are primarily used to provide reliability and security to electronically transmitted messages. The security and reliability is provided by mechanisms to create an electronic tag that is annexed to the message (McCullagh et al., 1998).

In traditional transactions, where a computer is not involved, it is possible to understand the intent of the transaction. The communication channel is physical and any component that is not understood is clarified before the signature is put on the physical document. It is also possible to ascertain the validity of the signature and intent by involving witnesses, a notary public etc. On the other hand, electronic signatures are a means of identification of a person and of the intent of that person to be associated with that electronic record. The term record refers to a transaction, a contract, a letter or any other form of communication. It may be difficult to involve a notary public or a witness as the transaction is not taking place in one single physical location. Further, it is important to note that the term electronic signature has no universally accepted meaning and is defined differently in various statutes (Judge, 1998).

While using IT for transaction purposes, a range of electronic authentication methods – of varying security and reliability – is available for a person to authenticate an electronic record. For example, the authentication can include typing a name at the end of an email, a personal
identification number and the swiping of a magnetic card, typing passwords, transmitting a
digitized version of a manual signature, encryption of a message using key and biometric
forms (Sneddon, 1998). Article 7 of Model Law developed by the United Nations addresses
a number of issues associated with electronic signatures by focusing on two basic functions
of electronic signatures, namely, the method and the approach in which the method is
established. This article very clearly specifies that the method used to identify a signature
should be as reliable as is appropriate for the purpose for which the data message is generated
or communicated, in the light of all circumstances, including any agreement between the
originator and the addressee of the data message.

While the concentration of this paper is on Article 13, it is important to understand the
color of an electronic signature prior to understanding the anatomy of Article 13. When a
transaction is conducted over a communication medium, such as the Internet, businesses need
to ensure and be satisfied that the transaction is reliable and secure. The reliability is
established in terms of the origin of the transaction, receipt of the transaction message, and
the integrity of the information. In addition to this, the identification of parties involved is
also essential in electronic transactions. The clarity of contents is most crucial. If the contents
consists of garbage characters, then understanding the information is a problem (Wyrough &
Klien, 1998). In electronic transmissions, security is established in terms of authenticity of
the message, whether the person whose name is appears as the bearer, is actually the person
who sent it and whether the message can be reproduced or duplicated by unauthorized users.
Electronic technologies such as transmission protocols and encryption are used to ensure the
reliability and security of the message. Authentication, a component of electronic signature,
is generally defined to establish the validity of the identity of a particular entity in a
transaction. This entity could be a sender or a receiver. Electronic signatures are used to
verify the authenticity of the parties involved by using the cryptic technology to transform the
transaction in a form that is not easily understood. This makes it difficult for others to
understand the contents or the origin of the message in a transaction (Evans, 2000) and hence
it is not possible to tamper with the message meaningfully.

Attributes of a data message

Article 13 of the Model Law describes the attributes of a data message involved in a
transaction. There are 6 specific components involved in this article, which is reproduced
below:

\textit{Article 13: Attribution of data messages}

1. A data message is that of the originator if it was sent by the originator itself.

2. As between the originator and the addressee, a data message is deemed to be that of the
originator if it was sent:

   a) by a person who had the authority to act on behalf of the originator in respect of that
data message; or

   (b) by an information system programmed by, or on behalf of, the originator to operate
automatically.

3. As between the originator and the addressee, an addressee is entitled to regard a data
message as being that of the originator, and to act on that assumption, if:
(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

(4) Paragraph (3) does not apply:

(a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or

(b) in a case within paragraph (3)(b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.

(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

A detailed examination of this article reveals some potential implementation difficulties in an IT environment. According to Point (1) of Article 13, a data message belongs to someone who has originated it. In a physical world, this is the sender. In an IT world, it can be anybody who has access to a computer with access to certain systems. A person can impersonate another having unauthorized access to a computer system. When this happens, things become complicated in a legal viewpoint as evidence is required to establish that an ‘identity theft’ has occurred. In a real life environment, this ‘identity theft’ can be established by certain forensic techniques. One example that comes to mind is the forgery of signatures, which could be detected using traditional forensic techniques. In an IT world, the question as to whether this should be dealt with as a problem of illegal access to computer systems, negligence on the person who is an authorized user of the computer system, lack of support from management to provide physical and logical security to its employees etc needs to be resolved.

When the above concept is applied onto Point (2), the implications become apparent. While this point deals with the explicit authority provided to a third party to act on behalf of a user, such as giving power of attorney or consent to an agent to deal in financial matters, when it comes to electronic transmissions, an unauthorized person can realize a message from a computer system that is not secured. When this happens, according to the legal system, a transaction is completed and parties involved are bound by the conditions of the transaction. The second part becomes important because, if an automated message is programmed, then the users are bound by this automated message. When it comes to abiding time constraints, it
may be possible that a contract can be disputed based on the automated clauses, such as non-availability to receive the contract and comply with its conditions. This clause has an impact on point (4) because of the time frame implications in taking action when the message is not meant to reach a recipient and if so happens, the recipient fails to take action.

Some interesting points arise here. For instance, when family members can enjoy the benefits of a company car, could they enjoy the same benefits with a data message and the tools used to produce these data messages? This will be discussed in detail later.

Point (3) states that if the addressee applies procedures that he or she regards as appropriate to ascertain the identity of the originator, then the attribution is completed. However, due to ever increasing security loop holes, it may not be possible to ascertain the originator’s details beyond doubt unless it is certified by a third party, similar to a witness or a notary public. How can we establish such procedures in an electronic transaction? While the concept of certifying authorities (CA) is emerging, there are some implementation difficulties, as discussed later.

Point (5) states that if the addressee knows of any errors in the transmission, then the message can be discarded and there is no binding between parties. End users may not have sufficient knowledge to ascertain whether a message is delivered due to any technical fault at either ends of transmission; whether any attachment is not delivered due to lack of server capabilities; filters could be employed to block big file sizes; incompatible versions; and technical faults at the service provider end.

A closer look at the six points gives a feeling that it is assumed that the technology is stable and there won’t be any glitches due to technical faults. However, in a real life environment, it is not possible to deliver messages always due to technical issues such as bandwidth limitations. In certain cases, the sender or receiver may not be notified as to the technical snags that occur from time to time. Due to the combination of all these issues, the basic assumptions made in this Article appear to be invalid. This is elaborated in the following sections.

**Australian Government Initiative(s)**

The Australian Government closely followed the UNCITRAL Model Law while drafting the transactions act. Articles 2 and 3 of the November note and Article B of the December note are drafted in accordance with Article 7 of the Model Law. According to the Model Law, the electronic signature is reliable for the purpose for which a data message was generated or communicated, including any relevant agreements. The Australian amendments stipulate that the electronic signatures comply with any legal requirements. This is a substantial advancement. It is important to note that the Model Law does not dictate the clarity of electronic messages.

Draft article 4 of the November Note\(^1\) of Australia’s Transaction Act provides details on enhanced signatures. According to the transactions act, an enhanced electronic signature is presumed to be that of the person by whom, or on whose behalf, it purports to have been generated. This presumption can be rebutted when the signature was applied neither by the purported signer nor by a person authorized by the purported signer. The December note of the transactions act does not deal with attribution. However, it was recognized that a decision

\(^1\) Hereafter referred as November Note
needs to be made on whether this issue should be left to national law or dealt with in the Uniform Rules.

There is an important point here. It is the need for specific attribution rules. If there is a necessity for specific attribution, then the relationship between this draft article and article 13 of the Model Law, which sets out the rules for the attribution of a data message, needs to be explained.

**Data Messages integrity**

When Article 13 is interpreted, other articles that are having a bearing on this article should also be considered to derive a complete picture. For instance, Article 5 establishes a presumption as to the integrity of a data message. This article stipulates that “where evidence is available that a signature and/or security procedure has actually been applied with a result, which shows that there has been no change to the message”. A closer examination of Article 5 shows that there is a need for further clarification because it is unclear whether the presumption is directed towards originality or authenticity. While the originality refers to the contents, the authenticity refers to the origination of the content. As mentioned in the opening paragraphs, Article 8 of Model Law deals with the requirements to produce information in its original form (content). While Article 5 discusses message integrity in terms of technical interference, it has a bearing on the originality as well. It can be argued that document forgery is perhaps implied here as it is possible to forge a document in physical world. In electronic world, it can be argued that, it is possible to change the contents without parties involved being aware of such changes and this is the intent of this Article (Article 5). However, the relationship between Article 5 and Article 8 of the Model Law is unclear and raises a few questions.

For example, Article 8 deals with compliance with requirements for an original. According to Australian regulations, it is not clear whether an integrity function is an integral part of forms of electronic signatures. Further, it is not possible to assume that a signature technology may satisfy the integrity function because of different operational modes. Accordingly, there does not appear to be a case for uniform implementation.

**Duty of a signature holder and the consequences of a breach of these duties**

Article 13 is developed so as to establish the duties of the person who is a signatory to a data message. All the components imply this and how to interpret the generation of a data message. It is generally agreed that a signature holder will have a duty of care to avoid the unauthorized use of his or her signature. In contracts, this is a binding feature. Further a signature holder will also prevent the recipient from relying on an unauthorized use of his or her signature. However, there is no consensus on the consequences which are to follow from a breach of this duty of care, or even whether such a statement of the duty of care needs to be contained. While reading the Australian legislation, it is understood that the signature holder is responsible for the consequences of breaching these obligations, but it is left to the state laws to determine the nature of those consequences. Realizing the implementation difficulties of such a system, the Australian regulations provided an alternative approach, reflected in Article 7. This Article specifically sets out the consequences of breaching those obligations.

In the Australian context, one clear problem with specifying the consequences of breaching the obligation is considering how a provision like Article 7, which establishes a liability rule
for the attribution of a signature, relates to article 13 of the Model Law on the attribution of a data message. In physical forms, liability may directly address acts such as negligence. In an electronic world, this can’t be confused with problems arising from transmission of data messages as technology plays an important role in delivering data messages. It appears that the Australian version of the Model Law confused the issue by specifying details on consequences of breaching prior to defining attribution of data messages. It is important to avoid confusion, in cases of signed data messages, as to which provision should be used to attribute the data message and deal with liability (Article 8 or Article 13). While some components of Australian legislation clearly link Article 13 of the Model Law to reliance on an enhanced electronic signature, others create confusion between the ‘content’ and the ‘originality’. Moreover, a provision would also need to provide details of the appropriate allocation of risk most likely to promote secure electronic transmission. It may be that the standards of care are not clear enough to support a rule based on negligence. Further consideration is needed here.

**Obligations of an information certifier**

The obligations of information certifiers are set out in the form of minimum standards in the Model Law and this appears to be reasonable. However, when it comes to liability issues, the details are not clear. For instance, Model Law indicates that the standard of liability is to be borne by an information certifier when attribution clauses are not resolved properly. The assumption made is that the certifier is responsible to certify users of electronic signatures, annexed to the data messages, and that this process is sound and fool-proof. However, when the parties are relying on the information certifier, the burden of proving breach of the obligations lies with the parties and NOT the information certifier who certifies the information. The information certifier also certifies the quality of content including signatures because contents originate from user’s machines. When technology is applied to this concept, users use their login details and hence the information certifier is able to understand from where the information or content is generated. However, as many businesses may not possess sufficient technical abilities, this will add unnecessary costs to businesses (Wyrough & Klien, 1998).

A related issue to consider is whether an information certifier and a certificate holder should be able to agree to limit their liability by contract, as suggested by the Australian version of the Model Law. The inclusion of this rule reflects, in part, an awareness of the need to encourage the information certifier market, while recognizing that there is a possibility that the risk of liability may be unfairly shifted to the holder of a certificate. Businesses should be aware of this.

In addition, it is not clear whether party agreements limiting liability should be subject to applicable domestic laws. One view is that some legal systems do not recognize the rights of parties to vary liability by agreement, meaning that subjecting an agreement to limit liability to domestic law would result in an excessively narrow application of the Uniform Rules. When businesses cross national boundaries, confusion arises even further (Desai, 1999).

What happens once references to party agreements concerning liability limits are deleted from the contractual agreements? This may result in an unlimited ability to limit or exclude liability. This issue relates to the issue of party autonomy. Another issue to be considered is whether the Uniform Rules should set out the obligations of an information certifier and the consequences that follow from any breach of these obligations, or whether any or all of these matters should be left to each State's law. Australian regulations set out in detail the
obligations of certification authorities and their liability for not satisfying those obligations and deals generally with the obligations of information certifiers by providing minimum standards and leaving the consequences of failure to satisfy the standards to national law (Desai, 1999). When disputes occur at international transaction level, this may create unnecessary problems to businesses as regulations with respect to liabilities differ among countries.

**Legal Consequences**

When businesses trade in international domain, they should be aware of the number of legal issues binding the concept of signature and the undecided issues influencing electronic signatures. Three issues become pertinent in this context. They are:

1. What is the stature of electronic signature in data messages?
2. Can we accept them as a signature always in data messages?
3. What is the role of witnesses in the context of data messages?

It has already been mentioned that a signature is only an authentication. In other words, a signature serves the purpose of a mark. The legal requirement is that the mark be made by the person on the document or by authority in order to satisfy legal requirements. When the signature is not needed to be an autograph, then a printed name is enough to satisfy the legal requirements. In certain cases, stamps can be used to satisfy legal requirements. In certain cases, the stamp is supported by the signature of the person (Dang, 2000).

There are three important points to note here. First, to constitute validity of a person’s signature, there is no need that the person should physically act by putting signature on the document. For example, this can be achieved via an agent. The second point is the signature assures the authenticity of the genuineness of a document. The third point is that the person must put his or her mind to the act of signing the document in order to be bound. Compulsion does not form the component of act and hence it may not be possible to bind the person and his signature (Lovell, 2000).

The fist point establishes that the concept of electronic signatures is valid and can be accepted. The current technology can perhaps assure the second point in the above paragraph. However, when the third point is considered, it is difficult to accept electronic signatures comparable to traditional signatures.

When electronic documents are sent through computers, it may be possible for an anonymous person to access computers in an unauthorized manner. For instance, when person A is operating a computer and when person A leaves the computer accessible by others, a person B can transmit a document using person A’s facilities (Kuechler & Grupe, 2003). This can happen in cases such as email documents.

In addition to this, it is possible for the document to be captured while in transmission and modified without the knowledge of the sender (Clarke, 2003). This may by mistake bind the sender to the contents of the document. In this case, the electronic signature cannot be accepted equivalent to the traditional signature. This is because, in traditional media, any modification can be detected and hence the concept of signature is valid in traditional media. However, the same can’t be said for electronic media because copies can be made easily.
Further, there used to be a school of thought that anything produced by a computer is a copy from the memory and the original is not released. When this argument is applied, the concept of original doesn’t find a place in data messages and hence the concept itself is rejected (Labkoff et al., 1997; Maini, 1998).

In traditional cases, a witness will be able to read the document and then sign the document. In certain cases, the witness will be able to attest a document to guarantee that the person who signs the document is the person in question. In other circumstances, notary public and authorized officials will be able to carry out these duties. The purpose of witness is to avoid any potential forgery. The role of witnesses is crucial in documents such as deeds (McCullagh et al., 1998).

When a dispute arises, usually the document in question is put before a court along with the witnesses. The court will inspect the document and cross-examine the witnesses in the process of settling the dispute. Witnesses are usually aware of this procedure.

In the case of traditional transactions, witnesses sign the document on their own. The act of signing or stamping is conducted according to their will and they engage themselves with complete knowledge in doing so. The signing is to endorse the person who is going to be bound by the document and NOT to endorse the contents.

This raises an interesting question. Is it possible for an attester to witness an electronic signature? In the traditional process, a witness understands the concept of writing and the concept of stamps. The process is well understood and in existence for centuries. When the same process is conducted in an electronic media, the process need not have to be straightforward. What the computer screen displays and what is actually retained in computer memory may be two different things. Further, the execution of certain keystrokes may be beyond the comprehension of the attester and these keystrokes can generate electronic signatures. The witness may not understand the process of generating electronic signatures and associated security issues in order to ensure that the electronic signatures refer to the person who is actually initiating them. The keystrokes involved will not reveal the true processing sequences in generating the electronic signatures. Therefore, it can be said that the witnesses do not engage themselves fully in the operation. This area needs more discussion in terms of legal consequences and technical development (McCullagh et al., 1998).

It should be noted that the current regulations do not provide any solution to this problem.

**Some General Legal Issues**

One of the principal legal issues raised by electronic signatures and data messages is the task of adapting existing legal and evidentiary requirements to the new means of contracting and communicating. Due to the number of intermediaries playing an active role in completing a transaction, it is essential to establish and determine the place and time of the contract in resolving disputes. When a contract is drawn using the traditional processes, the place and time stamps are automatically recognized. In addition to these stamps, a notary public will be able to authenticate the parties involved. However, when it comes to online contracts, which is popular in electronic commerce, these procedures may not be applicable (Desai, 1999).

Businesses face a major problem here. For example, when an insurance policy is taken by a business, the insurance intermediary’s computer can automatically generate an acceptance of
customer details and can generate a cover note. This cover note then can be sent to the customer. In this process, there is no human intervention. What happens if the computer generates some garbled message? Who is responsible for such garbled messages? Who is bound by these messages? Who is responsible (sender, ISP or another body involved in transmission) for errors generated in the overall processes? The transactions act does not control this.

The second problem that faces the businesses is the issue of proof. In an electronic transaction, such as the one mentioned above, how can one establish the identity of the offeror and offeree? What happens when a person other than the owner or authority of the computer sends an electronic message causing damages? The transactions act does not stipulate this clearly.

How can businesses reduce the legal risks when trading using electronic commerce techniques? Businesses should be aware of various legal issues in the area of contracts, how they are developed and generated, what are the binding agreements, the concept of authenticating parties signing the contracts and other international regulatory issues.

**Conclusion**

Despite the technical development in the domain of regulatory framework, it appears that there are difficulties in fully understanding and implementing the concept of electronic signatures as they pose a problem at the time of enforcement. Due to certain domestic understanding of the concept of signatures, the implementations of digital signatures vary between countries. While national laws attempt to address the problems in their jurisdiction, businesses may find it impossible to apply the national regulatory framework to international disputes.

The United Nation’s Model Law provides some form of solution by recognizing the fact that there should be very close functional alignments between the concept of traditional signatures and electronic signatures. However, what is not fully functional is the implementation system. Irrespective of the recent and encouraging developments in the area of electronic signatures, it is concluded that more concentrated effort is needed to arrive at perfection in implementing the centuries old traditional signature system. While such a system is slowly emerging, a trusted path between the memory and devices generating electronic signature should be established, in addition to the development of new software applications capable of verifying signatures in order for third parties to witness and attest electronic documents.

While electronic signatures and data message attribution will play an essential role in transactions facilitated by emerging technologies such as handheld devices, organizations need to understand their scope and limitations in order to realize benefits. It appears that organizations are having difficulty in implementing these concepts as many of them lack appropriate resources. The concepts discussed in this paper are being investigated further in order to assess the awareness of article 13 and related articles with a specific focus on regulatory frameworks. The subjects of the investigation include industries, consumers and government agencies in order to determine the general awareness and any challenges encountered in implementing electronic signatures in data message transmission.

**Reference**


