UNCITRAL & Electronic Signatures: A Light Touch at Harmonisation

Indira Carr
Reader in International Commercial Law, University of Kent, Canterbury; Senior Visiting Fellow, Institute of Advanced Legal Studies, London, Visiting Professor, University of Hertfordshire.

The first objective is to build trust and confidence. For e-commerce to develop, both consumers and businesses must be confident that their transaction will not be intercepted or modified, that the seller and buyer are who they say they are, and that transaction mechanisms are available, legal and secure. Building such trust and confidence is the pre-requisite to win over businesses and consumers to e-commerce.

Introduction

On July 5, 2001 UNCITRAL approved the Model Law on Electronic Signatures (hereinafter Model Law) thus completing Phase I of its programme for the facilitation of electronic commerce (e-commerce). By no means the first, it owes much to the American Bar Association Guidelines on Digital Signatures, the variety of legislation validating electronic signatures passed at the state level in the United States, and the European Directive on Electronic Signatures.

The Model Law on Electronic Commerce 1996 as amended 1998 is the other document that has received worldwide success. Countries such as Australia, Bermuda, Colombia, France, Hong Kong Special Administrative Region of China, India, Ireland, Philippines, Republic of Korea, Singapore, Slovenia have based their legislation on the Model Law. The issue of signatures was addressed by the Model Law on Electronic Commerce and Article 7, founded on the functions of a signature provides:

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if
   (a) a method is used to identify that person and to indicate that person’s approval of the information contained in the data message; and
   (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies where the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

The Model Law on Electronic Commerce however did not deal with issues such as reliability, certification processes, the liability issues of the various parties involved in the creation and use of electronic signatures. Hence the drafting of the Model Law on Electronic Signatures.
Electronic Signatures. It is trite to extol the virtues of the IT (information technology) revolution, its ability to shrink space and time, to bring people together without traversing long distances, to create new marketplaces and to contribute to global economic growth. The positive effects of e-commerce for the economy have been rehearsed and voiced in the policy documents of states and regional groupings, eagerly welcomed by the commercial community and enthusiastically celebrated by the media. Peculiarities of the digital medium (e.g. intangibility) however raise a number of issues at the legal level and concern that legal uncertainties may act as a barrier to e-commerce.

E-commerce is commonly defined as trade that takes place over the Internet with a buyer visiting the seller’s website and includes business-to-business (B2B); business-to-consumer (B2C), consumer-to-business (C2B) and customer-to-customer (C2C) trade. Many of the events and factors associated with a contract such as pre-contractual negotiations, offer, acceptance, terms of the contract are conveyed and stored electronically. Numerous questions relating to, for instance, authenticity, integrity and authentication immediately come to mind when the electronic medium is used for concluding contracts. For instance: Can the electronic message be trusted? Does it originate from the person claiming to send it? Can the message be relied upon? How secure is the message given that electronic documents can be easily manipulated? Is the received message the same as the message sent? What legal status does an electronically signed message have? Can a sender be held to his electronically communicated message should a dispute arise? Is it enforceable? Do electronic messages and electronic signatures meet the legal requirements of writing and signature?

IT professionals, as far back as the 1970s, were working on the confidentiality/integrity problems associated with electronic communications. Asymmetric cryptography was seen as providing the required level of security and systems such as Pretty Good Privacy (PGP) and Secure Sockets Layer (SSL) for encrypting data came to the fore. As opposed to symmetric cryptography, which uses the same key to encrypt and decrypt a message, asymmetric cryptography uses a pair of keys - a private key and public key - that are related mathematically. The private key kept by the owner is used to encrypt the data and the public key, available to those with whom he wishes to communicate, is used to decode the data. Associated with certificates issued by trusted third parties/certification service providers this technology could be used for establishing the identity of the sender and for authentication. Hailed as a digital signature (a digital answer to a handwritten signature) and expecting widespread adoption, legislators rushed to pass legislation authorising the use of this technology to meet the signature requirements prescribed by law. For instance, the Utah Digital Signature Act defines a digital signature by reference to this technology as a “transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer’s public key can accurately determine whether (a) the transformation was created using the private key that corresponds to the signer’s public key;
and (b) the message has been altered since the transformation was made.”\(^{13}\) While digital signature is a type of electronic signature,\(^ {14}\) confusion reigned, with some using ‘digital signature’ in a wider sense to mean electronic signature.\(^ {15}\) It was against this backdrop that UNCITRAL set out to work on its Model Law on Electronic Signatures with the intention of harmonising the law without resorting to the promotion of a specific technology.

This article sets out the founding principles of the Model Law and examines the various provisions. It concludes that the Model Law, while providing a workable framework, is by no means comprehensive. It leaves a lot for the state adopting the Model Law to work out what may be core legal issues - for instance, the type and levels of liability - thus making it a weak attempt at harmonisation.

**Founding Principles**

*Harmonisation and certainty*

Harmonisation at a global level, which also has the added advantage of imparting certainty, is at the heart of the Model Law. International conventions,\(^ {16}\) the most effective way to achieve harmonisation, have their shortcomings. Fuelled by politics, differences in legal systems and legal understanding and intranslatability of concepts at the linguistic level international conventions face interminable delays at the drafting stage. Once the text is agreed it may take years for it to go through the various bureaucratic processes at the state level for it to be ratified, and the required numbers of ratification for it to come into force.\(^ {17}\) Further, conventions may not attract widespread ratification due to their inflexibility. States may wish to opt out of certain provisions, which might not be possible under the convention. Of late, UNCITRAL (perhaps as a political move to maintain its status in the international arena as a major law making organisation in international trade matters) has been moving more towards drafting model laws\(^ {18}\) - that is, recommendations made by a body composed of government representatives and experts such as practitioners, and academics. While the differences in legal understanding cannot be totally cured, model laws; by comparison do not share bureaucratic nightmares or rigidity to the same extent.\(^ {19}\) They do not require the requisite numbers of ratification to come into force and States, while free to adopt the model law *verbatim*, may amend it to suit their needs, or use it as a framework for drafting their legislation. This level of flexibility increases the chance for widespread adoption, albeit at the cost of a high degree of harmonisation.\(^ {20}\) Widespread adoption should also contribute to certainty about the legal force of electronic signatures.

\(^{13}\) Also see Oregon Electronic Signature Act, Oregon Revised Statutes § 192.825; Nevada Revised Statutes: Chapters 720 Title 59. The various definitions of digital signatures are available on http://www.mbc.com/ecommerce.

\(^{14}\) It also includes PIN (Personal Identification Numbers) and biometrics based identifier such as a fingerprint.

\(^{15}\) See Texas Business and Commerce Code § 2.108.


\(^{17}\) For instance, the text of the United Nations Carriage of Goods by Sea (a.k.a the Hamburg Rules) drafted by the UNCITRAL and adopted in 1978 took fourteen years to come into force.


\(^{20}\) Paras 26-28.
**Party Autonomy**

In the absence of legal solutions to uncertainties it is not unknown for parties to a business transaction to agree to solutions in the contract. The Model Law preserves party autonomy. It is not mandatory in character and provides for variation by agreement subject to any limitations that may be imposed by the applicable law - for instance, on grounds of public policy. This principle is embodied in Article 5 which states that “[i]t he provisions of this Law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law”. Articles 3, 6 and 12\(^21\) in specific further reinforce the principle of party autonomy expressed by Article 5. While Article 5 does not indicate whether the agreement should be express or implied, the Draft Explanatory Memorandum makes clear that variation by agreement may be express or implied.\(^22\) Factors such as behaviour of the parties and past course of dealings would therefore be relevant to determine whether there is variation by agreement.

**Technology Neutrality and Non-Discrimination**

From the start, the issue of whether the electronic authentication legislation should be technology specific - referring to a particular type of technology such as asymmetric cryptosystem that uses private-public key pair - or technology neutral has been scrutinised closely by legislators. Technology specific legislation has the advantage of promoting legal certainty but is inflexible to accommodate new technology and legislation is likely to become quickly outdated if new technologies are adopted by the market place. Technology neutral legislation that is open textured, on the other hand, has the flexibility to adapt itself to new developments. Further, it does not stifle competition or innovation by giving preference to a specific technology.\(^23\) The Model Law is founded on the principle of technology neutrality as indicated by Article 3 which states that [n]othing in this Law … shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in article 6(1) or otherwise meets the requirements of applicable law”\(^24\). The Draft Explanatory Memorandum also makes clear that Article 3 “embodies the fundamental principle that no method of electronic signature should be discriminated against …[and] [t]he fundamental principle of non-discrimination is of general application”\(^25\) subject of course to the principle of party autonomy.

The principle of non-discrimination also encompasses cross-border recognition of electronic signatures and certificates for legal purposes. The place of origin of electronic signatures and certificates is not to contribute to determining the legal effectiveness of an electronic signature or certificate.\(^26\)

**Functional Equivalence**

The UNCITRAL adopts a ‘functional equivalent approach’ in drafting its legislation - an approach that extrapolates the functions of a paper document\(^27\) to create the criteria that need to

---

\(^{21}\) See below.  
\(^{22}\) Para 112.  
\(^{25}\) See below.  
\(^{26}\) See Sections E - paras 15-18 of Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce. It describes the functional equivalence approach as “based on analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes and functions could be fulfilled through electronic techniques”. As an illustration: “among the functions served by a paper document are the following: to provide that a document would be legible by all; to provide that a document would remain unaltered over time; to allow for the reproduction of a document so that each party would hold a copy of the same

© Indira Carr 2003  
The moral rights of the author have been asserted  
Database Right The Centre for International Law (maker)
be met by the paperless document for attaining a status equivalent to that of the paper document.  

The Model Law on Electronic Signatures

Interpretation

Before proceeding with an assessment of the Model Law a few words must be said about its interpretation. As part of the drive towards harmonisation and certainty, it includes an interpretation provision inspired by Article 7 of the Convention on the International Sale of Goods 1980 (also drafted by the UNCITRAL). According to Article 4, in interpreting the Model Law “regard is to be had to its international character and to the need to promote uniformity in its application and the observance of good faith”. While the provision is rational in a global world promoting transnational law it is difficult to assess what exactly is expected of a court or tribunal under Article 4? If legislation based on the Model Law becomes part of domestic law, are the courts expected to disregard rules of interpretation formulated and developed in their legal system? Are they to disregard the interpretation of identical words in other domestic legislation? Are they to explore how courts in other jurisdictions interpret the provisions? Are the judges expected to rid themselves of the conceptual framework derived from their own domestic law? In an ideal world, in aiming towards harmonisation it makes sense to leave the shackles created by sovereignty. However, there is a gap between theory and practice as experience with the Convention on the International Sale of Goods, 1980 (hereinafter the Vienna Convention) illustrates. In spite of the extensive case database maintained by UNCITRAL on the Vienna Convention (and available on their website) there is a reluctance on the part of courts to refer to opinions from other jurisdictions as an aid to interpretation. According to Murray judges tend to interpret the Vienna Convention, in spite of Article 7, with a ‘domestic legal lens’. This view is equally backed by scholars with a civil law background. For instance, Bonnell and Liguori state that “very rarely do decisions take into account the solutions adopted on the same point by courts in other countries.” If the response to Article 7 of an international treaty is so negative, what hope is there for an interpretation provision in a model law? Having said this, reference must be made to recognition of the international nature of conventions and the need to refer to foreign judgements on the part of British judges. For instance, even in the absence of an interpretation provision in the Hague Rules, the House of Lords in Stag Line Ltd v Foscola, Mango and Co took the view that the interpretation of international conventions should not be rigidly controlled by domestic precedents of antecedent date but that the language should be construed on broad principles of general acceptance. Similar sentiments have been expressed in the interpretation of other international transport conventions. In Corocraft Ltd v Pan American Airways Inc, Lord Denning said “even if I disagreed, I would

data; to allow for the authentication of data by means of a signature; and to provide that a document would be in a form acceptable to public authorities and courts … in respect of all the above-mentioned functions of a paper, electronic records can provide the same level of security as paper and, in most cases, a much higher degree of reliability and speed …”. As UNCITRAL notes, however, in adopting a functional equivalent approach one must not impose stringent standards of security on electronic commerce users than in a paper-based environment. (Para 16).

See Nature an Reliability of an Electronic Signature below for the functions identified for a handwritten signature.

It states: (1) In the interpretation of this Convention, regard is to be had to its international character and to the need to promote uniformity on its application and the observance of good faith in international trade. (2) Questions concerning matters governed by this Convention which are not expressly settled in it are to be settled in conformity with the general principles on which it is based or, in the absence of such principles, in conformity with the law applicable by virtue of the rules of private international law.


[1932] AC 328.

© Indira Carr 2003
The moral rights of the author have been asserted

Database Right The Centre for International Law (maker)
follow [decisions of other courts] in a manner which is of international concern. The courts of all countries should interpret [the Warsaw Convention\textsuperscript{33}] in the same way.”\textsuperscript{34}

The latter part of Article 4 makes reference to the observance of good faith. Good faith in what, by whom and at what stage? Are the parties to observe good faith in the use of electronic signatures? Where parties vary the terms by agreement are they bound by the principle of good faith? Are the parties to observe good faith in the performance of contracts that use electronic signatures? Are they to observe good faith during pre-contractual negotiations? Or, does it mean that the judiciary must take in good faith the interpretation of the Model Law in other jurisdictions? Is acting in good faith the same as acting reasonably? Impregnated with a moral flavour, good faith is a vague term that every one comprehends and does not comprehend at the same time. The Draft Explanatory Memorandum is of no help. In importing Article 7 of the Vienna Convention with a few changes the drafters have unwittingly brought into the Model Law the controversy and debate that is still raging around the good faith part of Article 7. Honnold, on the basis of its drafting history, is of the view that good faith relates only to the interpretation of the Convention while Schlechtreim is of the opinion that it is a general principle. And the developing interpretation in case law seemingly favouring good faith in contract performance has not been widely followed to give a decisive answer. So, are we likely to see a similar trend with the Model Law?

\textbf{Applicability}

The Model Law applies to electronic signatures that are used in the commercial sphere.\textsuperscript{37} Following the definition adopted in the Model Law on Electronic Commerce, the word ‘commercial’ is defined in a footnote to Article 1, and is interpreted widely to cover matters that arise from commercial relationship, be it contractual or not. Commercial relationships include “any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint ventures and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.” Though doubts may be raised, in the absence of specific mention, about its applicability to consumers, the second sentence of Article 1 states that it is not meant to override any consumer protection law, thus suggesting that the Model Law is not meant to exclude consumer transactions. The Draft Explanatory Memorandum endorses this view by stating that the provisions of the Model Law may be beneficial for consumer protection but goes on to state that dependent on existing consumer protection policies, legislators may wish to exclude consumers from the sphere of application.\textsuperscript{38} The Model Law does not define ‘consumer’ and leaves that to be determined by the applicable law.

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{33} Convention for the Unification of Certain Rules relating to International Carriage by Air 1929.
\item \textsuperscript{34} [1969] 1 QB 616 at 655.
\item \textsuperscript{35} Honnold, \textit{Uniform Law for International Sales under the 1980 United Nations Convention} 3\textsuperscript{rd} ed (1999).
\item \textsuperscript{37} Article 1 reads: “This Law applies where electronic signatures are used in the context of commercial activities. It does not override any rule of law intended for the protection of consumers.”
\item \textsuperscript{38} A/CN 9/WG IV/WP 88 para 90.
\end{itemize}
\end{footnotesize}
Nature and Reliability of an Electronic Signature

As stated earlier, the UNCITRAL followed a ‘functional equivalence’ approach for formulating both the Model Law for Electronic Commerce and Electronic Signatures. Among the functions for a handwritten signature identified by the Working Group are: “to identify a person; to provide certainty as to the personal involvement of that person in the act of signing; to associate that person with the content of a document.” Depending on the nature of the document signature, they also identified other uses: “to attest to: the intent of a party to be bound by the content of signed contract; the intent of a person to endorse authorship; the intent of a person to associate itself with the content of a document written by someone else; the fact that, and the time when, a person had been at a given place.” However, in order to define electronic signature for the purposes of the Model Law, the drafters took the smallest common denominator, these being the identification and the intent to sign. Article 2(a) defines electronic signature as “data in an electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory’s approval of information contained in the data message”. Data message refers to information that is sent, generated, received or stored by electronic, optical or similar means. It includes, but is not limited to electronic data interchange (EDI), electronic mail, telegram, telex or telecopy.

The definition of electronic signature is open ended and does not promote any specific technology. The electronic signature could be a digital signature, a digitised image of a handwritten signature or based on biometrics such as a fingerprint or iris scan. The level of security will vary depending on the type of electronic signature. For an electronic signature to be legally effective the Model Law requires electronic signatures meet the requirements of reliability in the light of all the circumstances including any agreement there might be between the parties. Similarly, the definition of data message with its reference to ‘similar means’ is sufficiently flexible to encompass new technological developments. Reliability requirements for a legally effective electronic signature are stated in Article 6(3). First, the signature creation data must be linked to a signatory and no other person; second, the signature creation data at the time of signing must be under the control of the signatory and of no other person, any alteration to the electronic signature after the time of signing is detectable, and where the legal requirement for a signature is for ensuring the integrity of the information to which it relates, any alteration made after signing is detectable. Issues such as whether the signature creation data is uniquely linked to or under the control of the signatory, or for that matter, the question of whether any alteration is detectable after signing are technical issues and will depend on the technology and the mechanisms that have been put in place by the signatory and the certification service provider. For instance, whether the signatory has sole control of the signature creation data will depend on the specific circumstances. To illustrate, where signature creation data is available on a network and is

39 See above.
40 A/CN 9/WG IV/WP 88 para 29.
41 Article 6(1) states: Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.
42 Article 6(3) reads as follows: An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph (1) if:
(a) the signature creation data are, within the context in which they are used, linked to the signatory and no other person;
(b) the signature creation data are, at the time of signing, under the control of the signatory and of no other person;
(c) any alteration to the electronic signature, made after the time of signing, is detectable; and
(d) where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.
43 Refers to codes that are used to link the electronic signature to the signatory.
capable of being used by any number of people, for the Model Law to be applicable it is essential that there is one signatory who maintains control over the signature creation data.  

Without intending to affect the principle of party autonomy, the Model Law makes room, in its Article 7, for the enacting state to designate a public or private authority to specify the types of electronic signatures that would meet the reliability criteria set out in Article 6 subject to the proviso that the recommended technology meet recognised international standards. The Explanatory Memorandum makes clear that the standard is not to be interpreted restrictively and is not confined to standards set by the ISO or IETF. It includes trade usages, industry practices, recommendations from international organisation such as the ICC and UNCITRAL. While trade usages are unlikely to raise eyebrows among Western commercial interests, inclusion of trade usages, for instance, in Article 9 of the Vienna Convention was fully debated during the preparatory stages. Developing countries feared that trade usages, which could include locally adopted usages, would be to the detriment of their traders since they introduce a surprise element into the contract. Hence Article 9(2) makes reference to internationally known usages thus minimising the risk of uncertainty associated with trade usages. The Draft Explanatory Memorandum to the Model Law does not state that trade usages have to be internationally known. The requirement in Article 7 that the recommended technology meets international standards however seems to suggest that trade usages also need to have an international status.

Responsibilities of the Parties

The UNCITRAL envisages three parties taking part in the use and creation of an electronic signature:
- the signatory, who is the holder of the signature creation device;
- the third party (known as the certificate service provider) who plays a central role in adding integrity to the electronic signature by issuing certificates that confirm the link between the signatory and the signature creation data; and
- the party who relies on the electronic signature.

Unlike other recent legislation on electronic signatures - for instance, the EU Directive on Electronic Signatures - the Model Law imposes responsibilities on all three actors engaged in the use and creation of an electronic signature that has legal effect.

44 See paras 119-123 A/CN 9/WG IV/WP 88
46 Internet Engineering Task Force.
47 International Chamber of Commerce.
48 A/CN 9/WG IV/WP 88 para 130.
49 It reads:
(1) The parties are bound by any usage to which they have agreed and by any practices which they have established between themselves.
(2) The parties are considered, unless otherwise agreed, to have impliedly made applicable to their contract or its formation a usage of which the parties knew or ought to have known and which in international trade is widely known to, and regularly observed by, parties to contracts of the type involved in the particular trade concerned.
50 They also perceived trade usages largely as a product a limited number of countries from the Western world, a view shared by the socialist countries.
51 Defined in Article 2(d) as “a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents”.
52 Defined in Article 2(e) as “a person that issues certificates and may provide other services related to electronic signatures”.
53 Defined in Art 2(b) as “a data message or other record confirming the link between a signatory and signature creation data”.
54 Relying party defined in Article 2(f) as “a person that may act on the basis of a certificate or an electronic signature”.
55 See Article 6 of the Directive which imposes liability on the certification service provider in relation to a qualified certificate.
The signatory, as the holder of signature creation data that creates signatures that have legal effect, is expected to keep it under his control and take reasonable care to avoid its unauthorised use.\textsuperscript{56} The issue of whether he has exercised reasonable care or not will presumably be determined on an objective basis. The signatory is placed under an obligation to use the means provided by the certification service provider or use reasonable efforts to inform those who are likely to rely on the electronic signature where he knows that the signature creation data has been compromised, or his knowledge of circumstances raise a substantial risk that the signature creation data may have been compromised. He is also to ensure that material representations made by him that are relevant to acquire a certificate are accurate and complete during the life cycle of certificate. From the Draft Explanatory Memorandum it appears that the life cycle of a certificate runs from the application to the revocation or expiry of a certificate.\textsuperscript{57} Applying the interpretation provision, it could be said that the signatory is expected to exercise good faith in making his material representations on the basis of which the certificate is issued.

Similarly, the certification service provider has to meet a list of obligations under the provisions of Article 9\textsuperscript{(1)}\textsuperscript{58} where the electronic signature used has a legal effect. In brief, the list can be grouped broadly into the following obligations: to adhere to representations made in its policy statements; to exercise reasonable care to ensure accuracy of information included in the certificate during its life cycle; to include information (such as, the identity of

\textsuperscript{56} Article 8(1) reads: Where signature creation data can be used to create a signature that has legal effect, each signatory shall:
(a) Exercise reasonable care to avoid unauthorised use of its signature creation data;
(b) Without undue delay, utilise means made available by the certification service provider pursuant to article 9 of this Law, or otherwise use reasonable efforts to, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:
(i) the signatory knows that the signature creation data have been compromised; or
(ii) the circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;
(c) Where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate.

\textsuperscript{57} A/CN 9/WG IV/WP 88 para 135.

\textsuperscript{58} It states: Where a certificate service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall:
(a) Act in accordance with representations made by it with respect to its policies and practices;
(b) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate;
(c) Provide reasonably accessible means that enable a relying party to ascertain from the certificate:
(i) The identity of the certification service provider;
(ii) That the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;
(iii) That the signature creation data were valid at or before the time when the certificate was issued;
(d) Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise:
(i) The method used to identify the signatory;
(ii) Any limitation on the purpose or value for which the signature creation data or the certificate may be used;
(iii) That the signature creation data are valid and have not been compromised;
(iv) Any limitation on the scope or extent of liability stipulated by the certification service provider;
(v) Whether means exist for the signatory to give notice pursuant to article 8, paragraph 1(b) of this Law;
(vi) Whether a timely revocation service is offered;
(e) Where services under paragraph (d)(v) are offered, provide a means for a signatory to give notice pursuant to article 8 paragraph 1(b) of this Law, and where services under paragraph d(vi) are offered ensure the availability of a timely revocation services;
(f) Utilize trustworthy systems, procedures and human resources in performing its services.
the certification service provider, limitation on the value for which the signature creation data may be used; to make available to the relying party information that would be relevant to a particular certificate; ensure availability of a notification system to the signatory which the signatory can use where the signature creation data has been compromised; and, to utilise trustworthy systems and human resources in conducting its services. Article 10 deals with the issue of trustworthiness raised in Article 9(1). It is broad in its interpretation, and among other factors, financial resources, quality of hardware and software, extent of audit by an independent body, accreditation of the certification service provider are be taken into consideration in establishing whether the requirement of trustworthiness is met.

As for the relying party, Article 11(a) places him under an obligation to verify the reliability of an electronic signature. And where it is supported by a certificate to take “reasonable steps to verify the validity, suspension or revocation of the certificate, and to observe any limitation with respect to the certificate.”

What happens if the actors do not meet the obligations set out in the Model Law? In Articles 8(2), 9(2) and 11, the Model Law provides that they will bear the legal consequences of their failure to exercise their respective obligations. While it is reasonable to impose obligations on the signatory and the certification service provider and expect them to bear the legal consequences it is debatable whether this should extend to all members who fall within the class termed ‘relying party’. Relying party could include not only big businesses including IT service providers but also small to medium sized enterprises and consumers. It is questionable whether small to medium sized enterprises, especially in developing countries, will have the expertise and personnel to take the necessary steps to verify the signatures. Given the Model Law is designed for global adoption, it is a pity that it has been drafted taking into account circumstances prevailing in developed countries. The same can be said for consumers. It is unclear whether the Working Group considered the possibility of varying the nature of the obligations by differentiating the ‘relying party’ into different types such as IT service providers (who, for instance, endorse certificates issued by foreign certification services), large businesses, small to medium sized enterprises, and consumers. Of course, parties who are unhappy with the obligations imposed by the Model Law are free to agree to their own terms. And, it is always open for a state to derogate from the provisions of the Model Law when legislating for electronic signatures.

What kind of legal consequences does the Model Law envisage in the event of a breach? Unfortunately, this is left open to be determined by the national law. Legal consequences could be criminal or civil liability, and the nature of liability could, for instance, be fines or damages. This open ended attitude towards legal consequences introduces an element of surprise and uncertainty given the promotion of cross border recognition of certificates and electronic signatures by the Model Law (see below). A certification service provider might find that he is suddenly subject to unexpected liabilities of a foreign jurisdiction. While it is open to a certification service provider to protect himself with insurance cover, uncertainties in respect of type and level of liability are likely to increase insurance premiums. It may even

---

59 It reads:
For the purposes of Article 9, paragraph 1(f), of this Law in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors:
(a) Financial and human resources, including existence of assets;
(b) Quality of hardware and software systems;
(c) Procedures for processing of certificates and applications for certificates and retention of records;
(d) Availability of information to signatories identified in certificates and to potential relying parties;
(e) Regularity and extent of audit by an independent body;
(f) The existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or the existence of the foregoing; or
(g) Any other relevant factor.

60 Article 11(b).
contribute to stifling not only competition but the development of certification service industry in developing countries.

It appears from the Draft Explanatory Memorandum that the Working Group had initially planned to draft detailed rules in respect of the obligations of the various parties involved in an electronic signature. They could not however agree on the content of the rules due to the emerging and significant role of self-regulation in various countries. In the end they opted for a minimal code of conduct as embodied in Articles 8, 9 and 11.\(^{61}\) It is a pity they did not persist in arriving at detailed rules since not all countries, especially the developing, have the infrastructure or the capacity in the IT industry for adopting a self regulatory scheme. At the end of the day they will have to draft supplemental rules to achieve a comprehensive framework for the facilitation of electronic signatures. Some might find this difficult lacking knowledge and experience of the consequences that flow from the use of electronic signatures. And in a world where international commerce is dependant on information technology, a legal framework to facilitate e-commerce is essential, if they wish to maintain their market share.

**Cross Border Recognition of Certificates and Electronic Signatures**

In keeping with the principle of non-discrimination the geographic location where the electronic signature was created or the certificate issued will not determine whether the certificate or electronic signature is legally effective.\(^{62}\) What will affect its effectiveness is the level of reliability. Realising that reliability requirements may vary from jurisdiction to jurisdiction the drafters of the Model Law use ‘equivalence’ rather than ‘identical’ as a measure. According to Article 12(2) and 12(3) a certificate or an electronic signature issued outside the domestic jurisdiction will be legally effective if it offers a “substantial equivalent level of reliability”. The courts will consider each case on its merits and look for equivalence using the requirements for domestic certificates and electronic signatures as a yardstick. The factors that are likely to make an impact are already set out in Articles 6, 9 and 10 (examined above). Article 12(4) further adds that for the purposes of Article 12(2) and (3) regard shall be had to “recognised international standards”. The Draft Explanatory Memorandum makes clear that this is to be interpreted as international technical and commercial standards and standards and norms adopted by governmental and intergovernmental bodies. These standards may be laid down as codes of conducts, statements of best practice, recommendations or guidelines.\(^{63}\)

The flexibility shown by the Model Law towards certificates and electronic signatures originating from foreign jurisdiction recognises the global nature of e-commerce and aims to ease the entry of businesses into the electronic marketplace. It is guided by the spirit of free trade. A framework based on licensing and registration in the jurisdiction where recognition is sought could have been used to ensure that foreign certificates and electronic signatures meet the requirements laid down in that jurisdiction. This would have proved costly and burdensome on those providing certification and electronic signature services and could have acted as a barrier in some circumstances. For instance, small to medium sized traders in developing countries could have found themselves unable to transact electronically if their electronic signature providers did not have the facilities to obtain licences in multiple jurisdictions and the trader did not have the financial strength to obtain the services of a provider from another jurisdiction (where allowed under the law of the trader’s state) who did have multiple jurisdiction licences.

---

\(^{61}\) A/CN 9/WG IV/WP 88 para 132.
\(^{62}\) Article 12(1)(a).
\(^{63}\) A/CN 9/WG IV/WP 88 para154.
Following the principle of party autonomy Article 12(5) provides that parties as between themselves are free to agree on the use of certain types of certificates and electronic signatures as sufficient for cross-border recognition. However, once again this freedom is curtailed by relevant mandatory provisions of the applicable law.

**Conclusion**

The global significance of e-commerce is a fact and it is important that divergent approaches to legislation and the resulting uncertainties do not curtail the growth of e-commerce. One way to achieve legal certainty and predictability is to harmonise the laws. UNCITRAL has played a central role in formulating Model Laws for both electronic commerce and electronic signatures. The focus of this paper was on electronic signatures. While the Model Law addresses the various legal issues including cross border recognition raised by electronic signatures sympathetically it is not sufficiently comprehensive to achieve the desired level of harmonisation. What may be core provisions are left to be addressed by national law. For instance, the issue of liability where obligations by the signatory, certification service provider and the relying party are not met provides a good illustration. Matters of procedure (such as the burden of proof) are also ignored. In a framework that promotes cross border recognition of certificates and signatures, the omission of liability and procedural issues is odd and it would not be unfair to say that the Model Law is a half hearted attempt at harmonisation.