International Journal of Humanities and Social Science Invention
ISSN (Online): 2319 – 7722, ISSN (Print): 2319 – 7714
www.ijhssi.org ||Volume 5 Issue 2 ||February. 2016 || PP.57-64

Electronic Contract : When Is a Contract Actually Concluded or Not?

Samson Masalu Peter Paschal

I. Legal Requirement as to Form

It is common in most jurisdictions that certain types of contracts require particular formalities to be observed in order to be enforceable. According to the UK legislation, unless particular formalities are required- such as a written form- a contract is formed when the **interested parties reach an agreement on its ter**ms. It is evident therefore that there is no specific legal obstacle for contracts to be concluded electronically. But even though the general rule does not prohibit the electronic contract formation, there are several issues that might need to be either specifically **regulated** or practically resolved.

II. Writing

In most commercial transactions the parties would require terms of the relevant contract to be recorded in writing. The rationale behind a written contract is to record the terms governing the transaction and facilitate the understanding between the parties involved aiming as well to evidence the parties' intentions. In absence of a clear, express understanding between the parties, the law implies certain terms into the contract, which may run counter to the parties' actual intentions. A written agreement gives certainty to the terms of the transaction. UNCITRAL in a 1990 report identified four reasons that had historically prompted a requirement that contracts be concluded in writing. These were the desire to reduce disputes, to make the parties aware of the consequences of their dealings, to provide evidence upon which third parties might rely upon the agreement and to facilitate tax accounting and regulator purposes. Furthermore, in most jurisdictions there are laws that require specific contracts, for example contracts that create or transfer real estate rights, to be concluded in writing or even require the participation of a public authority e.g. a notary public.

For contract where writing is a requirement it is important to determine whether documents stored magnetically in digital form comply. Fortunately, Schedule 1 to the Interpretation Act 1978 contains the following definition: 'Writing' includes typing, printing, lithography, photography and other modes of representing or reproducing words in a visible form, and expressions referring to writing are construed accordingly. David Bainbridge argued that 'this would appear to include computer storage. Words stored in a computer may be reproduced on screen or printed on paper. In any case, it is unlikely that a judge would take a restrictive view of this, although the preceding words are somewhat narrow.'[1]

Moreover, In the United States, Section 1-201(46) of the U.C.C. is also illustrative. It defines "written" and "writing" to include "printing, typewriting or any other intentional reduction to tangible form." However, cyberspace transactions, like their real world counterparts, are not all alike. Some are electronic transmissions that can be recorded in a tangible form while others represent electronic impulses coursing through the Internet. For example, e-mail, saved on a hard disk or in hard copy format comprise one end of the spectrum while real time chats, in which two online users strike up a bargain, comprise the other. Thus, Jeff C. Dodd and James A. Hernandez concluded that, 'if a record of the transaction is maintained; it seemed the writing requirement would be satisfied, although this is not entirely free from doubt'[2].

On the other hands, Jeff C. Dodd and James A. Hernandez are more critical about purely electronic transmissions that do not begin or result in printed or other tangible manifestation. They state that 'based on the U.C.C. definition of writing, the answer depends on how records of the transaction are retained and whether a court can be convinced that storage of the electronic records is tantamount to reducing the message to "tangible form". They finally concluded that 'E-mail, online chats and bulletin board dialogues that are not stored or printed would probably not satisfy the writing requirement. Similarly, transactions in which the sending and receiving computers maintain only a momentary record of each separate transaction, prior to dispatching transaction information into a general database, would probably not satisfy the writing requirement'[3].

[1] Introduction to Computer Law, David Bainbridge, 5th ed (2004) P305.
[2] CLRTJ-Summer 1998, p 15.
[3] CLRTJ-Summer 1998, Jeff C. Dodd and James A. Hernandez, P16.

In France, the academics deemed that when writing is requested *ad validitatem*, the electronic communication with a code signature is not able, in the actual state of the law, to constitute writing. The law does not give the meaning of writing. The French Civil Code requires a writing *ad validitatem* or *ad probationem*[4], but no definition may help the academics or judges for the application of the writing to the electronic environment. Nevertheless, the French parliament is going to act out a new general article in the civil law that will give to the electronic writing the same force as the paper writing[5], as it has been already done for the proof. 'However, French academics regret that this project of new provision is not prepared with more nuances. Indeed, the writing demanded *ad validitatem* is a mode of protection of a party because it has as aim to draw his attention to the importance of his agreement. But, the simple showing of writing stipulations on a computer screen does not come up to the gist of this formalism'[6].

III. Signature

The question of writing requested for e- contracts is not yet settled. Nevertheless, one of its aspects, the signature of a contract, seemed to have already been resolved by a technical means, the digital signature.

As Reed explained: 'manuscript signature is accepted without question as legally effective in all jurisdictions, assuming it has not been procured by fraud, and it is rarely asked what effects such a signature is required by law to achieve. However, in those cases where the question has been asked, other methods of signing a document, such as signature by means of a printed or rubber stamp facsimile, have been assessed for validity. The most common approach is to define the functions, which a signature must perform, and then to treat signature methods, which affect those functions as valid signatures. The primary function of a physical world signature is to provide evidence of three matters: (1) the identity of the signatory; (2) that the signatory intended the 'signature' to be his signature; and (3) that the signature approves of and adopts the contents of the documents[7].

Reed came to the conclusion that Manuscript signatures meet these functional requirements in a number of ways.

According to him, Identity is established by comparing the signature on the document with other signatures, which can be proved, by extrinsic evidence, to have been written by the signatory. The assumption is that manuscript signatures are unique, and that therefore such a comparison is all that is necessary to provide evidence of identity. In practice, manuscript signature are usually acknowledged by the signatory once they are shown to him, and extrinsic evidence is only required where it is alleged that the signature has been forged.

Moreover, he concluded that intention to sign is normally presumed also, according to him the act of affixing a manuscript signature to a document is universally recognised as signing[8]. Intention to sign is normally only disputed where the affixing of the signature has been procured by fraud, and in those cases the signatory bears the burden of displacing the presumption that he intended to sign. Intention to adopt the contents of the document is similarly presumed because it is general knowledge that affixing a manuscript signature to a document has that effect. In both cases, the burden of displacing the presumption is on the signatory.[9]

However, Reed pointed out that a difficulty arises, if the relevant law imposes specific requirements as to the form a signature must take. In the context of Internet communications, the thing to be signed, an electronic document exists more as a matter of metaphysics than a physical object. For this reason it is very difficult for an electronic signature method to meet any physical requirement of form[10]. For example, some of the cases and statutes on physical world signatures appear to state that a signature must take the form of a mark on a document.[11]

[4] Art 1341 of the French Civil Code.
[5] Project of law " on the information society" of 14 June 2001(Doc. An, no 3143): an Art 1369-1 would be inserted in the French Civil code.
[6] A Comparative Study of English and French Law on E-Commerce, Damien Gallet, P 38.
[7] Internet Law Text and Materials, Chris Reed, 2nd Ed P 182.
[8] See e.g. L'Estrange v F Graucob Ltd [1934] 2 KB 394 at 403, per Scrutton LJ.
[9] See e.g. Saunders v Anglia Building Society [1971] AC 1004.
[10] See Utah Digital Signature Rules, (Rule 154-10 of the Utah Commerce, Corporations and Commercial Code).
[11] Morton v Copeland (1855) 16 CB 517 at 535, per Maule J, see Reed at P183.

Despite the difficulty, Reed stressed that, 'if the relevant law defines the validity of a signature in terms of the evidential functions it achieves, an electronic document may be signed by the use of a mathematical function based on the document's data content. This process can meet all the law's evidential requirements for signatures, but can only be considered as a logical mark in that it is in many respects functionally equivalent to a mark on paper, primarily because it cannot easily be altered without leaving some trace. The process can be undertaken in a way that will easily produce evidence of the intention to sign and authenticate the signatory and the electronic document's contents, but the result is if anything less visible than and equally as metaphysical as adding text or an image'[12].

IV. Electronic Signature Technology

'An electronic signature is produced by performing a mathematical function on the document, or part of it, which identifies the signatory and authenticates the contents of the document. To be an effective signature, the modified document must be producible only by the maker, and any change to the content of the document must invalidate the signature. These modifications can be achieved through the use of encryption technology.
Because an electronic document is a string of 1s and 0s it can be treated as a series of numbers. Performing a series of mathematical functions, which has two inputs; the series of numbers, which represents the document, and a key, which is it, a number, carries out encryption. The result is a series of different numbers, the cipher text. There are two distinct types of encryption algorithm: (1) single key or symmetric encryption; and (2) public key or asymmetric encryption'[13].

V. How Digital Signature Technology Works

'Digital signature are created and verified by cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. Digital signatures use what is known as 'public key cryptography', which employs an algorithm using two different but mathematically related 'keys'; one for creating a digital signature or transforming data into a seemingly unintelligible form, and another key for verifying a digital signature or returning the message to its original form. Computer equipment and software utilising two such keys are often collectively termed an 'asymmetric cryptosystem'.

The complementary keys of an asymmetric cryptosystem for digital signatures are arbitrarily termed the private key, which is known only to the signer and used to create the digital signature. The public key, which is ordinarily more widely known, is used by a relying party to verify the digital signature. If many people need to verify the signer's digital signatures, the public key must be available or distributed to all of them, perhaps by publication in an-online repository or directory where it is easily accessible. Although the keys of the pair are mathematically related, if the asymmetric cryptosystem has been design and implemented securely it is computationally infeasible to derive the private key from the knowledge of the public key. Thus, although many people may know the public key of a given signer and use it to verify that signer's signatures, they cannot discover that signer's private key and use it to forge digital signatures. This is sometimes referred to as the principle of 'irreversibility'[14].

Another fundamental process, termed a 'hash function,' is used in both creating and verifying a digital signature. A harsh function is an algorithm which creates a digital representation or 'fingerprint' in the form of a 'hash value' or 'harsh result' of a standard length which is usually much smaller than the message but nevertheless substantially unique to it. Any change to the message invariably produces a different hash result when the same hash function is used. In the case of a secure hash function, sometimes termed a 'one-way hash function,' it is computationally infeasible to derive the original message from knowledge of its hash value. Hash functions therefore enable the software for creating digital signatures to operate on smaller and predictable amounts of data, while still providing robust evidentiary correlation to the original message content, thereby efficiently providing assurance that there has been no modification of the message since it was digitally signed.

Thus, the process described above can verify both the message's authenticity (i.e., it was digitally signed by the sender) and its integrity (i.e., it has not been altered). If the sender's private key has not been "compromised," the process can also prevent the sender from denying that it sent the message'.

[12] Reed, Internet Law, P 184.
[13] Reed, p184.
[14] Reed, p 184

Although the ABA Guidelines establish a legal and institutional framework for applying digital signature technology to electronic commerce, digital signatures are not yet uniformly recognised throughout the United States. Nevertheless, the impetus provided by the four-year project that culminated in the ABA Guidelines has influenced a number of states to pass or propose digital signature legislation in efforts to legitimise the use of electronic contracting technology in online commerce[15].

Utah has enacted the most comprehensive legislation to date.[16] Passed in 1995 and amended in 1996, the Utah Digital Signature Act was the first effort to "facilitate commerce by means of reliable electronic messages."[17] Modelled after the ABA Guidelines, the Utah Act, in addition to setting forth a comprehensive regulatory regime complete with a licensing mechanism for certification authorities, establishes a technology specific approach. This approach specifies the use of asymmetric cryptosystem as part of its definition of digital signature[18]. Specifically, under Utah's, the results in the signature and text of an electronic message being deemed to constitute a signature, a writing, an original of the document, an acknowledged writing or signature under applicable law[19].

VI. Law and Jurisdiction

E-commerce is clearly a global activity and it is quite likely that the contracting parties will be in different countries. Obviously, this can lead to potential for disputes about which country's law applies, and also as to jurisdiction over the defendant. A full review of the principles of choice of law and jurisdiction is, however, well beyond the scope of this work. We will concentrate instead on concerns that are e-commerce specific and, in particular, issues of localisation, it often being difficult in e-commerce disputes to determine precisely where something has happened.

VII. Whose Law Applies?

In the UK, contract proper law issues are determined by **the Rome Convention**, which was brought into force in the UK **by the Contracts (Applicable Law) Act 1990**. In an Internet context, there are a number of when and where issues. The most important provisions are these:

(1) A contract shall be governed by the law chosen by the parties. The choice must be expressed or demonstrate with reasonable certainty by the terms of the contract or the circumstances of the case. By their choice the parties can select the law applicable to the whole or a part only of the contract.

The safest way to resolve any possible dispute about whose law applies is expressly to provide for it. This is quite straightforward but in reality, of course, in web-based transaction, only the web operator can use this provision, not a customer. **Article 3 is also subject to art3 (3):**

The fact that the parties have chosen a foreign law, whether or not accompanied by the choice of a foreign tribunal, shall not, where all the other elements relevant to the situation at the time of the choice are connected with one country only, prejudice the application of rules of the law of that country which cannot be derogated from by contract, hereinafter called 'mandatory rules.'

The point of a provision such as this is to ensure that the parties do not, for example, in what is clearly an English contract, by choosing a foreign law avoid, for example, the Unfair Contract Terms Act 1977, which would almost certainly be regarded as 'mandatory rules'. The provision does not seem to cause any Internet-specific problems, except that it is clearly necessary to localise 'all the other elements relevant to the situation at the time of the choice'.

If the parties do not expressly choose a proper law, art 4 applies:

(1) To the extent that the law applicable to the contract has not been chosen in accordance with Article 3, the contract shall be governed by the law of the country with which it is most closely connected…

(2) Subject to the provisions of paragraph 5 of this Article, it shall be presumed that the contract is most closely connected with the country where the party who is to effect the performance which is characteristic

[15] CLRTJ- Summer 1998, P 22.
[16] UTAH CODE ANN. S 46-3-101(1995)
[17] Id. S 46-3-102.
[18] UTAH CODE s 46-3-103(10).
[19] UTAH ACT s 46-3-401.

of the contract has, at the time of conclusion of the contract, his habitual residence, or, in the case of a body corporate or unincorporated, its central administration. However, if the contract is entered into in the course of that party's trade or profession, that country shall be the country in which the principal place of business is situated or, where under the terms of the contract the performance is to be effected through a place of business other than the principle place of business, the country in which that other place of business is situated.

(5) Paragraph 2 shall not apply if the characteristic performance cannot be determined...

Article 4 in general does not seem to create many Internet- specific issues. However, there are then specific consumer provisions in Art 5:

(1) This Article applies to a contract the object of which is the supply of goods or services to a person (the consumer) for a purpose which can be regarded as being outside his trade or profession, or a contract for the provision of credit for that object.
(2) Notwithstanding the provisions of Article 3, a choice of law made by the parties shall not have the result of depriving the consumer of the protection afforded to him by the mandatory rules of the law of the country in which he has his habitual residence:

- *If in that country the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising, and he had taken in that country all the steps necessary on his part for the conclusion of the contract, or*
- *If the other party or his agent received the consumer's order in that country, or*
- *If the contract is for sale of goods and the consumer travelled from that country to another country and there gave his order, provided thatt he consumer's journey was arranged by the seller for the purpose of inducing the consumer to buy.*

(3) Notwithstanding the provisions of the Article4, a contract to which this article applies shall, in the absence of choice in accordance with Article 3, be governed by the law of the country in which the consumer has his habitual residence if it is entered into in the circumstances described in paragraph 2 of this Article.

This is intended to prevent sellers, by inducing consumers to leave their habitual country of residence, to contract by the law of a country that is less beneficial to them. To operate Art5(2), however, we need to know in which country a web advertisement is addressed, where an order is received, and where an order is made, and perhaps also what is meant by 'all the steps necessary on his part for the conclusion of the contract'. The last could create problems, for example, if the consumer is roaming cybercafés throughout the world, or even perhaps staying at home but using an overseas ISP.

VIII. Jurisdiction

Whether jurisdiction can be asserted against a defendant who does not submit to it depends on where the defendant has his domicile.

If the defendant is not domiciled in an EU or EFTA[20] state, then RSC Ord 11 applies[21]. Among the criteria are that the contract was made within the jurisdiction or that there is a breach of contract within the jurisdiction[22]. In order to determine whether the contract was made within the jurisdiction, we have already seen that the place of acceptance is the crucial factor[23].
Where the defendant is domiciled in the EU, the Brussels Convention applies, and if he is domiciled in an EFTA state, the Lugarno Convention. The Conventions are quite similar and are Schedules to the Civil Judgments and Jurisdiction Act 1982, as subsequently amended[24].

[20] The only members of EFTA today are Iceland, Liechtenstein, Norway and Switzerland.
[21] Paul Todd, E-Commerce Law, 2005 p 210.
[22] RSC Ord 11rr1(1)(d)(i).
[23] EntoresLtd case and Brinkibon case.
[24] See the Contracts (Applicable Law) Act 1990.

Article5 (1) of the Brussels Convention allows a person domiciled in a contracting State to be sued in the courts of another Contracting state in matter relating to the performance, perhaps of the contract there. This requires the localisation of the performance, perhaps problematic with electronic material itself sent over the Internet[25]. Article 13 applies to consumer contracts, the criteria in art13 (3) being basically the same as the first criterion in art5 (2) of the Rome Convention.

IX. Where Things Happen on the Internet

If we start by considering where a delivery of electronic data such as music, software or a film take place, this may at first sight seem to be analogous to acceptance in contract,[26] but in fact the issues are different in principle. The problem of not knowing whether the communication has arrived is likely to be less serious because, it does not arrive, the intended recipient can simply request a resend. There are none of the problems of potential revocation of the offer in the meantime, or fluctuating markets.

On the other hand, delivery to the recipient's agent being delivery to the recipient is a principle of general application[27] and it would be difficult to justify departing from that principle here. That being said, delivery should take place at the recipient's server. This need not be in the country of the recipient's domicile. The problem is that this could be entirely capricious from the supplier's viewpoint and hence arguably unfair in that jurisdictional rules could turn on it.

If the recipient collects the data from the supplier's website, there is a case for saying that delivery takes place there. Since there is no reason why this should necessarily be in the same country as the supplier's domicile, this could operate equally capriciously from the viewpoint of the recipient. There is also the problem that the website itself could straddle many jurisdictions but, unless the data itself is comprised of packets originating from several servers it ought at least to be possible to localise the server which actually sent the data.

It is far more difficult to determine where a consumer took steps towards contract formation. The logic of the legislation suggests that the physical location of the consumer should be the determining factor. From the supplier's viewpoint, of course, he may have no way of knowing where that is. For example, a travelling consumer could easily access his server from a cybercafé anywhere in the world and the supplier would have no way of knowing where the consumer was.

This seems to be one of those areas where e-commerce is, in the absence of legislation to the contrary, governed by the existing law, which operates entirely haphazardly in an Internet context. There are good arguments for Internet-specific legislation. In Australia, for example, at least for the place of receipt of communications, the emphasis is on the normal physical location of the parties. This seems to be a reasonable and sensible rule, and one which is likely to operate less capriciously than one which attempts to locate the server[28].

X. EU Regulation and International Regulations of E-commerce

Directive's preamble (61) states: "If the market is actually to operate by electronic means in the context of globalisation, the European Union and the major non-European areas need to consult each other with a view to making laws and procedures compatible."

> 'There are, however, few signs of any such international consultation having been carried out in the drafting of the contract provisions in the E-Commerce Directive. In particular, there appears to be no influences from **The Vienna Convention of the International Sales of Goods (CISG)**, t**he Principles of European Contract Law (PECL)**, **the UNIDROIT Principles of International Commercial Contracts, and the UNCITRAL Model Law on Electronic Commerce, or the US Uniform Electronic Transaction Act'**[29].

One of the objections against the original draft of the section on contract law in the E-Commerce Directive was that all Member States (except the UK) have ratified **CISG,** in which formation of contract is regulated[30]. Naturally, it would be unfortunate if CISG were to be set aside within the EU, since it already contributes

[25] Paul Todd, p212.
[26] Reed, C, Internet Law: Text and Materials, 2nd ed, 2004, see Paul Todd, p 212.
[27] Eg, there is a somewhat similar principle relating to sale of goods, delivery to a carrier being regarded as delivery to the buyer, in sale of Goods act 1979, s32(1).
[28] See Paul Todd E- Commerce Law, p 213.
[29] See, www.uncitral.org.
[30] Denmark, Sweden and Finland have not ratified CISG Part II, which contains the rules on formation of contracts. Initiatives have been taken in these states to ratify CISG Part II.

greatly to the harmonisation of European contract law. CISG is also well adapted to electronic contracts for the sale of moveable[31]. However, CISG does not cover all types of electronic contracts, since it is applicable only to sale of moveable and to business-to-business transactions. This problem could have been solved by extending the applicability of CISG's rules on the formation of contracts.

According to Ramberg, another apparently neglected source of inspiration in relation to the E-Commerce Directive's section on contract law is the UNCITRAL Model Law on Electronic Commerce. The Model Law is based on the important principle of functional equivalency, which is an exceptionally helpful tool in analysing problems related to e-commerce. It has been widely adopted in some form throughout the world. The UNCITRAL Model Law Art. 5 states: "A data message shall not be denied legal effect, validity or enforceability solely on the ground that it is in electronic form". Vague traces of this principle can be found in the EU's Directive on Electronic Signatures, Art. 5. The E-Commerce Directive, however, shows nothing of it. The fact that the EU has chosen not to refer to the UNCITRAL Model Law's concept of functional equivalency deserves an express explanation in the preamble.

What the EU wanted to achieve in the E-Commerce Directive was accomplished more efficiently in the USA by the Uniform Electronic Transaction Act (UETA), which is greatly influenced by the UNCITRAL Model Law on Electronic Commerce. The principle of functional equivalency is expressly incorporated in UETA sec 7:

"(A) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

(a) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation."

UETA was introduced in August 1999 and has been a success. UETA can be implemented voluntarily by the US states (as opposed to the E-Commerce Directive, which the Member States of the EU are compelled to implement). As of January 2001, UETA has been adopted (wholly or in part) by 23 states.

In the process of drafting the E-Commerce Directive the EU Commission could have benefited from communicating with the drafters of UETA. The Directive shows no sign of any such communication having taken place, despite the fact that the drafting of UETA was made in an open environment in which all interested parties were invited to participate (for example, practitioners, academics, public servants, including Europeans).

XI. Global Approaches to the Regulation of Internet Transactions

Apart from the EU there are also a few proposals for harmonising Internet related problems with a true worldwide prospectus. The most comprehensive proposal is the 1996 UNCITRAL Model Law on Electronic Commerce[32] that parties to any kind of information in the form of a data message used in the context of commercial activities (Article 1)[33] Data message is here defined as: 'information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy' (Article 2a).

The Model law deals generally with the formation and validity of (electronic) contracts (Article.11), the legal recognition of data messages (writing, Article6, signature, Article 7; original document, Article8), and especially with the carriage of goods (transport documents, Article.17). All in all, the Model Law puts (electronic) data messages in the same category as paper-based messages. Unfortunately, only a handful of States have currently adopted it[34].

The Council of the OECD adopted in 1997 Guidelines for Cryptography Policy. The aim of these Guidelines was mainly to facilitate electronic commerce by fostering trust in electronic signatures. The OECD was also In favour of a flexible legal framework allowing the user to choose between different methods of cryptography in an ongoing process of development of international standards according to the changes in technology[35]. 'OECD

[31] See, UNCITRAL Working Group on Electronic Commerce, Feb 2000 at www.uncitral.org.
[32] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment of 16 December 1996, see http://www.uncitral.org/english/texts/electcom.
[33] A.Brooke Overby, 'Will Cyberlaw Be Uniform? An Introduction to the UNCITRAL Model Law on Electronic Commerce', (Spring 2000) 7 Tul.J.Int'l & Comp.L.219,at 21.
[34] Op.cit., p59
[35] See OECD Guidelines for Cryptography Policy , http://www.oecd.org/dsti/sti/it/secur/prod/crypto2.htm.

recognised that cryptography for the protection of privacy and data security is an essential key to the confidence of users in information and communications infrastructures. Without this Guidelines are no legal rules but policy recommendations primarily aimed at governments' future enactments in cryptography issues relating to electronic commerce'[36].

Finally, UNCITRAL issued in 1998 'Draft Uniform Rules on Electronic Signatures'. These rules favour the concept of a secure electronic signature that is defined by Article.1(c) as an electronic signature, which is a digital signature, or can otherwise be verified to be the signature of a specific person through the application of a security procedure that is:

(a) Uniquely linked to the person using it;
(b) Capable of promptly, objectively and automatically identifying that person;
(c) Created in a manner or using a means under the sole control of the person using it; and
(d) Is linked to the data message to which it relates in a manner such that if the message is altered the electronic signature is invalidated.
(e) Or is commercially reasonable under the circumstances, previously agreed to and properly applied, by the parties.

Given that a data message was authenticated by means of a secure electronic signature, it is presumed by Article.2 that:

1. The data message has not been altered since the time the secure electronic signature was affixed to the data message;
2. The secure electronic signature is the signature of the person to whom it relates;
3. That person with the intention of signing the message affixed the secure electronic signature.

However, according to Farhan-Al-Farhan, 'the UNCITRAL rules on electronic signatures are similar to the proposed EU Directive on Electronic Signatures insofar as they also recognise different forms of electronic signatures, not only digital ones. But the value of rebuttable presumptions in favour of electronic signatures in the UNCITRAL draft rules remains doubtful because electronic signatures do not constitute full evidence as handwritten signatures do. So the straightforward EU approach with electronic signatures being equivalent to handwritten ones seems to be methodically sounder. Nevertheless, UNCITRAL is still in draft form and it is still unclear what the final version of the Uniform Rules will contain'[37].

[36] Farhan-Al-Farhan, the impacts of the UNCITRAL Model Law on international Legal system(2000), p 21.
[37] See also A.Murray, 'Entering into Contracts Electronically:The Real WWW.