Comments to the UNCITRAL Model Law on Electronic Signatures

Apol·lònia Martínez-Nadal and Josep Lluís Ferrer-Gomila

Universitat de les Illes Balears
Carretera de Valldemossa km. 7.5, Palma de Mallorca, 07071, Spain
{dpramn0, dijjfg}@clust.uib.es

Abstract. Electronic signatures, together with certificates, are offered as a substitutive solution of hand-written signatures for a wide scale electronic commerce. The use of these electronic authentication techniques has suggested the need for a specific legal framework to reduce uncertainties, specially regarding to the legal effect that may result from the use of such techniques. The risk of diverging legislative approaches taken in various countries calls for uniform legislative provisions to establish the basic rules of what is inherently an international phenomenon, where not only technical but legal interoperability is essential. So, these new legal issues should be addressed in an internationally acceptable legal framework. This is the objective of the UNCITRAL Model Law on electronic signatures (2001). The aim of this paper is comment and criticise the content of this Model Law, studying their different precepts. The paper concludes with some observations that show that the Model Law, although positive, presents important oversights.

1 Introduction

Nowadays the use of new technologies to facilitate commercial transactions electronically is becoming more frequent. Then hand-written signatures are not possible and neither are any of the functions they perform. From the technological point of view, digital signatures are offered as substitutes for hand-written signatures together with certificates and certification authorities (also known as certifying entities, certifiers, or certification service providers).

The increased use of these electronic authentication techniques has suggested the need for a specific legal framework to reduce uncertainties, specially regarding to the legal effect that may result from the use of such modern techniques. From a legal point of view, these elements (which may be referred to, generally, as "electronic signatures") have been the object of various initiatives, differing in origin, nature and application. Amongst these, it must be mentioned the Utah Digital Signature Law (1996), the first law to attempt regulation of electronic signatures, certificates and certification authorities. Since then, a great number of states or entities have also enacted or are preparing legislation to rule electronic signatures (USA, Germany, Italy, Spain, Argentina, European Union, etc.).

A.H. Chan and V. Gligor (Eds.): ISC 2002, LNCS 2433, pp. 229–243, 2002.

Anyway, we consider that local or national legislation is not enough. The risk that diverging legislative approaches being taken in various countries with respect to electronic signatures calls for uniform legislative provisions to establish the basic rules of what is inherently an international phenomenon, where legal (as well as technical) interoperability is essential. Different and diverging legislation can produce difficulties in reaching a common understanding of the new legal issues that arose from the increased use of digital signatures. So, these new legal issues should be addressed in an internationally acceptable legal framework.

Attending to the need of uniform legislation, and after some years of works, the United Nations Commission on International Trade (UNCITRAL) adopted the Model Law on Electronic Signatures on 5 July 2001. This new Model Law rules the legal effectiveness that may be expected from a given electronic signature, adopting an approach under which the legal effectiveness of a given electronic signature technique may be pre-determined (or assessed prior to being actually used). Moreover, by establishing with appropriate flexibility a set of basic rules of conduct for the various parties that may become involved in the use of electronic signatures the Model Law may assist in shaping more harmonious commercial practices in cyberspace. By incorporating the procedures prescribed in the Model Law in its national legislation, the different enacting States would establish harmonised legislative framework to address more effectively the issues of electronic signatures.

As the UNCITRAL Model Law on Electronic Commerce (1996), the new Model Law on electronic signatures is in the form of a legislative text that is recommended to States for incorporation into their national law. Unlike an international convention, model legislation does not require the State enacting it to notify the United Nations or other States that may have also enacted it. However, States are strongly encouraged to inform the UNCITRAL Secretariat of any enactment of the new Model Law (or any other model law resulting from the work of UNCITRAL). In incorporating the text of the model legislation into its legal system, a State may modify or leave out some of its provisions. In the case of a convention, the possibility of changes being made to the uniform text by the States parties is much more restricted. Model legislation is then more flexible but this flexibility, however, also means that the degree of, and certainty about, harmonisation achieved through model legislation is likely to be lower than in the case of a convention.

Regarding the question of application of Model Law to use of electronic signatures in international and domestic transactions, it is recommended that application of the Model Law be made as wide as possible. Particular caution should be used in excluding the application of the Model Law by way of a limitation of its scope to international uses of electronic signatures, since such a limitation may be seen as not fully achieving the objectives of the Model Law. The legal certainty to be provided by the Model Law is necessary for both domestic and international trade, and a duality of regimes governing the use of electronic signatures might create a serious obstacle to the use of such techniques.

In preparing and adopting the Model Law on Electronic Signatures the United Nations Commission on International Trade Law was mindful that the Model Law would be a more effective tool for States modernising their legislation if background

and explanatory information were provided to Governments and legislators to assist them in using the Model Law. It's the Guide to enactment of the UNCITRAL Model Law on electronic signatures. For example, it was decided in respect of a number of issues not to settle them in the Model Law but to address them in the Guide so as to provide guidance to States enacting the Model Law.

The Model Law on electronic signatures is now object of analysis, albeit in brief, in order to understand the fundamental aspects of the subject and the basic legal principles as regards electronic signatures established in the Model Law that probably will inspire the legislation of a great number of countries. First we will analyse its sphere of application; next, basic subjective and objective notions; we'll continue with the essential question of legal effects of electronic signature and we'll end this analysis with the study of the conduct that must perform the different parties. Finally, this work will finish with some conclusions, suggestions and reflections.

2 Sphere of Application

The Model Law contains an explicit indication that its focus was on the types of situations encountered in the commercial area. According to Article 1 "This Law applies where electronic signatures are used in the context of commercial activities". So, the "Sphere of application" of Model Law would be only commercial uses, and non-commercial (e.g., administrative) uses would be excluded. Anyway, the Guide to enactment of the UNCITRAL Model Law explains that the term "commercial" should be given non a strict but a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not, and provides indications as to what is meant thereby.

Furthermore, UNCITRAL admits that nothing in the Model Law should prevent an enacting State from extending the scope of the Model Law to cover uses of electronic signatures outside the commercial sphere. For example, while the focus of the Model Law is not on the relationships between users of electronic signatures and public authorities, the Model Law is not intended to be inapplicable to such relationships.

3 Definitions. Basic Notions: Subjective and Objective Elements

Article 2 establishes for the purposes of the Model Law the basic notions, which can be classified in two categories: objective notions: electronic signature, certificate and data message; and subjective notions: signatory, certification service provider and relying party.

3.1 Objective Notions

(a) *"Electronic signature"* means data in 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 to indicate the signatory's approval of the information contained in the data message (art. 2, paragraph a).

This notion of "electronic signature" is intended to cover all traditional uses of a hand-written signature for legal effect: the identification of the signatory and the intent to sign. It's a wide and technologically-neutral definition, similar to the notion of electronic signature established in other legislation (e.g., European Directive on electronic signatures, 1999). The reason of this neutrality, according to Guide, is that the scope of the Model Law is to provide for the coverage of all factual situations where electronic signatures are used, irrespective of the specific electronic signature or authentication technique being applied. However, the Guide admits that in the preparation of the Model Law, special attention has been given to "digital signatures", i.e., those electronic signatures obtained through the application of dual-key cryptography, which were regarded by the UNCITRAL Working Group on Electronic Commerce as a particularly widespread technology. Observe that due to this neutrality it seems that the juridical concept of electronic signature is not equivalent to the technical concept of digital signature: a digital signature is an electronic signature but not always an electronic signature will be a digital signature. Because according to the Model Law another authentication techniques (currently available on the market or still under development) relying on techniques other than public-key cryptography can offer the technical means by which some or all of the functions identified as characteristic of hand-written signatures can be performed in an electronic environment. Such techniques may be referred to broadly as "electronic signatures".

So, UNCITRAL has intended to develop uniform legislation that can facilitate the use of both digital signatures and other forms of electronic signatures. Anyway, we consider this neutral definition too wide, in the sense that it could include techniques that are not really electronic signatures because they don't satisfy the function of authentication (probably techniques such as authentication through a biometrics device based on hand-written signatures, the use of personal identification numbers, digitised versions of hand-written signatures, and other methods). This problem is solved in other legislation establishing a second concept of electronic signature which must fulfil some additional requirements that gives more security to the concept (e.g., the advanced electronic signature of European Directive). In UNCITRAL Model Law on electronic signatures there's no a clear definition of this second concept of qualified or enhanced electronic signatures. Anyway, we consider that, as we shall see, the content and the requirements of art. 6 establishes implicitly this second concept of electronic signatures.

Furthermore, given the rapidity of technological development, this neutrality surely allows the doors to be left open for future technologies; however, on the other hand, carried to this extreme, it leaves without resolution many of the questions posed now by the digital signature, which is probably the only secure form of electronic signature available today. We do understand that it doubtless would have been better to adopt a technically open position, in order to not discourage the means for other secure technologies in the future to come forward, but, at the same time, focusing on the regulation of the digital signature, given the predominance of the function performed by the public key cryptography in the recent practices of electronic commerce.

(b) *"Certificate"* means a data message or other record confirming the link between a signatory and signature creation data (art. 2, paragraph b).

The purpose of the certificate is to recognise, or confirm a link between signature creation data and the signatory. This notion uses a concept ("signature creation data") that is not defined in the Model Law. Another legislation uses and defines this concept (e.g., the European Directive on electronic signatures: those unique data, such as codes or *private cryptographic keys*, which are used by the signatory to create an electronic signature). Only Guide of Model Law explains that the terms "signature creation data" is intended to designate those secret keys, codes, or other elements that, in the process of creating an electronic signature, are used to provide a secure link between the resulting electronic signature and the person of the signatory. For example, in the context of digital signatures relying on asymmetric cryptography, the cryptographic key pair; in the context of electronic signatures based on biometrics devices, the biometrics indicator, such as a fingerprint or retina-scan data.

Observe that while in general legislation on electronic signatures defines the certificate as a link of a person to a signature verification data (e.g., European Directive), in the Model Law the certificate establishes a link between a person (the signatory) and the opposed element: the signature creation data. In fact, the certificates of digital signature contain as basic requirement the identity of the subscriber and the public or verification key, the certificate establishes a direct link between this two elements (and only and indirect link between the subscriber and the private or signature key, which does not appear in the certificate).

Differing from other legislation the Model Law doesn't approach in this definition the essential question of confirmation or verification of the identity of the signatory (e.g., European Directive defines the certificate in general, as "an electronic attestation which links signature-verification data to a person and confirms the identity of that person"). This verification is essential for the security of the electronic signature. And it is also essential that the certification service provider assumes liability for this role and function. In practice, distinct ways of verification of identity are used (physical presence, presentation of accreditation documentation, submission of information on-line). Among them, the only one that offers security is physical identification (even so, this is not completely safe, as an impostor could assume an identity and not be detected, not even by a diligent service provider) Although from the commercial point of view it is understandable that the certification service providers offer products with differing costs and levels of security, from the legal point of view this commercial diversification doesn't allow the basic function of the certificates. Furthermore, if an excessive flexibility in commercial practices is permitted in order to facilitate the growth of certification providers the certification system will become degraded and will never achieve its final aim, which although bordering on other subjective commercial interests, is, we mustn't forget, the security of electronic commerce.

(c) "*Data message*" means 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 (art. 2, paragraph c).

The definition of "data message" is taken from article 2 of the UNCITRAL Model Law on Electronic Commerce as a broad notion encompassing all messages generated

in the context of electronic commerce, including web-based commerce. The notion of "data message" is not limited to communication but is also intended to encompass computer-generated records that are not intended for communication. Thus, the notion of "message" includes the notion of "record". The reference to "similar means" is intended to reflect the fact that the Model Law was not intended only for application in the context of existing communication techniques but also to accommodate foreseeable technical developments.

3.2 Subjective Notions

Together to the previous objective notions, the Model Law defines three other subjective notions referred to the parties that normally act with respect to electronic signatures: signatories, certification services providers and relying parties. The Guide remarks that this parties corresponds to one possible PKI (Public Key Infrastructure) model, but other models are already commonly used in the marketplace (e.g., where no independent certification authority is involved). The Guide explains that focusing on the functions performed in a PKI environment and not on any specific model also makes it easier to develop a fully media-neutral rule to the extent that similar functions are served in non-PKI electronic signature technology.

(a) *"Signatory"* means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents (art. 2, paragraph d)

The signatory is defined simply as "a person". The Guide explains that any reference in the new Model Law to a "person" should be understood as covering all types of persons or entities, whether physical, corporate or other legal persons.

This explanation seems to solve the debated question of the nature of the person who can sign electronically. In a paper-based environment legal entities cannot strictly be signatories of documents drawn up on their behalf, because only natural persons can produce authentic hand-written signatures. Electronic signatures, however, can be conceived so as to be attributable to companies, or other legal entities (including governmental and other public authorities), and there may be situations where the identity of the person who actually generates the signature, where human action is required, is not relevant for the purposes for which the signature was created. Nevertheless, according to the Guide, under the Model Law, the notion of "signatory" cannot be severed from the person or entity that actually generated the electronic signature, since a number of specific obligations of the signatory under the Model Law are logically linked to actual control over the signature creation data. However, in order to cover situations where the signatory would be acting in representation of another person, the phrase "or on behalf of the person it represents" has been retained in the definition of "signatory". The extent to which a person would be bound by an electronic signature generated "on its behalf" is a matter to be settled in accordance with the law governing, as appropriate, the legal relationship between the signatory and the person on whose behalf the electronic signature is generated, on the one hand, and the relying party, on the other hand. That matter, as well as other matters pertaining to the underlying transaction, including issues of agency and other questions

as to who bears the ultimate liability for failure by the signatory to comply with its obligations under article 8 (whether the signatory or the person represented by the signatory) are outside, according to the Guide, the scope of the Model Law.

(b) *"Certification service provider"* means a person that issues certificates and may provide other services related to electronic signatures (art. 2, paragraph e).

As a minimum, the certification service provider as defined for the purposes of the Model Law would have to provide certification services, possibly together with other services. No distinction has been drawn in the Model Law between situations where a certification service provider engages in the provision of certification services as its main activity or as an ancillary business, on a habitual or an occasional basis, directly or through a subcontractor. The definition covers all entities that provide certification services within the scope of the Model Law, i.e., "in the context of commercial activities". However, in view of that limitation in the scope of application of the Model Law, entities that issue certificates for internal purposes and not for commercial purposes would not fall under the category "certification service providers" as defined in article 2.

(c) *"Relying party"* means a person that may act on the basis of a certificate or an electronic signature (art. 2, paragraph f).

The Model Law concludes the definition of subjective elements with the notion of 'Relying party", often forgotten in other legislation. According to the Guide, the definition of "relying party" is intended to ensure symmetry in the definition of the various parties involved in the operation of electronic signature schemes under the Model Law. Observe that he is not only the person who relies on a certificate but also the person who relies simply on an electronic signature. Thus, the electronic signatures schemes ruled in the Model Law are not always based in a certificate.

4 Legal Effects of Electronic Signatures

4.1 Rule of Equivalent Function for Reliable Signatures Art. 6, Paragraph 1 and 2)

Article 6 is one of the core provisions of the Model Law, because approaches the question of legal effects of electronic signatures. In particular, art. 6, paragraph 1 and 2, of Model Law establishes that:

"1. 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.

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

The purpose of that provision is to ensure that, where any legal consequence would have flowed from the use of a hand-written signature, the same consequence should flow from the use of a reliable electronic signature. In the preparation of the Model

Law, the view was expressed that (either through a reference to the notion of "enhanced electronic signature" or through a direct mention of criteria for establishing the technical reliability of a given signature technique) a dual purpose of article 6 should be to establish: (1) that legal effects would result from the application of those electronic signature techniques that were recognised as reliable; and (2), conversely, that no such legal effects would flow from the use of techniques of a lesser reliability. It's thus the rule of equivalent function between hand-written signatures and reliable electronic signatures.

4.2 Requirements for a Reliable Signature (Art. 6, Paragraph 3)

However, the problem is the determination of what constitutes a reliable method of signature in the light of the circumstances. This determination can be made *ex post* by a court, possibly long after the electronic signature has been used. In contrast, the Model Law creates a benefit in favour of certain techniques, which are recognised as particularly reliable. That is the purpose of paragraph (3) of art. 6 ("An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if: …", which is expected to create certainty, at or before the time any such technique of electronic signature is used (*ex ante*), that using a recognised technique will result in legal effects equivalent to those of a hand-written signature. Thus, paragraph (3) is an essential provision if the Model Law is to meet its goal of providing certainty as to the legal effect to be expected from the use of particularly reliable types of electronic signatures. Subparagraphs (a) to (d) of paragraph (3) are intended to express objective criteria of technical reliability of electronic signatures:

a) "The signature creation data are, within the context in which they are used, linked to the signatory and to no other person" (paragraph 3, subparagraph a). Subparagraph (a) focuses on the objective characteristics of the signature creation data, which must be "linked to the signatory and to no other person". According to the Guide, from a technical point of view, the signature creation data could be uniquely "linked" to the signatory, without being "unique" in itself. The linkage between the data used for creation of the signature and the signatory is the essential element. While certain electronic signature creation data may be shared by a variety of users, for example where several employees would share the use of a corporate signature-creation data, that data must be capable of identifying one user unambiguously in the context of each electronic signature.

b) "The signature creation data were, at the time of signing, under the control of the signatory and of no other person" (paragraph 3, subparagraph a). Subparagraph (b) deals with the circumstances in which the signature creation data is used. At the time it is used, the signature creation data must be under the sole control of the signatory. In relation to the notion of sole control by the signatory, a question is whether the signatory would retain its ability to authorise another person to use the signature data on its behalf. Such a situation might arise where the signature data is used in the corporate context where the corporate entity would be the signatory but would require a number of persons to be able to sign on its behalf. When the signatory loose the sole

control of signature data (e.g., in case of robbery), and these data can be used a third non authorised party, it's necessary to revoke the link of those data to the signatory (in case of digital signatures, the certificate must be revoked) and eventually important questions of liability should be solved. The first question (revocation) is approached later by Model Law in art. 8; however, there are no rules in order to allocations risks and liabilities in this situations.

c) and d) "Any alteration to the electronic signature, made after the time of signing, is detectable" (paragraph 3, subparagraph c); and "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" (paragraph 3, subparagraph d). Subparagraphs (c) and (d) deal with the issues of integrity of the electronic signature and integrity of the information being signed electronically. It would have been possible to combine the two provisions to emphasise that, where a signature is attached to a document, the integrity of the document and the integrity of the signature are so closely related that it is difficult to conceive of one without the other. Where a signature is used to sign a document, the idea of the integrity of the document is inherent in the use of the signature. However, it was decided that the Model Law should follow the distinction drawn in the UNCITRAL Model Law on Electronic Commerce between articles 7 and 8. Although some technologies provide both authentication (article 7 of the UNCITRAL Model Law on Electronic Commerce) and integrity (article 8 of the UNCITRAL Model Law on Electronic Commerce), those concepts can be seen as distinct legal concepts and treated as such. Since a hand-written signature provides neither a guarantee of the integrity of the document to which it is attached nor a guarantee that any change made to the document would be detectable, the functional equivalence approach requires that those concepts should not be dealt with in a single provision.

4.3 Predetermination of Status of Electronic Signature: Satisfaction of Requirements of Art. 6 (Art. 7)

Article 7 ("Satisfaction of article 6") establishes in paragraph 1 that: "[Any person, organ or authority, whether public or private, specified by the enacting State as competent] may determine which electronic signatures satisfy the provisions of article 6 of this Law".

Article 7 describes the role played by the enacting State in establishing or recognising any entity that might validate the use of electronic signatures or otherwise certify their quality. The purpose of article 7 is to make it clear that an enacting State may designate an organ or authority that will have the power to make determinations as to what specific technologies may benefit from the presumptions or substantive rule established under article 6. Like article 6, article 7 is based on the positive idea that what is required to facilitate the development of electronic commerce is certainty and predictability at the time when commercial parties make use of electronic signature techniques, not at the time when there is a dispute before a court.

5 Basic Rules of Conduct for the Parties Involved

Article 8 (and articles 9 and 11) had been initially planned to contain rules regarding the obligations and liabilities of the various parties involved (the signatory, the relying party and any certification services provider). However, it was difficult to achieve consensus as to the contents of such rules. So, those issues are left to applicable law outside the Model Law. So, the Model Law does not deal in any detail with the issues of liability that may affect the various parties involved in the operation of electronic signature systems. On the contrary, other legislations, such as the European Directive, rule liability of certification service providers but do not regulate in a particular and systematic way the rights and obligations of the parties participating in the certification system. Any way, as we shall see, although there's not specific regulation of liability in UNCITRAL Model law, some of the rules on the conduct of parties contribute to clarify the question of liability.

5.1 Conduct of the Signatory

Article 8 rules the conduct of the signatory establishing in paragraph 1 that "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 relation data". The obligation in paragraph (1) (a), in particular, to exercise reasonable care to prevent unauthorised use of a signature data, constitutes a basic obligation that is, for example, generally contained in certificate practice statements and legislation on electronic signatures. This obligation can be one the criteria to solve the question of allocation of risks in case of compromise of the signature creation data, a question not approached by the Model Law.

"(b) Without undue delay, utilize means made available by the certification service provider pursuant to article 9 of this Law, or otherwise use reasonable efforts, 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".

Paragraph (1) (b) establishes the obligation of notification to relying parties in case of compromise of the signature creation data. But there is not a clear regulation of liability of the different parties in this case. This paragraph refers to the notion of "person who may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature". Depending on the technology being used, such a "relying party" may be not only a person who might seek to rely on the signature, but also a person such as a certification service provider, a certificate revocation service provider and any other interested party.

"(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." Paragraph (1) (c) applies where a certificate is used to support the signature data. The "life-cycle of the certificate" is intended to be interpreted broadly as covering the period starting with the application for the certificate or the creation of the certificate and ending with the expiry or revocation of the certificate.

After establishing the obligations of the signatory in paragraph 1, paragraph 2 approaches the question of the consequences in case of non-fulfilment of those requirements:

"2. A signatory shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1."

Observe that paragraph (2) does not specify either the consequences or the limits of liability, both of which are left to national law of every state. However, even though it leaves the consequences of liability up to national law, paragraph (2) serves to give a clear signal to enacting States that liability should attach to a failure to satisfy the obligations set forth in paragraph (1). Paragraph (2) is based on the conclusion reached by the Working Group at its thirty-fifth session that it might be difficult to achieve consensus as to what consequences might flow from the liability of the signature data holder. Depending on the context in which the electronic signature is used, such consequences might range, under existing law, from the signature data holder being bound by the contents of the message to liability for damages.

5.2 Conduct of the Certification Service Provider

Independent of whether a licensing system were or were not established with or without its own set of exigencies, every provider of certification services would have to comply, in order to be considered a trusted third party, with a certain series of fundamental requisites in order to generate trust and security in its organisation and activities both before and after the issuing of a certificate. These requisites as they appear in Art. 9 ("Conduct of the certification service provider") paragraph 1 of the Model Law ("1. Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall: …") are basically classified as follows:

"(a) Act in accordance with representations made by it with respect to its policies and practices". Subparagraph (a) expresses the basic rule that a certification service provider should adhere to the representations and commitments made by that supplier, for example in a certification practices statement or in any other type of policy statement.

"(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". Subparagraph (b) replicates in the context of the activities of the certification service provider the standard of conduct set forth in article 8(1)(c) with respect to the signatory.

"(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 signature creation data were valid at or before the time when the certificate was issued." Subparagraph (c) defines the essential contents and the core effect of any certificate under the Model Law.

"(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". We consider this provision positive because in order to inspire confidence a certificate would have to establish or incorporate, amongst other things, the degree of investigation developed by the authority to confirm the identity of the signatory. It also may be useful to homologate the certificates; that is to say, establish classes or categories of certificates generally accepted by the certifying entities and widely known throughout the community of users, in which would be fixed definite types of certificate issued by each authority, permitting the relying party an approximate idea of the value of each certificate.

"(ii) Any limitation on the purpose or value for which the signature creation data or the certificate may be used". The liability of certification authority without a specific legislation, under the general regulations for liability, is potentially high and unforeseeable, given the indefinite number of operations covered by a same certificate. Because of this, and in order to stimulate the development of certification authorities which could be halted in cases of unforeseeable or unlimited risk, different legislation and legislative initiatives do expressly admit or favourably contemplate the existence of possible limitations to the liability of the providers of certification services (it must be pointed out that the existence of limitations to liability of the signatories can be equally as necessary). In the same fashion the Model Law, establishes distinct limits to liability which benefit the providers of certification services.

"(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" (whether means exist for the signatory to give notice that a signature device has been compromised)

"(vi) Whether a timely revocation service is offered".

"(e) Where services under subparagraph (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 subparagraph (d) (vi) are offered, ensure the availability of a timely revocation service". Subparagraph (e) is not intended to apply to certificates such as transactional certificates, which are one-time certificates, or low-cost certificates for low-risk applications, both of which might not be subject to revocation.

"(f) Utilize trustworthy systems, procedures and human resources in performing its services". For the assessment of the trustworthiness of the systems, procedures and human resources utilized by the certification service provider, the Model Law provides an open-ended list of indicative factors in art. 10. That list is intended to provide a flexible notion of trustworthiness, which could vary in content depending upon what is expected of the certificate in the context in which it is created.

After establishing obligations for certifications provider in paragraph 1, paragraph 2 or art. 9 approach but do no solve the question of the legal consequences of the non-fulfilment: "A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1. Paragraph (2) mirrors the basic rule of liability set forth in article 8(2) with respect to the signatory. The effect of that provision is to leave it up to national law to determine the consequences of liability."

5.3 Conduct of the Relying Party (Art. 11)

Article 11 ("Conduct of the relying party") establishes that:

"A relying party shall bear the legal consequences of its failure:

(a) To take reasonable steps to verify the reliability of an electronic signature; or

(b) Where an electronic signature is supported by a certificate, to take reasonable steps:

(i) To verify the validity, suspension or revocation of the certificate; and

(ii) To observe any limitation with respect to the certificate."

Article 11 reflects the idea that a party who intends to rely on an electronic signature should bear in mind the question whether and to what extent such reliance is reasonable in the light of the circumstances. While article 11 might place a burden on relying parties, particularly where such parties are consumers, it may be recalled that the Model Law is not intended to overrule any rule governing the protection of consumers. However, the Model Law might play a useful role in educating all the parties involved, including relying parties, as to the standard of reasonable conduct to be met with respect to electronic signatures. In addition, establishing a standard of conduct under which the relying party should verify the reliability of the signature through readily accessible means may be seen as essential to the development of any public-key infrastructure system.

As to the possible impact of establishing as a general obligation that the relying party should verify the validity of the electronic signature or certificate, a question arises where the relying party fails to comply with the requirements of article 11. Should it fail to comply with those requirements, the relying party should not be precluded from availing itself of the signature or certificate if reasonable verification would not have revealed that the signature or certificate was invalid. Such a situation may need to be dealt with by the law applicable outside the Model Law.

6 Conclusions

In conclusion, the following observations may be made about the UNCITRAL Model Law of electronic signatures, that in general is positive but presents yet important oversights:

1. In the first place, the Model Law is positive because offers to those countries where legislative authorities are in the process of preparing legislation on electronic signature the guidance of an international instrument. The risk that diverging

legislative approaches be taken in various countries with respect to electronic signatures calls for uniform legislative provisions to establish the basic rules of what is inherently an international phenomenon, where legal (as well as technical) interoperability is essential.

2. In the second place, it was considered that, although digital signatures play a predominant role in the emerging electronic-commerce practice, the uniform rules should be adopt the media-neutral approach. Given the rapidity of technological development, this neutrality surely allows the doors to be left open for future technologies; however, on the other hand, carried to this extreme, it leaves without resolution many of the questions posed now by the digital signature, which is the only secure form of electronic signature available today. We do understand that it doubtless would have been better to adopt a technically open position, in order to not discourage the means for other secure technologies in the future to come forward, but, at the same time, focusing on the regulation of the digital signature, given the predominance of the function performed by the public key cryptography in the recent practices of electronic commerce.

3. There doesn't exist a complete vision of the certificate and its life cycle, with those distinct stages through which the certificate may pass (issue, distribution, use, revocation and/or suspension and expiry). And with regard to a question as important as the revocation of a certificate, the Model Law does not consider propoerly the distribution and assignation of liability among the different parties (certifying entity, subscriber and third user) during the period of the revocation (from, for example, the date of compromise of the private key to the effective publication of the revocation of that key); in that sense, the content of Model Law is partial and incomplete. In consequence, there are yet unresolved questions, not approached (or only partially) by the legislator. For example, what would happen if, as the consequence of the loss of a private key, that key were used for an illegitimate purpose by another party? What would happen if the applicant of the certificate had requested a revocation but the certifying entity hadn't in fact cancelled the certificate out of negligence, or if it were still checking the request? What would happen if the decision to revoke a certificate had been taken but wasn't yet known to the third relying party by reason of the time taken for publication of the information by the system (for example, periodically updated revocation lists)? And what would happen if the provider of the certification service revoked a certificate accidentally? All these questions should be solved by the national law of the enacting states and, if not, certification practice statements will the essential rule..

4. There does not exist a complete vision of the persons implicated in the certification system (basically, the certification service provider, the subscriber and the user of the certificate). It's true that the personal elements are defined in the Model Law (even there is definition of the third party who puts their trust in the certificate. However, there do not exist detailed regulations about, e.g., the first of these personal elements, the providers. There are no provisions on matters so important as whether the certification authorities certifying the validity of cryptographic key pairs should be public entities or whether private entities might act as certification authorities; or whether the process of allowing a given entity to act as a certification authority should

take the form of an express authorization, or "licensing", by the State, or whether other methods should be used to control the quality of certification authorities if they were allowed to operate in the absence of a specific authorization. The Model Law does not deal with those issues which should be approached in respective national laws..

5. The Model Law does not approach the delicate theme of liability. This is an essential but a non-resolved question in these initial stages of commercial and legal development of certification entities. And this uncertainties could seriously affect its progress. Hence the need to establish and delineate very clearly the rules and conditions of liability derived from the issuing and use of certificates, taking into account the interests of all parties contracted in the electronic transaction (not only the certifier but also, e.g., a consumer subscriber or user of a certificate).

References

1. ABA (American Bar Association), *Digital signature guidelines, Legal infrastructure for Certification Authorities and secure electronic commerce*, August 1, 1996, USA.
2. COMMISSION OF THE EUROPEAN COMMUNITIES, *Directive of the European Parliament, and the Council for a common framework on electronic signature (13 december 1999).*
3. MARTINEZ NADAL, A., *Comercio electrónico, firma digital y autoridades de certificación,* Madrid, 2001.
4. UNCITRAL (Commission of the United Nations for the International commercial Law), *Model Law on Electronic commerce*, 1997.
5. UNCITRAL (Commission of the United Nations for the International commercial Law), *Model Law on electronic signatures*, 2001.
6. UNCITRAL (Commission of the United Nations for the International commercial Law), *Guide to Enactment of the Uncitral Model Law on electronic signatures, 2001.*