UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES
2001

(Excerpt from the report of the United Nations Commission on International Trade Law on the work of its thirty-fourth session, held at Vienna, from 25 June to 13 July 2001. The text of the UNCITRAL Model Law on Electronic Signatures was adopted on 5 July 2001 [Note: the final version of the Guide to Enactment of the Model Law will be published during the second semester of the year 2001])

Annex II

UNCITRAL Model Law on Electronic Signatures (2001)

Article 1
Sphere of application

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.

---

* The Commission suggests the following text for States that might wish to extend the applicability of this Law:

"This Law applies where electronic signatures are used, except in the following situations: [...]."

** The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited, to the following transactions: 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 venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.

Article 2
Definitions

For the purposes of this Law:

(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;

(b) "Certificate" means a data message or other record confirming the link between a signatory and signature creation data;

(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;

(d) "Signatory" means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents;

(e) "Certification service provider" means a person that issues certificates and may provide other services related to electronic signatures;

(f) "Relying party" means a person that may act on the basis of a certificate or an electronic signature.

Article 3
Equal treatment of signature technologies

Nothing in this Law, except article 5, 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, paragraph 1, or otherwise meets the requirements of applicable law.

Article 4
Interpretation

1. In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.

2. Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

Article 5
Variation by agreement

The 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.

Article 6
Compliance with a requirement for a signature

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.

3. 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 to no other person;

(b) The signature creation data were, 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.

4. Paragraph 3 does not limit the ability of any person:

(a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or

(b) To adduce evidence of the non-reliability of an electronic signature.

5. The provisions of this article do not apply to the following: [...].

Article 7
Satisfaction of article 6

1. [*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.

2. Any determination made under paragraph 1 shall be consistent with recognized international standards.

3. Nothing in this article affects the operation of the rules of private international law.

Article 8
Conduct of the signatory

1. Where signature creation data can be used to create a signature that has legal effect, each signatory shall:

(a) Exercise reasonable care to avoid unauthorized use of its signature creation data;

(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;

(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.

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

Article 9
Conduct of the certification service provider

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:

(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 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 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;

(f) Utilize trustworthy systems, procedures and human resources in performing its services.

2. A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

Article 10
Trustworthiness

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 existence of the foregoing; or

(g) Any other relevant factor.

Article 11
Conduct of the relying party

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 12
Recognition of foreign certificates and electronic signatures

1. In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had:

(a) To the geographic location where the certificate is issued or the electronic signature created or used; or

(b) To the geographic location of the place of business of the issuer or signatory.

2. A certificate issued outside [*the enacting State*] shall have the same legal effect in [*the enacting State*] as a certificate issued in [*the enacting State*] if it offers a substantially equivalent level of reliability.

3. An electronic signature created or used outside [*the enacting State*] shall have the same legal effect in [*the enacting State*] as an electronic signature created or used in [*the enacting State*] if it offers a substantially equivalent level of reliability.

4. In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph 2 or 3, regard shall be had to recognized international standards and to any other relevant factors.

5. Where, notwithstanding paragraphs 2, 3 and 4, parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.