United Nations A/CN.9/578/Add.10

General Assembly

Distr.: General
17 May 2005

Original: English

United Nations Commission on International Trade Law
Thirty-eighth session
Vienna, 4-15 July 2005

Draft Convention on the Use of Electronic Communications in International Contracts

Compilation of comments by Governments and international organizations

Addendum

Contents

V.05-84458 (E) 310505 010605

II. Compilation of comments

A. States

8. Singapore

[Original: English]
[16 May 2005]

Comment on the draft UNCITRAL Convention on the Use of Electronic Communications in International Contracts

1. Singapore expresses its appreciation to Working Group IV on the completion of its work at the forty-fourth session, and considers that the revised version of the draft Convention (A/CN.9/577) represents a sound basis for consideration and adoption by the Commission.

2. At this juncture, we wish to highlight only certain limited issues which we feel were not fully considered by Working Group IV in its deliberations. We propose that the Commission consider:

(a) Amending paragraph 3 (a) of article 9 of the draft Convention (A/CN.9/577) to recognize that electronic signatures are sometimes required by law only for the purpose of identifying the person signing ("the signor") and associating the information with the signor, but not necessarily to indicate the signor's "approval" of the information contained in the electronic communication; and

(b) Deleting paragraph 3 (b) of article 9 of the draft Convention (A/CN.9/577), to achieve functional equivalence between handwritten signatures and electronic signatures, and to avoid the unintended difficulties that would be created by the inclusion of the general legal "reliability requirement" in paragraph 3 (b).

Issues relating to paragraph 3 (a) of article 9

3. Paragraph 3 (a) of article 9 lays down general criteria for functional equivalence between handwritten signatures and electronic signatures.[1] Paragraph 3 (a) provides that only an electronic signature that fulfils both the function of identification of the party *as well as* the function of indicating that

---

[1] Paragraph 3 (a) of article 9 is based on article 7, paragraph 1 (a), of the UNICTRAL Model Law on Electronic Commerce 1996. Article 7 of the UNCITRAL Model Law on Electronic Commerce states:

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

party's approval of the information contained in the electronic communication meets that legal requirement of a signature in relation to an electronic communication.[2]

4. However, there may be instances where the law requires a signature that does not fulfil the function of indicating the signing party's approval of the information contained in the electronic communication. For example, many countries have requirements of law for notarization of a document by a notary or attestation by a commissioner for oath. In such cases, it is not the intention of the law to require the notary or commissioner, by signing, to indicate his approval of the information contained in the electronic communication. In such cases, the signature of the notary or commissioner merely identifies the notary or commissioner, and associates the notary or commissioner with the contents of the document, but does not indicate the approval by the notary or commissioner of the information contained in the document. Similarly, there may be laws that require the execution of a document to be witnessed by a witness, who may be required to append his signature to that document. The signature of the witness merely identifies the witness and associates the witness with the contents of the document witnessed, but does not indicate the approval by the witness of the information contained in the document.

5. The conjunctive requirement in paragraph 3 (a) of article 9 would prevent electronic signatures from satisfying the requirement of law for a signature in such situations where the function of indicating approval of the contents of the electronic communication cannot be fulfilled by such signatures.

6. In order to also allow electronic signatures that are not intended to fulfil the function of indicating the signor's approval of the information contained in the electronic communication, to also satisfy a requirement of law for a signature, we therefore propose that paragraph 3 (a) of article 9 should be amended to read as follows:

> "(a) A method is used to identify the party and to associate that party with the information contained in the electronic communication, and as may be appropriate in relation to that legal requirement, to indicate that the party's approval of the information contained in the electronic communication; and".

7. The phrase "*A method is used to identify the party and to associate that party with the information contained in the electronic communication*" represents the minimum functional requirements of any signature, handwritten or electronic. This phrase provides that electronic signatures that only fulfil these minimum functions will satisfy the requirement of law for signatures. The phrase "*and as may be appropriate in relation to that legal requirement*" recognizes that the function that the electronic signature is intended to perform will depend on the policy or purpose behind that particular requirement of law in question, and provides that the electronic signature is required to fulfil the function of indicating the signing party's approval of the information contained in the electronic communication, where it is

---

[2] It should be noted that under paragraph 3 of article 9, which originated from article 7, paragraph 1, of the UNCITRAL Model Law on Electronic Commerce, the mere signing of an electronic communication by means of a functional equivalent of a handwritten signature is not intended, in and of itself, to confer legal validity on the data message. Whether an electronic communication that fulfilled the requirement of a signature has legal validity is to be settled under the law applicable outside the draft convention. See paragraph 61 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996).

appropriate in relation to that legal requirement. For example, if the law requires a party to sign an offer document to indicate his acceptance of the terms contained in the document, that electronic signature would fulfil the requirements of the proposed paragraph 3 (a) of article 9 if it identifies the signing party, associates that party with the information contained in the document **and** indicates that party's approval of the information contained in the document.

Issues relating to paragraph 3 (b) of article 9

8. Paragraph 3 (b) of article 9 contains a requirement that the method of signing must be "as reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement" in order for the electronic signature to be legally valid.

9. This "reliability requirement" in paragraph 3 (b) of article 9 has its origins in article 7, paragraph 1 (b), of the UNCITRAL Model Law on Electronic Commerce 1996.

10. In the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures 2001, it was already noted that article 7 of the UNCITRAL Model Law on Electronic Commerce creates uncertainty as the determination of appropriately sufficient reliability can only be made *ex post* by a court or other trier of fact. In order to create more certainty *ex ante*, article 6, paragraph 3, of the UNCITRAL Model Law on Electronic Signatures 2001 was introduced. Paragraph 118 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures 2001 states:

> "... However, under article 7 of the UNCITRAL Model Law on Electronic Commerce, the determination of what constitutes a reliable method of signature in the light of the circumstances, can be made only by a court or other trier of fact intervening *ex post*, possibly long after the electronic signature has been used. In contrast, the new Model Law [on Electronic Signatures 2001] is expected to create a benefit in favour of certain techniques, which are recognised as particularly reliable, irrespective of the circumstances in which they are used. That is the purpose of paragraph 3, which is expected to create certainty (through either a presumption or a substantive rule), 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 handwritten signature. Thus, paragraph 3 is an essential provision if the new Model Law is to meet its goal of *providing more certainty than readily offered by the UNCITRAL Model Law on Electronic Commerce* as to the legal effect to be expected from the use of particularly reliable types of electronic signatures. …" [Emphasis added]

11. At the forty-second session, the Working Group had considered two variants in paragraph 3 of article 9. Variant A was based on article 7 of the UNCITRAL Model Law on Electronic Commerce, while variant B was based on article 6, paragraph 3,

of the UNCITRAL Model Law on Electronic Signatures.[3] The Working Group decided in favour of retaining variant A only.[4]

12. In choosing to retain only variant A, the Working Group may not have fully considered the implications of retaining in paragraph 3 (b) of article 9, the general "reliability requirement" based on article 7 of the Model Law on Electronic Commerce.

13. Under paragraph 3 (b) of article 9, the satisfaction by an electronic signature of a requirement of law for signature depends on whether the signature method was appropriately reliable for the purpose of the electronic communication in light of all the circumstances, as determined *ex post* by a court or other trier of fact. This means that the parties to the electronic communication or contract are not able to know with certainty *ex ante* whether the electronic signature used will be upheld by a court or other trier of fact as "appropriately reliable" and therefore not be denied legal validity, until after a legal dispute arises subsequently. It also means that even if there was *no dispute* about the identity of the person signing or the fact of signing (i.e. no dispute as to authenticity of the electronic signature), a court or trier of fact may still rule that the electronic signature was not appropriately reliable, and therefore invalidate the entire contract.

14. Such a provision will potentially have serious practical implications for electronic commerce:

(a) It will create uncertainty in electronic transactions because whether a signature method is appropriately reliable and hence not be denied legal validity will be determined *ex post* by the court or trier of fact, and not *ex ante* by the parties. Although parties can exercise party autonomy by agreeing on a signature method, it remains that the parties' agreement is only one of the factors in paragraph 3 (b) of article 9 taken into consideration by the court or trier of fact.[5] Even if the parties were satisfied at the outset as to the reliability of the signature method, a court or trier of fact may rule otherwise.

(b) It could be used to the detriment of the very class of persons that the legal requirements for signature are intended to protect. A party could try to invalidate his own electronic signature as being insufficiently reliable, in order to invalidate a contract, where it is convenient to him. This would be to the detriment of the other party relying on the signor's signature. This provision then risks becoming a trap for the unwary or a loophole for the unscrupulous.

(c) It may be an impediment to electronic commerce. It will add to business costs if users feel compelled to use more sophisticated and costly technology to ensure that the reliability requirement is satisfied. Conversely, such uncertainty and additional costs may even discourage the use of electronic transactions.

---

[3] A/CN.9/546, paragraph 48.

[4] A/CN.9/546, paragraphs 54-57.

[5] This was explicitly noted at paragraph 60 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996), which states, "However, a possible agreement between originators and addressees of data messages as to the use of a method of authentication is not conclusive evidence of whether that method is reliable or not."

15. It is noted that the reliability requirement originated from language in laws relating to the closed and heavily regulated area of funds transfer.[6] In that context, the question of whether the authentication or security procedure, e.g. a signature, is appropriate relates to the concept of attribution of that signature to the person. The UNCITRAL Model Law on Electronic Commerce originally needed a reliability test because it contained a general attribution rule in article 13.[7] In the Model Law on Electronic Commerce, article 7 and article 13 together affirmed the validity of an electronic signature and allowed the attribution of the data message to an originator as long as the addressee used a method agreed upon with the originator to verify the authenticity of the message, without the need to demonstrate the authenticity of the signature itself.[8] The attribution rule in the UNCITRAL Model Law on Electronic Commerce was ultimately limited to technology agreed between the signor and the relying party.

16. The draft Convention does not deal with the attribution of electronic communications.[9] Therefore, the current paragraph 3 (b) of article 9 of the draft convention imposes a general "reliability requirement" without any corollary attribution provision. In the absence of an acceptable attribution rule, attribution of a signature should be a matter of proof. There is no necessity for a "reliability requirement" to be introduced as a complement to a non-existent attribution rule.

17. It is noted that there is no such "reliability requirement" for the legal validity of handwritten signatures (or any of the other marks on paper that may constitute a signature at law). Common law does not impose any form requirement on signatures. A person can sign by marking a cross "X" on a document. A person can also sign by a machine that prints his name on a document. Both the cross "X" and machine-printed name are legally valid signatures, though questions of proof may arise. In each case, it is a matter of proof whether the purported signor did in fact sign in that manner and intended thereby to sign the document. In order to establish the signature's function of linking the signor with the signed document, the context of the signing will always have to be demonstrated, whether the signature is on paper or electronic.

18. It is not the form of the signature, but the proven link between the signature and the purported signor based on the context, that gives the signature its legal effect. In our view, electronic signatures are merely another form of signature, and

---

[6] See A/CN.9/387, paragraphs 81 to 87. At the 26th session of the Working Group on Electronic Data Interchange, which considered the Draft Provisions for Uniform Rules on the Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Trade Data Communication (which later revisions became the Model Law on Electronic Commerce), an earlier draft of article 7 contained the phrase "and the mode of identification of the sender is in the circumstances a **[commercially] reasonable** method of security against unauthorized messages", before it was suggested that the phrase be replaced by "a method of authentication is sufficient if it is **as reliable as is appropriate** in all the circumstances to the purpose for which a communication was made". The phrase "commercially reasonable" originated from language used in article 5 of the UNCITRAL Model Law on International Credit Transfers, and article 4A of the Uniform Commercial Code (UCC).

[7] If, as a matter of law, a signature is to be attributed to a particular person, then in fairness to that person it is necessary to ensure that the technical features of the signature are technically reliable.

[8] A/CN.9/571, paragraph 127.

[9] A/CN.9/546, paragraph 127.

should in principle be legally valid as signatures without any special requirements of reliability. Questions of proof of the making of the signature (which exist for both handwritten and electronic signatures) should not distort the law on the validity of signatures. If it is recognized that the legal effect of a signature is based on the proven link between the document, the signature and the purported signor, then it is irrelevant whether the signature method was of an appropriate level of reliability. In order to achieve functional equivalence between handwritten signatures and electronic signatures, there should not be any additional reliability requirement for electronic signatures as contained in paragraph 3 (b) of article 9.

19. In commercial transactions, the person relying on a signature always takes the risk that the signature is not genuine, so he evaluates the risk that the signature is not genuine and protects himself accordingly.[10] The risk analysis will of course include the cost of having the signature made more reliable and the cost of its being not genuine. So a history of dealings with the purported signor, or a low-value transaction, may persuade someone to rely on a signature that would not be satisfactory if it were from a stranger or for a high value transaction. These precautions and judgements are not a matter of law but a matter of prudence. That is, a party may not feel comfortable about relying on a signature in the form of a cross "X", but that is a judgement by that party as a matter of prudence, and not a matter of law, as the signature in the form of a cross "X" is fully valid as a signature at law. We are of the view that this analysis applies equally where electronic commercial transactions and electronic signatures are concerned.

20. We recognize that people have had many years of experience in evaluating how reliable a handwritten signature is, and therefore are able to easily judge what types of handwritten signatures are prudent to be relied upon. People are currently less familiar with the potentials and vulnerabilities of methods of signing electronically, and may be less proficient in making that prudential judgement. However, the law does not add any value to this lack of familiarity by introducing a general reliability requirement such as paragraph 3 (b) of article 9. Such a reliability requirement merely transfers the prudential judgement from the relying party to the judge or adjudicator. The judge or adjudicator may be no more competent to make that prudential judgement, although he or she may have the benefit of expert evidence. Such expert evidence is also available to the relying party, but at a more useful point of time, before the transaction is consummated. As people become more familiar with electronic signatures, they will become more experienced at making that prudential judgement.

21. We note that in order to achieve the objective of harmonization of laws relating to electronic commerce, the draft convention should contain either a uniform standard for the reliability requirement for electronic signatures (which can be in the form of a general "reliability requirement" as in paragraph 3 (b) of article 9), or no reliability requirement (which will be achieved if paragraph 3 (b) of article 9 were deleted). As pointed out above, the current paragraph 3 (b) of article 9 creates significant uncertainty which does not promote the use of electronic commerce, and we are of the view that such a reliability requirement is unnecessary and inappropriate in the circumstances. We therefore propose that the better and

[10] This may involve checking the signature against known genuine versions of it, or getting the signature witnessed, notarized or guaranteed by a bank, etc.

more appropriate option is to have no reliability requirement for electronic signatures, and that paragraph 3 (b) of article 9 be deleted.

22. If paragraph 3 (b) of article 9 (and therefore the reliability requirement) is deleted, article 9 will provide that *all electronic signatures* that fulfil the functions described in paragraph 3 (a) of article 9 will satisfy the requirement of law for signatures. This will provide parties with the certainty of knowing that the electronic signatures appended by them or being relied upon by them do satisfy the requirement of law for signatures, and therefore would not be denied legal validity on that basis.