UNITED NATIONS

A

General Assembly

Distr.
GENERAL

A/CN.9/454
21 August 1998

ORIGINAL: ENGLISH

UNITED NATIONS COMMISSION
ON INTERNATIONAL TRADE LAW
Thirty-second session
Vienna, 17 May-4 June 1999

REPORT OF THE WORKING GROUP ON ELECTRONIC COMMERCE ON THE WORK OF ITS THIRTY-THIRD SESSION (New York, 29 June-10 July 1998)

CONTENTS

Introduction

1. The Commission, at its twenty-ninth session (1996), decided to place the issues of digital signatures and certification authorities on its agenda. The Working Group on Electronic Commerce was requested to examine the desirability and feasibility of preparing uniform rules on those topics. It was agreed that work to be carried out by the Working Group at its thirty-first session could involve the preparation of draft rules on certain aspects of the above-mentioned topics. The Working Group was requested to provide the Commission with sufficient elements for an informed decision to be made as to the scope of the uniform rules to be prepared. As to a more precise mandate for the Working Group, it was agreed that the uniform rules to be prepared should deal with such issues as: the legal basis supporting certification processes, including emerging digital authentication and certification technology; the applicability of the certification process; the allocation of risk and liabilities of users, providers and third parties in the context of the use of certification techniques; the specific issues of certification through the use of registries; and incorporation by reference. [1/]

2. At its thirtieth session (1997), the Commission had before it the report of the Working Group on the work of its thirty-first session (A/CN.9/437). As to the desirability and feasibility of preparing uniform rules on issues of digital signatures and certification authorities, the Working Group indicated to the Commission that it had reached consensus as to the importance of, and the need for, working towards harmonization of law in that area. While it had not made a firm decision as to the form and content of such work, it had come to the preliminary conclusion that it was feasible to undertake the preparation of draft uniform rules at least on issues of digital signatures and certification authorities, and possibly on related matters. The Working Group recalled that, alongside digital signatures and certification authorities, future work in the area of electronic commerce might also need to address: issues of technical alternatives to public-key cryptography; general issues of functions performed by third-party service providers; and electronic contracting (A/CN.9/437, paras. 156-157).

3. The Commission expressed its appreciation for the work already accomplished by the Working Group at its thirty-first session, endorsed the conclusions reached by the Working Group, and entrusted the Working Group with the preparation of uniform rules on the legal issues of digital signatures and certification authorities (hereinafter referred to as “the Uniform Rules”).

4. With respect to the exact scope and form of the Uniform Rules, the Commission generally agreed that no decision could be made at this early stage of the process. It was felt that, while the Working Group might appropriately focus its attention on the issues of digital signatures in view of the apparently predominant role played by public-key cryptography in the emerging electronic-commerce practice, the Uniform Rules should be consistent with the media-neutral approach taken in the UNCITRAL Model Law on Electronic Commerce. Thus, the Uniform Rules should not discourage the use of other authentication techniques. Moreover, in dealing with public-key cryptography, the Uniform Rules might need to accommodate various levels of security and to recognize the various legal effects and levels of liability corresponding to the various types of services being provided in the context of digital signatures. With respect to certification authorities, while the value of market-driven standards was recognized by the Commission, it was widely felt that the Working Group might appropriately envisage the establishment of a minimum set of standards to be met by certification authorities, particularly where cross-border certification was sought. [2/]

5. The Working Group began the preparation of the Uniform Rules at its thirty-second session on the basis of a note prepared by the Secretariat (A/CN.9/WG.IV/WP.73). The Secretariat was requested to prepare, on the basis of the deliberations and conclusions of the Working Group, a set of revised provisions, with possible variants, for consideration by the Working Group at a future session.

6. At its thirty-first session (1998), the Commission had before it the report of the Working Group on the work of its thirty-second session (A/CN.9/446). The Commission expressed its appreciation of the efforts accomplished by the Working Group in its preparation of draft Uniform Rules on Electronic Signatures. It was noted that the Working Group, throughout its thirty-first and thirty-second sessions, had experienced manifest difficulties in reaching a common understanding of the new legal issues that arose from the increased use of digital and other electronic signatures. It was also noted that a consensus was still to be found as to how those issues might be addressed in an internationally acceptable legal framework. However, it was generally felt by the Commission that the progress realized so far indicated that the draft Uniform Rules on Electronic Signatures were progressively being shaped into a workable structure.

7. The Commission reaffirmed the decision made at its thirty-first session as to the feasibility of preparing such Uniform Rules and expressed its confidence that more progress could be accomplished by the Working Group at its thirty-third session (New York, 29 June-10 July 1998) on the basis of the revised draft prepared by the Secretariat (A/CN.9/WG.IV/WP.76). In the context of that discussion, the Commission noted with satisfaction that the Working Group had become generally recognized as a particularly important international forum for the exchange of views regarding the legal issues of electronic commerce and for the preparation of solutions to those issues.

8. The Commission noted that, at the close of the thirty-second session of the Working Group, a proposal had been made that the Working Group might wish to give preliminary consideration to undertaking the preparation of an international convention based on provisions of the Model Law and of the draft Uniform Rules. The Working Group had agreed that the topic might need to be taken up as an agenda item at the thirty-third session of the Working Group on the basis of more detailed proposals possibly to be made by interested delegations. However, the preliminary conclusion of the Working Group had been that the preparation of a convention should in any event be regarded as a project separate from both the preparation of the Uniform Rules and any other possible addition to the Model Law. Pending a final decision as to the form of the Uniform Rules, the suggestion to prepare a convention at a later stage should not distract the Working Group from its current task, which was to focus on the preparation of draft uniform rules on digital and other electronic signatures, and from its current working assumption that the Uniform Rules would be in the form of draft legislative provisions. It had been generally understood in the Working Group that the possible preparation of a draft convention should not be used as a means of reopening the issues settled in the Model Law, which might negatively affect the increased use of that already successful instrument (A/CN.9/446, para. 212).

9. The Commission noted that a specific and detailed proposal for the preparation of a convention had been submitted by a delegation to the Working Group for consideration at a future session (A/CN.9/WG.IV/WP.77). Diverging views were expressed in that respect. One view expressed was that a convention based on the provisions of the Model Law was necessary, since the UNCITRAL Model Law on Electronic Commerce might not suffice to establish a universal legal framework for electronic commerce. Owing to the nature of the instrument, the provisions of the Model Law were subject to

variation by any national legislator that enacted them, thus detracting from the desired harmonization of the legal rules applicable to electronic commerce. The opposite view was that, owing to the rapidly changing technical background of electronic commerce, the matter did not easily lend itself to the rigid approach suggested by an international convention. It was pointed out that the Model Law was of particular value as a collection of principles, which could be enacted in domestic legislation through various formulations to accommodate the increased use of electronic commerce.

10. The prevailing view was that it would be premature to undertake the preparation of the suggested convention. Delegations of various countries indicated that law reform projects based on the provisions of the Model Law were currently under way in those countries. Concern was expressed that the preparation of an international convention based on the Model Law might adversely affect the widespread enactment of the Model Law itself which, only two years after its adoption by the Commission, was already being implemented in a significant number of countries. Moreover, it was generally felt that the Working Group should not be distracted from its current task, namely, the preparation of draft Uniform Rules on Electronic Signatures, as agreed by the Commission. Upon concluding that task, the Working Group would be welcome, in the context of its general advisory function with respect to the issues of electronic commerce, to make proposals to the Commission for future work in that area. It was suggested by the proponents of a convention that the matter might need to be further discussed at a future session of the Commission and in the context of the Working Group, possibly through informal consultations. It was recalled that, while possible future work might include the preparation of a convention, other topics had also been proposed, such as the issues of jurisdiction, applicable law and dispute settlement on the Internet. [3/]

11. The Working Group on Electronic Commerce, which was composed of all the States members of the Commission, held its thirty-third session in New York from 29 June to 10 July 1998. The session was attended by representatives of the following States members of the Working Group: Australia, Austria, Brazil, Cameroon, China, Colombia, Egypt, Finland, France, Germany, Honduras, Hungary, Iran (Islamic Republic of), Italy, Japan, Lithuania, Mexico, Romania, Singapore, Spain, Thailand, Uganda, United Kingdom of Great Britain and Northern Ireland and the United States of America.

12. The session was attended by observers from the following States: Canada, the Czech Republic, the Democratic Republic of Congo, Denmark, Gabon, Indonesia, Ireland, Madagascar, the Netherlands, Panama, Poland, Portugal, the Republic of Korea, Saudi Arabia, Sweden, Switzerland, Tunisia and Turkey.

13. The session was attended by observers from the following international organizations: United Nations Development Programme (UNDP), World Intellectual Property Organization (WIPO), African Development Bank, European Commission, Organisation for Economic Cooperation and Development (OECD), *Comité maritime international* (CMI), European Law Student Association (ELSA) International, Grupo Latinoamericano de Abogados para el Comercio Internacional (GRULACI), Instituto Iberoamericano de Derecho Maritimo (INIDIE), International Association of Ports and Harbors (IAPH), International Bar Association (IBA), International Chamber of Commerce (ICC), Internet Law and Policy Forum (ILPF), Society for Worldwide Interbank Financial Telecommunications (S.W.I.F.T.), and *Union internationale des avocats* (UIA).

14. The Working Group elected the following officers:

Chairman: Mr. Mads Bryde **Andersen** (Denmark);

Vice-Chairman: Mr. **Pang** Khang Chau (Singapore);

Rapporteur: Mr. Jair Fernando **Imbachi Ceron** (Colombia).

15. The Working Group had before it the following documents: provisional agenda (A/CN.9/WG.IV/WP.75); a note by the Secretariat containing draft uniform rules on digital signatures, other electronic signatures, certification authorities and related legal issues (A/CN.9/WG.IV/WP.76); and a note reproducing the text of a proposal by the United States of America for a draft international convention on electronic transactions (A/CN.9/WG.IV/WP.77).

16. The Working Group adopted the following agenda:

1. Election of officers.

2. Adoption of the agenda.

3. Legal aspects of electronic commerce: draft uniform rules on electronic signatures.

4. Other business.

5. Adoption of the report.

I. Deliberations and decisions

17. The Working Group discussed the issue of digital signatures, other electronic signatures, certification authorities and related legal issues on the basis of the note prepared by the Secretariat (A/CN.9/WG.IV/WP. 76). The deliberations and conclusions of the Working Group with respect to those issues are reflected in Part II below. The Secretariat was requested to prepare, on the basis of those deliberations and conclusions, a set of revised provisions, with possible variants, for consideration by the Working Group at a future session. A delegation proposed future work on a convention on electronic transactions. That proposal was discussed informally, as reflected in Part III below.

II. Draft Uniform Rules on Electronic Signatures

General remarks

18. At the outset, the Working Group generally agreed that the current structure of the Uniform Rules constituted an acceptable basis for discussion. However, the view was expressed that the combination of a general part on electronic signatures and a specific part with very detailed rules on digital signatures might cause problems in respect of the relationship and interplay between these two parts. It was pointed out that the Uniform Rules to a large extent, could accommodate the various types of electronic signatures that were gradually becoming available on the market. The Uniform Rules could play an important role in enabling the use of electronic signature techniques in an open environment, in creating confidence as to the use of those techniques, and in avoiding discrimination among them. It was emphasized, however, that more clarity might be needed with respect to a number of issues, for example: the extent to which the Uniform Rules recognized party autonomy in the context of closed or semi-closed networks; the capability of the Uniform Rules to accommodate systems where certification authorities functioned as independent service providers and systems where parties would rely on a certificate issued by one of the parties; the adaptability of the Uniform Rules to specific techniques other than digital signatures; and the compatibility of the Uniform Rules with the existence of different degrees of security.

Chapter I. Sphere of application and general provisions

19. The Working Group decided to postpone its consideration of chapter I until it had completed its review of the substantive provisions of the Uniform Rules.

Chapter II. Electronic signatures

Section I. Electronic signatures in general

Article 1. Definitions

20. The Working Group decided to postpone its consideration of draft article 1 until it had completed its review of the substantive provisions of the Uniform Rules.

Article 2. Effect of electronic signature

21. The text of draft article 2 as considered by the Working Group was as follows:

> "(1) With respect to a data message authenticated by means of an electronic signature [other than a secure electronic signature], the electronic signature satisfies any legal requirement for

a signature if the electronic signature is as reliable as appropriate for the purpose for which the electronic signature was used, in the light of all the circumstances, including any relevant agreement.

"(2) Paragraph (1) applies whether the legal 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) Unless expressly provided elsewhere in [this Law], electronic signatures that are not [enhanced] [secure] electronic signatures are not subject to the regulations, standards, or licensing procedures established by ... *[the State-specified organs or authorities referenced in article]* or to the presumptions created by articles 4, 5 and 6.

"(4) The provisions of this article do not apply to the following: [...]."

Title

22. The view was expressed that the reference in the title of the draft article to the "effect of electronic signature" might be misleading. It was stated that, rather than focusing on the effects of electronic signatures, draft article 2 dealt with the circumstances under which an electronic signature would comply with the requirements of law, as referred to in article 7 of the Model Law. After discussion, it was agreed that the title of the draft article should read along the lines of "compliance with requirements of law".

Paragraph (1)

23. The view was expressed that the wording of paragraph (1) should parallel exactly the wording used in article 7 of the Model Law. Accordingly, it was suggested that paragraph (1) should read as follows:

"(1) With respect to a data message authenticated by means of an electronic signature [other than a secure electronic signature], the electronic signature meets any requirement of law or evidence for a signature if the method used to apply the electronic signature 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."

24. While support was expressed in favour of the suggested wording, it was pointed out that the reference to "any requirement of law or evidence" was inconsistent with the wording used in the Model Law. Article 7 of the Model Law referred to "where the law requires a signature", which addressed both requirements of law and requirements of evidence. Any inconsistency between the Model Law and the Uniform Rules in that respect might create difficulties in the interpretation of both instruments. Subject to the deletion of the words "or evidence", the Working Group adopted the suggested wording.

Paragraph (2)

25. The substance of paragraph (2) was found to be generally acceptable. For reasons of consistency with the terminology used in the Model Law, the Working Group agreed that the word "legal" should be deleted.

Paragraph (3)

26. The view was expressed that paragraph (3) was stating the obvious and should be deleted. The prevailing view, however, was that, since it could be expected that the vast majority of electronic signatures used in practice would not fall within the narrow category of "enhanced" or "secure" electronic signatures (which were being regulated in some countries), the Uniform Rules should make it abundantly clear that regulation applying to the higher level of "enhanced" or "secure" electronic signatures did not apply in general to all types of "electronic signatures". After discussion, it was agreed that paragraph (3) should be maintained in the Uniform Rules for the purpose of clarity.

Paragraph (4)

27. The Working Group found the substance of paragraph (4) to be generally acceptable.

Section II. [Enhanced][Secure] electronic signatures

Article 3. Presumption of signing

28. The text of draft article 3 as considered by the Working Group was as follows:

> "(1) A data message is presumed to have been signed [if] [as of the time] a[n] [enhanced] [secure] electronic signature is affixed to the data message.
>
> "(2) The provisions of this article do not apply to the following: [...]."

Paragraph (1)

29. It was generally agreed that it was appropriate for the Uniform Rules to distinguish a narrow range of techniques that were capable of providing a high degree of reliability from "electronic signatures" in general. However, as a matter of drafting, doubts were expressed as to whether either of the words "enhanced" or "secure" electronic signature was acceptable. Although use of the word "secure" was acknowledged to be a term that was familiar in the context of electronic signatures, it was criticized on the ground that it introduced a subjective criterion and implied that signatures that did not fall within the category of "secure" were inherently insecure. The view was also expressed that "secure" might be interpreted as implying too much in terms of the "security" of the signature under draft article 3. Use of the term "enhanced" was said to be capable of referring to almost any attribute of a signature and was generally too uncertain, especially in relation to the concept of security of a signature. While the view was expressed that the word "enhanced" was almost meaningless in this context, the prevailing view was that, in the absence of a more appropriate term, which should be sought later, "enhanced" would be used. Suggestions for an alternative term included "qualified" and "certified", but these did not receive support.

30. Another concern of a drafting nature was that draft article 3 concentrated upon the "affixing"

of a signature, while the definition of an electronic signature in draft article 1(a) included the broader term "logically associated with a data message". It was suggested that language parallel to that of draft article 1 should be included in draft article 3.

31. The view was expressed that the words "[as of the time]" the electronic signature was affixed to the data message should be deleted. In support of that view, it was stated that the time of signing of a data message was not the focus of draft article 3 and the inclusion of such a reference was likely to lead to uncertainty. In reply, it was stated that the time at which a data message was signed had important legal consequences, especially in the context of third parties, and should be retained in the text of the draft article. After discussion, the Working Group generally felt that the question of the time at which the data message had been signed should not be addressed in the context of draft article 3, but might need to be further considered at a later stage in the preparation of the Uniform Rules.

32. A concern was expressed that draft article 3 was insufficiently distinguished from draft article 4. It was pointed out that, in some legal systems, the question of whether or not a data message was signed could not be separated from the issue of attribution of the signature. It was suggested that this difficulty could be overcome by combining draft articles 3 and 4. In reply, it was stated that, in other legal systems, the question of whether or not a data message had been signed, irrespective of the identity of the signer, could be important where the law required a signature, without indicating the identity of the signer, or where the sender's identity was not at issue.

33. The discussion focused upon the question of whether draft article 3 should be deleted, retained in the form of a presumption, or redrafted to establish a substantive rule of law. The concern was expressed that a presumption should be capable of rebuttal and the act of signature would be difficult to rebut. In response, it was stated that the presumption raised evidentiary issues which could be rebutted by evidence relating to the intention of the signing party, or to the reliability or appropriateness of the method used to sign the data message. By attaching the presumption to an enhanced electronic signature, the intention of the draft article was to distinguish the "enhanced" form of electronic signature from the more general form of electronic signature referred to in draft article 2. It was stated that, by achieving that special status, the enhanced electronic signature could be regarded as having passed certain tests and should not therefore be subjected to the same level of inquiry as the more general form of electronic signature.

34. As an alternative, the Working Group was invited to consider a proposed new paragraph (1) as follows:

> "Where the law requires a signature, that requirement is met by an enhanced electronic signature."

35. The discussion continued on the basis of that proposal. It was stated that the proposed text avoided the problems that might arise from the use of a presumption and recognized the principle of non-discrimination contained in article 5 of the Model Law. The purpose of the proposal was to establish a rule that an enhanced electronic signature met the requirement of article 7 of the Model Law that the method of authentication should be "as reliable as appropriate".

36. While support for the proposal was expressed, it was pointed out that it could only be properly

considered in the context of the definition of what constituted "enhanced" electronic signature. It was suggested that the proposal should be retained in square brackets pending consideration of that definition. Some support was expressed for the suggestion that the language of the proposal should be more directly related to article 7 of the Model Law. It should make it clear that an enhanced electronic signature could be regarded as one that satisfied the requirements established by the Model Law for reliability and appropriateness, and could thus be regarded as functionally equivalent to a handwritten signature.

37. A further concern was that article 7 of the Model Law, by emphasizing the appropriateness of the method in the light of the circumstances for which it was used, established a test in which the substantive rule was tied to a flexible measure. The proposed text established, in contrast, a fixed test. The suggestion was made that words along the lines of "unless it is proved that the enhanced electronic signature does not fulfil the requirements set out in article 7 of the Model Law" should be added at the end of the proposed text to ensure flexibility. In response, it was pointed out that the purpose of the proposal was to move beyond the test of article 7 of the Model Law and to establish a rule that all legal requirements for a signature would be met by an enhanced electronic signature, without reference to the circumstances of each case. The addition of the suggested words would indicate that there were doubts about whether an enhanced electronic signature did meet all requirements for a signature, and should not be included.

38. After consideration, there was wide support for the substance of the proposed text, but the Working Group decided to retain it in square brackets pending consideration of the definition of [enhanced] electronic signature. It was also decided that words along the lines of "unless it is proved that the enhanced electronic signature does not fulfil the requirements of article 7 of the Model Law" should be added in square brackets for continuation of the discussion at a future session.

Paragraph (2)

39. The Working Group found the substance of paragraph (2) to be generally acceptable.

Article 4. Presumption of attribution

40. The text of draft article 4 as considered by the Working Group was as follows:

"(1) A[n] [enhanced] [secure] electronic signature is presumed to be that of the person by whom, or on whose behalf, it purports to have been used,

Variant A unless the purported signer establishes that the [enhanced] [secure] electronic signature was affixed without authorization.

Variant B provided that the relying party establishes that the security procedure or combination of security procedures used to verify the signature was

(a) commercially reasonable under the circumstances;

(b) applied by the relying party in a trustworthy manner; and

(c) relied upon by the relying party reasonably and in good faith.

"(2) The provisions of this article do not apply to the following: [...]."

General remarks

41. Doubts were expressed regarding the usefulness and appropriateness of including a presumption of attribution along the lines of draft article 4 in the draft Uniform Rules. It was stated that the matter dealt with under draft article 4 was relevant to general civil procedure and, as such, might not easily lend itself to harmonization by way of an international instrument. It was suggested that the question of attribution of electronic signatures should be left to applicable domestic law.

42. The prevailing view, however, was that an article along the lines of draft article 4 was needed. While some objections to the alternative variations of draft article 4 were expressed, it was widely felt not only that attribution might be essential for establishing the legal effect of a signature, but also that an article on attribution was important for establishing trust and certainty in the use of electronic signatures.

Paragraph (1)

43. Support was expressed in favour of retaining Variant A. Support was also expressed for a draft article which would include both Variant A and Variant B. It was pointed out that consideration of the Variants as alternative texts was difficult because they were not true alternatives and dealt with different aspects of the presumption of attribution. Variant A dealt directly with the fact of signature and the questions of attribution and authorization of the signature, while Variant B established the grounds upon which the relying party could get the benefit of the presumption of attribution, notwithstanding that the signature might have been affixed without authorization.

44. In favour of retaining only Variant A, the view was expressed that it appropriately placed the burden of proof on the party most able to prove the fact of signature, namely, the signer, while the rules in Variant B relied upon a number of subjective standards that would be difficult to apply in practice. In addition, it was pointed out that Variant B unfairly imposed potential liability on the signer, notwithstanding that the signer might have proved, in satisfaction of the proviso in Variant A, that the signature was not authorized. In that context, the view was strongly expressed that a provision along the lines of Variant B would not be appropriate for transactions involving consumers. While the Working Group decided not to enter at that stage into a general debate as to whether the draft Uniform Rules should be applicable to consumer transactions, it was widely agreed that, in preparing the Uniform Rules, the Working Group should focus on transactions between commercial users of electronic communication techniques.

45. In support of retaining elements of Variant B in the Uniform Rules, it was stated that it was important, in the context of determining legal effect, for any party relying on the electronic signature to have to prove the matters set out in subparagraphs (a) to (c) before that party could claim the benefit of any presumption. The view was expressed that the requirements contained in Variant B were not

properly located as part of a provision establishing a presumption. In this regard, it was suggested that the placement of Variant B might need to be reconsidered, not only in terms of its location in article 4, but also in terms of the relationship of article 4 to the definitions in draft article 1 and the substantive articles of the Uniform Rules. Subparagraph (c) of Variant B, for example, was noted as being of relevance to draft article 7 dealing with liability. There was some support for this suggestion, and it was agreed that it would be appropriate to reconsider the issues raised by Variant B in the context of the definition of [enhanced] electronic signature and the substantive provisions on liability. After discussion, the Working Group agreed that Variant B should be deleted.

46. As in the case of draft article 3, the drafting of draft article 4 in the form of a presumption was questioned, particularly in relation to whether it was a rebuttable presumption and the means by which it could be rebutted. The view was expressed that this should be made clear in the text of the article itself. It was pointed out that there might be a problem in establishing a general presumption applicable to all types of transactions, because such a presumption depended for its efficacy upon a number of variable factors, such as: the technical reliability of certain signatures; the expectation of the parties as to how certain signature devices were to be treated; and the nature of the transaction itself. In some types of transactions, for example, financial transactions, it might be appropriate to have a high level of responsibility attaching to the use of a signature without authorization. For low level transactions, such a high level of responsibility might not be appropriate.

47. There was also some concern expressed about whether the presumption should be structured to provide that rebuttal could be achieved simply by denial of the application of the signature, or whether it should also require proof of absence of authorization.

48. The focus of the article on the parties required to perform certain acts was criticized as being too narrow and specific. The requirement that it should be the relying party who must establish the requirements set out in subparagraphs (a) to (c) of Variant B was too narrow. Similarly, the requirement in subparagraph (b) that the security procedure must be applied by the relying party was too restrictive. The focus of the draft article should be on whether a security procedure was applied in a reasonable manner (irrespective of who applied it), or on what was required to be proved. The same criticism was made in respect of Variant A in relation to the requirement that the purported signer must establish the lack of authorization. It was generally agreed that the drafting of draft article 4 should be depersonalized to reflect these concerns.

49. The draft article was also criticized on the ground that it dealt with both authorization and attribution, two different concepts which should be treated separately. The proposal was made that draft article 4 should focus upon the issue of authorization, rather than attribution. In reply, it was noted that paragraph (2) of article 13 of the Model Law included authorization in provisions dealing with attribution.

50. The drafting of draft article 4 gave rise to a number of concerns. One suggestion was that the draft Uniform Rules should respect the principles of technology and implementation neutrality, and that the drafting of Variant B did not accord with these principles. In particular, it was pointed out that the words “relying party” were generally understood to be specific to digital signature technology. Since the phrase was not defined in the context of the Uniform Rules, it needed to be made clear in draft article 4 that the meaning of “relying party” was not limited to the relying party in the situation of a certified digital signature, but could include a broader application. In view of the decision to delete

Variant B, this proposal was not pursued. It was understood, however, that a text reflecting the substance of deleted Variant B might be proposed at a future meeting.

51. Additional suggestions were made to improve the drafting of draft article 4. One suggestion was that, instead of the word "used" in respect to the signature, wording along the lines of "created", "originated" or "generated" should be adopted. That suggestion was accepted by the Working Group. Another suggestion was that the use of the phrase "a combination of security procedures" in the deleted Variant B would have been unnecessary because the use of different procedures would still result in the use of "a security procedure". The Working Group agreed that that suggestion would need to be considered further in the context of other draft articles in which that phrase was used.

52. In order to reflect the suggestion made to depersonalize the text of draft article 4 and to expand the category of persons who could perform the required acts, the following text was proposed as an alternative to paragraph (1):

> "An [enhanced] electronic signature is presumed to be that of the person by whom, or on whose behalf, it purports to have been generated, unless it is established that the [enhanced] electronic signature was applied neither by the purported signer nor by a person who had the authority to act on its behalf."

After discussion, the Working Group adopted that reformulation of paragraph (1).

Paragraph (2)

53. The Working Group found the substance of paragraph (2) to be generally acceptable.

Article 5. Presumption of integrity

54. The text of draft article 5 as considered by the Working Group was as follows:

> "(1) If the purported signer has used a security procedure which is capable of providing [reliable] evidence that a data message or any [[enhanced] [secure] electronic] [electronic] signature thereon has not been changed since the time the security procedure was applied to the data message or to any signature, then it is presumed [in the absence of evidence to the contrary,] that the data message or the signature has not been changed.
>
> "(2) The provisions of this article do not apply to the following: [...]."

Paragraph (1)

55. It was generally agreed, at the outset, that a provision along the lines of paragraph (1) was useful to clarify the ways in which the requirements of article 8 of the Model Law could be fulfilled. Various views were expressed and suggestions were made for possible improvement of paragraph (1).

56. The Working Group considered the question of whether draft article 5 should deal with both the

integrity of the signature and the integrity of the data message. It was generally felt that the current wording of paragraph (1), which referred to the integrity of the data message "or any signature", was unclear and might lead to erroneous interpretation, for example, as to whether verification of the integrity of the signature only would create any presumption as to the integrity of the message. The suggestion was made that draft article 5 should deal with the integrity of the signature and the integrity of the data message in separate provisions. Alternatively, it was suggested that draft article 5 should deal only with those security procedures that provided evidence as to the integrity of both the signature and the message. After discussion, however, it was generally agreed that the Uniform Rules should focus on the integrity of the message only.

57. With respect to the notion of "security procedure", a concern was expressed that a definition might be needed to clarify the relationship between a security procedure and an electronic signature or an "enhanced" electronic signature. It was suggested that the notion of "enhanced security procedure" might need to be introduced to deal with issues of integrity of the message, as opposed to unqualified "security procedures" that might be appropriate for dealing with the issue of identity of the signer. It was generally agreed that the questions regarding the definition of "security procedure" and the level of security that would need to be reached to give rise to a presumption might be solved through the application of draft article 6, under which determination of what constituted an acceptable "security procedure" would be made by a declaration of a competent authority or by agreement of the parties.

58. As to whether the security procedure should be applied by the signer only, it was widely felt that the wording of paragraph (1) should be depersonalized. It was agreed that such a reformulation would more appropriately reflect situations (which were reported to be of considerable practical importance) where the security procedure would not be "applied" by the signer, but would suppose action on the part of both the signer and the relying party.

59. With respect to the words "capable of providing", the view was expressed that paragraph (1) insufficiently reflected the need for any security procedure to be applied properly and successfully in order to give rise to a presumption of integrity of the data message. To that effect, it was proposed that the words "is capable of providing reliable evidence" should be replaced by wording along the lines of "ensures", or "provides reliable evidence". Those suggested wordings were objected to on the grounds that it would be pointless to prescribe that evidence of integrity should be provided in order to give rise to a presumption of integrity. The aim of draft article 5 was precisely to establish that the use of certain security procedures (that might be recognized at an early stage through draft article 6, or at a later stage by a court under article 8 of the Model Law) should entail a presumption of integrity based on the recognition of the fact that such procedures were "capable" of verifying the integrity of the message. It was generally agreed, however, that draft article 5 should clarify that the presumption of integrity would only result if the security procedure had been successfully and properly applied.

60. As regards the words "in the absence of evidence to the contrary" between square brackets, a concern was expressed that such wording provided only a very weak presumption, since any evidence to the contrary would rebut the presumption. Compared to the presumption in draft article 4, draft article 5 provided a weaker presumption and the discrepancy might need to be addressed. A further concern was that, while draft article 5 was formulated as a rebuttable presumption, it contained no indication as to how the presumption might be rebutted. It was suggested that additional wording might need to be added to that effect to draft article 5. The prevailing view, however, was that, while it was

appropriate for draft article 5 to establish a rule of evidence, it might be difficult to harmonize in more detail the level of the presumption and the means by which it could be rebutted. It was generally felt that those matters might be better dealt with by applicable domestic law outside the Uniform Rules.

61. With a view to reflecting the above-mentioned views and concerns, the following alternative formulations were proposed for paragraph (1):

"*Variant A* Where [a trustworthy security procedure] [an enhanced electronic signature] is properly applied to a designated portion of a data message and indicates that the designated portion of the data message has not been changed since a specific point in time, it is presumed that the designated portion of the data message has not been changed since that time.

"*Variant B* Where a security procedure is capable of showing [reliably] [with substantial certainty] that the designated portion of a data message has not been changed since a specific point in time, and a proper application of that procedure indicates that the data message has not been changed, it is presumed that [the integrity of the data message has been preserved] [the data message has not been changed] since that time."

62. While considerable support was expressed in favour of Variant B, the Working Group decided that both Variants should be reflected in the revised draft of the Uniform Rules to be prepared by the Secretariat for continuation of the discussion at a later session. It was pointed out that, depending on the final decision as to the contents of paragraph (1), the placement of draft article 5 might need to be reconsidered. Should the text of paragraph (1) contain no reference to the notion of "enhanced electronic signature", the scope of draft article 5 would be broader and the provision might be more appropriately placed in section I, which dealt with electronic signatures in general, or in a separate section of the Uniform Rules.

Paragraph (2)

63. The substance of paragraph (2) was found to be generally acceptable.

Article 6. Predetermination of [enhanced] [secure] electronic signature

64. The text of draft article 6 as considered by the Working Group was as follows:

"(1) A security procedure or a combination of security procedures satisfies the requirements of an [enhanced] [secure] electronic signature if it is so declared by ... *[the organ or authority specified by the enacting State as competent to make such declaration ...]*

"(2) As between the person signing a data message and any person relying on the signed message, a security procedure or a combination of security procedures is deemed to fulfil the requirements of an [enhanced] [secure] electronic signature if expressly so agreed by the parties.

"(3) The provisions of this article do not apply to the following: [...]."

General remarks

65. There was general support for the inclusion of an article along the lines of draft article 6 on the ground that predetermination of qualified security procedures would contribute to the certainty and trustworthiness of electronic signatures and electronic commerce generally. With respect to the issue of party autonomy as provided in paragraph (2), while there was widespread support for the principle of freedom of contract, there was a general view that this issue needed to be discussed in respect of the text as a whole, to determine which provisions could (and which could not) be varied by agreement. It was pointed out that, should the Working Group decide that the Uniform Rules should form part of the Model Law, the relationship of these Rules with article 4 of the Model Law would need to be considered and article 4 amended as necessary. The Working Group agreed to defer its discussion on the issue of mandatory and non-mandatory provisions until it had completed its review of the substantive provisions of the Uniform Rules.

Paragraph (1)

66. Paragraph (1) was generally regarded as an acceptable means of assisting the predetermination of what constituted an [enhanced] electronic signature. A number of suggestions were made to clarify and improve the drafting.

67. The Working Group recalled that, in the context of the discussion of draft article 4, it had been agreed that the words "a security procedure" should be substituted for "a security procedure or combination of security procedures".

68. It was observed that a declaration made under paragraph (1) without restraint could diminish trust and confidence in electronic commerce and that it would therefore be appropriate to require conformation to international standards, to the extent that they existed and were relevant. After discussion of this proposal, the Secretariat was asked to prepare appropriate text along the lines of "the declaration should be consistent with recognized international technical standards to the extent that they exist" for addition to paragraph (1).

69. It was widely felt that, given the far-reaching potential of a predetermination of [enhanced] electronic signature status, any declaration made under paragraph (1) should only be made by an organ

or authority which was clearly in a position or authorized to make such a declaration, whether it be a public authority or a publicly-appointed private authority. In order to focus the draft article more clearly on how predetermination of [enhanced] status could occur, it was proposed that paragraph (1) should be redrafted to align the language with the heading by substituting "determination" for "declaration" and referring to the authority making the determination at the beginning of the provision along the following lines: "*[The organ or authority specified by the enacting State as competent]* may determine that a security procedure satisfies the requirements of an [enhanced] [secure] electronic signature". Wide support was expressed in favour of that proposal.

Paragraph (2)

70. There was general support for the inclusion of a provision along the lines of paragraph (2) providing for party autonomy. It was pointed out that paragraph (2) allowed a flexible approach to the issue of predetermination of [enhanced] electronic signatures and also reflected the importance of party autonomy in the context of closed systems. There was some concern, however, that paragraph (2) might allow parties to agree to deviate from mandatory form requirements and that the provision should be limited to allowing party autonomy within the bounds of national law. In that regard, it was proposed that the words "to the extent permitted by law" should be added to the end of the paragraph, and that paragraph (3) should be deleted. In support of that proposal, it was pointed out that paragraph (3) required an enacting State to give careful consideration to possible exclusions, while the proposed language implemented existing restrictions and could include future restrictions in the general law. After discussion, the Working Group adopted that proposal.

71. As a matter of drafting, concern was expressed that, given the generally understood meaning of the phrase, use of the words "relying party" in paragraph (2) might be misinterpreted as referring to a party outside the contractual agreement affecting the determination of [enhanced] signature status. Such a misinterpretation would have the undesirable result that third parties could be adversely affected by that agreement. It was generally agreed that, as between themselves and for their own use, parties could agree on the effect of the security procedure they used, including that it was an [enhanced] electronic signature, but that the language of the paragraph needed to clarify that such an agreement could not affect persons who were not party to the agreement. It was pointed out that it was not the intention of the provision to allow a third party to be affected by an agreement between the signer and the addressee of the signed data message. Another view was that it needed to be indicated more clearly that the provision only applied in a commercial context and that the emphasis should be upon consenting parties, and not simply contracting parties.

72. A related concern was the relationship between article 7 of the Model Law, which was not subject to variation by agreement, and draft article 6. The effect of paragraphs (1) and (2), it was suggested, might lead parties to believe that, by agreeing on what constituted an [enhanced] electronic signature, they could avoid the requirements of article 7 as to what constituted a functional equivalent to a signature. The effect of paragraph (2), it was stated, should be that once a security procedure had satisfied the requirements for a signature under article 7 of the Model Law, parties could agree on what would constitute an [enhanced] electronic signature. It was also observed that, in addition to the situations envisaged by paragraphs (1) and (2), there could be a third possibility, namely, that a procedure not covered by either paragraph (1) or (2) could nevertheless satisfy the definition of an [enhanced] signature, for example, where so recognized by a court. That issue was not pursued in the

discussion.

Proposed redrafting of draft article 6

73. A proposal was made for a revision of draft article 6, taking into account the redrafting that had been discussed and agreed in respect of paragraph (1). Pursuant to that proposal, paragraph (1) should be divided into two parts, the first dealing with determinations that security procedures would satisfy the requirements of an electronic signature, and the second addressing security procedures that would satisfy the integrity requirements of article 5. A new paragraph (2) would allow parties to determine the legal effect of their signatures. Language along the following lines was proposed:

> "(1) *[The organ or authority specified by the enacting State as competent]* may determine:
>
> (a) that an electronic signature satisfies the [requirements] of article 1(b);
>
> (b) that a security procedure satisfies the requirements of article 5."
>
> "(2) As between the person signing a data message and any person relying on the signed message, the parties may determine the effect of a signature or a security procedure if expressly agreed between the parties, subject to these Rules and applicable law."

74. The Working Group generally agreed with the proposed text, subject to some drafting changes. One proposal was that the words "these Rules and" should be placed within square brackets, pending future discussion regarding the issue of compliance with mandatory provisions of the Uniform Rules. That proposal was accepted and the Working Group agreed that discussion on the issue of which provisions of the Uniform Rules should be mandatory should be postponed, together with issues touching upon consumer law.

75. Some concern was expressed as to what the reference to parties determining "the effect" of the signature would mean. One objection was that parties could not agree on the legal effect that signatures would have, but could agree on how they should sign a data message. Another view was that the parties could agree as to the legal effect that a particular form of signature would have, but could not agree to confer legal status on a particular form of signature. Yet another view was that the provision in paragraph (2) should be limited to a single instance of the use of a particular signature. After discussion, it was agreed that the words "the effect" be placed in square brackets pending further discussion of what this phrase might mean. The Secretariat was requested to prepare a revised version of draft article 6 to reflect the above discussion.

Article 7. Liability for [enhanced] [secure] electronic signature

76. The text of draft article 7 as considered by the Working Group was as follows:

"*Variant A*

Where the use of a[n] [enhanced][secure] electronic signature was unauthorized and the purported signer did not exercise reasonable care to avoid the unauthorized use of its signature and to prevent the addressee from relying on such a signature, the purported signer is liable [to pay damages to compensate the relying party] for harm caused, unless the relying party knew or should have known that the signature was not that of the purported signer.

"*Variant B*

Where the use of a[n] [enhanced][secure] electronic signature was unauthorized and the purported signer did not exercise reasonable care to avoid the unauthorized use of its signature and to prevent the addressee from relying on such a signature, the signature shall nevertheless be regarded as that of the purported signer, unless the relying party knew or should have known that the signature was not that of the purported signer."

77. It was suggested that the title of the draft article might need to be reworded to indicate that the focus of the provision was on the unauthorized use of the signature. Wording along the lines of: "Liability for unauthorized use of [enhanced][secure] electronic signature" was proposed.

78. As to the scope of the draft article, it was suggested that the rule on liability for unauthorized use of an enhanced signature should be expanded to apply to ordinary electronic signatures as well. Another suggestion was that draft article 7 should be restructured to distinguish the cases where: (a) the unauthorized use of the signature resulted from the criminal intervention of a hacker; (b) the signature was used by an unauthorized employee or former employee of the purported signer; or (c) the signature was used by an authorized employee, but for purposes outside the scope of the authorization.

79. It was stated by a number of delegations that, in order to avoid possible interference with the domestic law of contracts and the law of agency, the subject matter of draft article 7 should be left to applicable domestic law and draft article 7 should be deleted. However, this proposal did not receive sufficient support. Further discussion focused on Variants A and B.

Variant A

80. Strong support was expressed in favour of Variant A. It was pointed out that a provision along the lines of Variant A was necessary to make it clear that the purported signer could not repudiate its signature merely by indicating, under draft article 4, that the signature had been used without authorization. In addition to the lack of authorization referred to in draft article 4, the purported signer should demonstrate under draft article 7 that it had not been negligent in protecting its signature from unauthorized use. In that context, a concern was expressed that the allocation of the burden of proof under Variant A might not be appropriate. It was pointed out that, under Variant A, the relying party

would be burdened with the need to prove that the purported signer had not exercised reasonable care to avoid the unauthorized use of its signature. It was suggested that the provision might need to be redrafted to the effect of reversing the burden of proof, so that the purported signer would have to prove that it had exercised reasonable care in protecting its electronic signature.

81. In support of Variant A, it was also pointed out that the provision appropriately focused on issues of liability, as opposed to Variant B, which might be excessively burdensome for the purported signer if it were to be interpreted as tying strictly the purported signer to the contents of the message authenticated by means of an unauthorized signature.

82. However, objections were expressed against Variant A. One objection was that it might not be appropriate to create a standard of reasonable care with respect to emerging practices such as those of electronic signatures, which were developing in a rapidly changing technical environment and did not have a background of established usages or practices. In that context, a provision along the lines of Variant A might discourage the use of electronic signatures by setting too strict a standard. The mere reference to the notion of "liability" in a provision dealing with purported signers and relying parties might deter potential users from engaging into electronic signature practice. In that respect, Variant B, which avoided any reference to the notion of liability, might be more acceptable (see below, para. 84).

83. In response, it was observed that, in many countries, the standard of reasonable care established by Variant A was already applicable to electronic commerce as a generally applicable rule of conduct under domestic law. While the provisions of Variant A might be unnecessary in those countries, it was emphasized that international harmonization of the law with respect to that issue might be useful. While it would be unwise for the Uniform Rules to attempt to unify the law applicable to compensation for pure economic loss, or otherwise to interfere with the law of contractual or tortious liability, the Working Group should not shy away from providing clarity as to the basic rules of conduct to be followed by parties when using electronic signatures. It was also observed that the standard of reasonable care, as contained in Variant A, was sufficiently flexible to accommodate newly emerging practices of electronic commerce. Moreover, the standard of conduct set forth in Variant A might be less stringent than standards of conduct applicable under specific areas of domestic laws. Furthermore, it was pointed out that, far from discouraging the use of electronic signatures, the existence of known uniform standards of conduct was likely to generate increased confidence in the use of electronic commerce in general, provided that those standards of conduct were sufficiently reflective of industry practice.

Variant B

84. Limited support was expressed in favour of Variant B. It was stated that Variant B appropriately focused on attribution of enhanced electronic signatures in cases where the electronic signature was unauthorized, while leaving the question of liability to be dealt with by courts on the basis of domestic law. In that context, it was suggested that Variant B might be redrafted to limit its application in time, to include an element of foreseeability of the amount of damages that might result from the unauthorized use of the signature, and to make it clear that loss of expected profits would not fall within the scope of draft article 7. Alternatively, it was proposed that the wording of Variant B should be redrafted along the following lines:

> "Where the use of an [enhanced] electronic signature was unauthorized and the purported signer did not exercise reasonable care to avoid the unauthorized use of its signature and to prevent the addressee from relying on such a signature, the signature shall nevertheless be regarded as authorized, unless the relying party knew or should have known that the signature was not authorized".

85. It was generally agreed that draft article 7 could be maintained in square brackets in the Uniform Rules for continuation of the discussion at a later session. It was generally agreed that the issue of liability of the purported signer for negligence in protecting its electronic signature might need to be reopened in the context of draft article 13(2), which contained an obligation to revoke a certificate if the private key had been compromised.

86. With a view to accommodating the various views and concerns that had been expressed with respect to Variants A and B, the following was suggested as a possible revision of draft article 7:

> "Where (1) the use of an [enhanced] electronic signature was unauthorized; (2) the addressee reasonably relied on the signature in good faith to its detriment; and (3) the purported signer did not exercise reasonable care to avoid the unauthorized use of its signature and to prevent the addressee from relying on such signature, the signature shall be attributable to the purported signer for the purpose of allocating responsibility for the cost of restoring the parties to their position prior to the unauthorized use of the signature. The foregoing shall not apply to the extent that the addressee knew or should have known that the signature was unauthorized".

87. Alternatively, it was proposed that draft article 7 should read as follows:

> "Where the use of a[n] [enhanced][secure] electronic signature was unauthorized and the purported signer did not exercise reasonable care to avoid the unauthorized use of its signature and to prevent the addressee from relying on such a signature, the purported signer may be held liable only for the cost of restoring the parties to their position before the unauthorized use of the signature, unless the relying party knew or should have known that the signature was not that of the purported signer".

88. After discussion, the Working Group decided that the various texts suggested as possible alternatives for draft article 7 should be included as possible variants in the revised version of the Uniform Rules to be prepared for consideration at a future session, together with the text of Variant A as set forth in the note by the Secretariat.

Section III. Digital signatures supported by certificates

Article 8. Contents of [enhanced][secure] certificates

89. The text of draft article 8 as considered by the Working Group was as follows:

"For the purposes of these Rules, a[n] [enhanced][secure] certificate shall, as a minimum:

(a) identify the certification authority using it;

(b) name or identify the [signer][subject of the certificate] or a device or electronic agent under the control of [the signer] [the subject of the certificate] [that person];

(c) contain a public key which corresponds to a private key under the control of the [signer][subject of the certificate];

(d) specify the operational period of the certificate;

(e) be digitally signed or otherwise secured by the certification authority issuing it;

[(f) specify restrictions, if any, on the scope of the use of the public key;]

[(g) identify the algorithm to be applied]."

General remarks

90. At the outset of the discussion of draft article 8, concerns were expressed about the relationship between the article and the definition of an enhanced electronic signature in draft article 1(b). While the Working Group acknowledged that the definitions in draft article 1 of the Uniform Rules would need to be considered at a future session after the substantive articles had been finalized, it was agreed that the possible content of the definitions should be borne in mind in considering what the necessary elements of the substantive provisions might be.

91. Another concern related to the technology upon which the inclusion of draft article 8 in the Uniform Rules was based. It was pointed out that the draft article was based on three-party certification technology involving an independent certification authority in addition to the signer and addressee of a data message. In fact, what was currently developing in commercial usage was an emphasis upon two-party certification technology, and the view was expressed that the draft article might not be appropriate in that context. In that regard, a number of questions were raised as to whether inclusion of an article along the lines of draft article 8 would adversely affect two-party certification, whether it would it be necessary to establish a similar rule for two-party certification, or whether two-party certification should be specifically excluded from the scope of draft article 8. In reply, it was stated that, while two-party certification was largely contractual, there were situations where a third party might rely on the signature and it might be important to secure the interests of that relying party. The view was expressed that, notwithstanding any apparent similarity in that case with the situation of a relying

party in three-party certification, it would be difficult to draft a rule which applied to the different circumstances of two- and three-party certification. The application of draft article 8 to two-party certification and the need for a specific exclusion was widely felt to be an issue which should be pursued by the Working Group at a later stage.

92. Another concern related to technology was that, while the inclusion of a list of requirements to be met by the issuer of a certificate might add certainty to the use of digital signatures, the rapid development of technology was likely quickly to render such a detailed list irrelevant.

93. The view was expressed that it was not clear from the text of draft article 8 what the consequences would be where a certificate did not include all the information set forth in subparagraphs (a) to (g), what the purpose of draft article 8 was and how it related to draft articles 9 and 10. It was questioned whether draft article 8 was needed at all. It was pointed out that the obligations established by articles 9 and 10, which tied together the public and private keys and linked the two keys to identification of the signer, were central to the concept of an enhanced certificate supporting an enhanced signature and could not be considered separately from draft article 8. It was generally agreed that those issues were central to the inclusion of draft article 8 in the text and to the manner in which it should be formulated. A related concern was the relationship between draft article 8 and article 7 of the Model Law. In this regard, it was pointed out that it should not be assumed that, once draft article 8 was satisfied, the requirements of article 7 automatically would be satisfied. It was also pointed out that some of the requirements of draft article 8, including subparagraphs (d) to (g), did not go to establishing the reliability of the signature, as required by the test in article 7 of the Model Law. The relationship between these articles was not finally resolved in the context of draft article 8, but the Working Group agreed that that question would need to be considered again in the context of discussion on draft articles 9 and 10.

94. A number of different views were expressed as to the possible consequences of a certificate failing to satisfy the requirements of draft article 8. One view was that the consequences of failing to satisfy the requirements of draft article 8 appeared to be that use of the certificate might be prohibited under the Uniform Rules and the remaining rules in section III of the Uniform Rules would not apply. It was stated that this was a serious penalty, which was out of proportion to the requirements of subparagraphs (a) to (g). Another view was that the failure of a certificate to meet the conditions set forth in subparagraphs (a) to (g) did not mean that the signature supported by the certificate would cease to be a digital signature, although it might cease to have enhanced status. Under that view, the signature would still be considered to be a digital signature and the rules covering digital signatures which were not supported by a certificate would apply. A contrary view was that, while the certificate would not qualify under section III of the Uniform Rules as a certificate which could support an enhanced signature, the signature could still qualify as an enhanced signature under draft article 1(b) of the Uniform Rules; the only difference would be that the shortcut provided by section III of the Uniform Rules would not be available and the elements of the definition in draft article 1(b) would have to be proved. Yet another view was that the consequences could include that the certificate was not a certificate for the purposes of the Uniform Rules or, alternatively, that it might still be a certificate, but that the issuer of the certificate might be liable for misrepresentation if it were to represent that the certificate supported an enhanced signature. A related view was that a certification authority should not be able to escape liability under the Rules on the basis that it had not issued a certificate which qualified as an enhanced certificate. In such a situation, the certification authority should be treated as

if it had issued an enhanced certificate. While the Working Group did not reach agreement on what the consequences of failure to comply with draft article 8 should be, it was agreed that it was not necessary to do so at this time, but that it would be important to consider this issue in the context of the remaining provisions of section III.

95. It was suggested that, because draft article 5 as revised by the Working Group included provisions applicable to certificates and signatures to be used for securing the integrity of the data message (as distinct from identification), this distinction should to be reflected in draft article 8. That proposal received little support.

96. As a matter of drafting, there was some support for use of the term "signer". A contrary view was that this term was not appropriate in the context of the issuing of a certificate, where the parties involved were the issuer and the subject of the certificate. Only where a certificate had been issued and the subject of the certificate actually signed something could it be said that there was a "signer". Another view was that use of the word "signer" would potentially exclude electronic agents. It was also pointed out that where there was an interloper, the actual signer was not the "signer" in the sense of being the subject of the certificate. It was suggested that the phrase "the subject of the certificate" would resolve the uncertainty associated with the use of "signer". It was agreed that the discussion on terminology might need to be reopened at a future session on the basis of the revised draft prepared by the Secretariat.

97. A suggestion was made that an additional requirement should be added after subparagraph (b) to cover attributes of a signer other than identity. The proposal was made that words to the effect of "identify a specific attribute [of the signer] such as address, authority to act on behalf of a company, or the existence of specific permits or licences" should be added in a new subparagraph (c). That proposal received little support.

Chapeau

98. As a matter of drafting, it was proposed that the words "and in the context of digital signatures" should be added after the word "Rules" in order to clarify the scope of the provision. Another proposal was that the *chapeau* should establish a positive obligation, binding on the issuer of the certificate, rather than a standard which established minimum criteria to be met for qualification as an enhanced certificate. In addition, it was suggested that draft article 8 should allow for variation by agreement between the parties. The following text was proposed:

> "For the purposes of these Rules and in the context of digital signatures, the issuer of an [enhanced] certificate shall, at a minimum, include the following information in the certificate, in the absence of contrary agreement:"

99. While there was general support for the proposal to change draft article 8 from an impersonal standard to an obligation binding on the issuer, the reference to party autonomy was criticized on the same grounds as those discussed in the context of draft article 6 concerning the possible effect of any such agreement upon third parties. The view was also expressed that allowing variation by agreement in draft article 8 would give the article the effect of a default rule, rather than a minimum standard. It was pointed out in this regard that the original purpose of the draft article was to establish a minimum

standard for the information to be included on the face of the certificate and that this would assist in harmonization of certification practices and build trust in electronic commerce. In response to these criticisms, it was proposed that the words “in the absence of contrary agreement” should be placed in square brackets pending further consideration of the issue of party autonomy.

100. Another proposal in relation to the sphere of application of draft article 8 was that it should apply to all certificates and that the reference to enhanced certificates should be deleted. In opposition to that proposal, it was stated that the only purpose of draft article 8 was to support enhanced signatures and the following text was proposed to reflect that scope:

> “For the purposes of these Rules, a certificate issued to support an enhanced signature shall, at a minimum, include:”

Although that proposal did not receive support, these words were used in a subsequent proposal for a new draft article 8 (see below, para. 112).

101. Yet another suggestion, which related to the scope of draft article 8, was made to the effect that use of the word “issue” might cover only the handing out of the certificate to the subject of the certificate, involving a contractual relationship between the certification authority and the subject of the certificate, as opposed to disclosure by the certification authority of the information in the certificate to any relying third party. Such a provision could apply to any type of certificate, whether enhanced or not. To give effect to that proposal, the following text was proposed:

> “A certification authority shall ensure that in disclosing to any party the information contained in a certificate at least the information in paragraph (2) shall be disclosed. The foregoing shall apply except to the extent that is otherwise expressly agreed between the certification authority and such party.”

102. As part of that proposal, it was stated that paragraph (2) should include subparagraphs (a) to (g) of draft article 8. Some support was expressed in favour of that inclusion, and these words were used in a subsequent proposal for a new draft article 8 (see below, para. 114).

Subparagraph (a)

103. The Working Group agreed that the substance of the requirement contained in subparagraph (a) was generally acceptable.

Subparagraph (b)

104. It was pointed out that the phrase “device or electronic agent” was a new concept in these Rules and might need to be defined. In support of including these words, the view was expressed that the Uniform Rules needed to provide clearly for the situation where a system could be set in process by a user and then function by itself, including signing data messages and having a certificate issued to it.

Subparagraph (c)

105. One concern expressed in respect of subparagraph (c) was that the public key did not need to

be referred to in the certificate as there were other means by which the relevant information could be made available. A proposal was made that the requirement could be changed to "identifying" rather than "containing" the public key.

Subparagraph (d)

106. Subparagraph (d) was criticized on the ground that the meaning of "operational period" was unclear. It was proposed that the words "specify the period during which the certificate may be used for verification of a digital signature" should be substituted. In opposition to that proposal, it was pointed out that the operational period of a certificate was the period during which a digital signature could be created validly. After a signature became invalid, the certificate could still be used to verify a signing which occurred before the time at which the signature became invalid. Retention of the current subparagraph (d) was generally agreed.

Subparagraph (e)

107. It was generally agreed that subparagraph (e) should be included in draft article 8. For reasons of clarity, and because signature of the certificate by the issuer was central to the validity of the certificate, it was suggested that the subparagraph should be included after draft subparagraph (a).

Subparagraph (f)

108. Discussion of subparagraph (f) focused upon the issue of incorporation by reference. Support was expressed in favour of retaining the subparagraph and removing the square brackets on the basis that the purpose of draft article 8 was to provide information to contracting and relying parties. The view was expressed that it was therefore essential that, if there were restrictions on the certificate, these should be made clear on the face of the certificate itself. In support of deleting subparagraph (f), it was pointed out that it might potentially include a very broad range of restrictions included in various other documents, such as a certification practice statement. Since such restrictions would need to be in human readable form to ensure accessibility to the user, rather than incorporated by reference to identifying codes, in some instances it might be technically infeasible to include a sufficiently large amount of information in the certificate in order to comply with this requirement.

109. In response to that criticism, it was suggested that, if restrictions were applicable to the certificate, it would be sufficient, as a minimum approach, for the certificate to simply "indicate" the existence of restrictions, rather than to specify the actual restrictions.

110. Another proposal was that an additional subparagraph should be added to subparagraph (f) to the effect that "In circumstances where restrictions are not stated in the certificate, the certificate may not be used to the detriment of third parties". That proposal was not supported. Yet another proposal was that it should be possible to recognize a "short form certificate" provided that: the certificate itself indicated that it was a short form; the certificate stated where the remote information was; and the information was accessible to an inquiring party. That proposal received some support. After further discussion, the Working Group agreed that the issue of incorporation by reference raised a number of difficult issues which had already been discussed in the context of the formulation of article 5 *bis* of the Model Law. The view was expressed that article 5 *bis* recognized that the issue of incorporation by reference could not be resolved in the context of electronic commerce until it had been resolved in the

general law, and that such a resolution could not be achieved in this discussion. A contrary view was that, since article 5 *bis* did not solve all issues related to incorporation by reference as it was only formulated in the negative, the issue needed to be secured in the Uniform Rules. After discussion, the Working Group agreed to leave the issue of incorporation by reference to be resolved according to national law.

Subparagraph (g)

111. Although some support was expressed in favour of retaining subparagraph (g), there was general agreement that it was not as important as subparagraphs (a) to (f).

Proposals for a new article 8

112. In response to criticisms that draft article 8 was too detailed and likely to be rendered irrelevant by the development of technology, the following text was proposed as a substitute for draft article 8:

> "For the purposes of these Rules, an enhanced certificate shall, at a minimum, include, or [where technically impractical] summarize and reference, information reasonable to satisfy [the applicable requirements of the relevant security procedure][its intended purpose]."

That proposal received little support.

113. Another proposal for a new draft article 8 was based on the view that the subparagraphs of the draft article were not of equal importance, and that there were two categories of elements, that is, those that should be mandatory and those where failure to comply did not necessarily lead to the loss of enhanced status, but rather to the loss of the ability to assert the enhanced status as against third parties. In support of that view, it was stated that subparagraphs (d) to (g) did not support the establishment of either the identification of the public and private keys and their functionality as a key pair, or the identification of the holder of the key pair, as required in draft articles 9 and 10. It was pointed out that these requirements might be difficult to satisfy with certain applications of certification practices. Subparagraphs (d) to (g) were therefore not essential requirements for an enhanced certificate. Subparagraphs (a) to (c), on the other hand, were stated to be essential to the purpose of draft article 8, formed the substance of draft articles 9 and 10 of the Uniform Rules, and indicated the linkage between draft article 8 and draft articles 9 and 10.

114. Yet another proposal based on the view that the subparagraphs of draft article 8 were not of equal importance was as follows:

> "(1) In disclosing to any party the information in a certificate, a certification authority [or the subject of a certificate] shall ensure that such information shall include, at least, that which is set out in paragraph (2), except to the extent expressly otherwise agreed between the certification authority [or the subject, as the case may be] and such party.
>
> "*Variant A* (2) The information referred to in paragraph (1) shall be:
>
> (i) for all certificates, [(a) to (c) and (e) of draft article 8], and

(ii) for [.....] certificates, [(d), (f), (g) of draft article 8].

"*Variant B* (2) The information referred to in paragraph (1) shall be [(a) to (c) and (e) of draft article 8].

(3) Certificates may also contain other information, including [(d), (f) and g)]"

115. With respect to the type of certificate referred to in subparagraph (ii) of Variant A, agreement could not be reached. It was widely felt that the provision should neither refer to enhanced certificates, nor describe the certificate by reference to the signature supported. It was pointed out that subparagraphs (a) to (g) would require some redrafting. It was suggested that the words "certification authority" should be deleted and the words "certificate issuer" substituted.

116. The proposed revision of the drafting of draft article 8 set forth in paragraph 114 above was widely supported, with some preference being expressed for Variant B. After discussion, the Working Group agreed that, for the purposes of future discussion, a revised draft of article 8 should include: the above proposal (including Variants A and B of subparagraph (ii) and paragraph (3)) and the text set forth in document A/CN.9/WG.IV/WP.76.

Article 9. Effect of digital signatures supported by certificates

117. The text of draft article 9 as considered by the Working Group was as follows:

"(1) In respect of all or any part of a data message, where the originator is identified by a digital signature, the digital signature [is a[n] [enhanced][secure] electronic signature][satisfies the conditions in article 7 of the UNCITRAL Model Law on Electronic Commerce] if:

(a) the digital signature was securely created during the operational period of a valid certificate and is securely verified by reference to the public key listed in the certificate; and

(b) the certificate binds a public key to [the signer's][a person's] identity by virtue of the fact that:

(i) the certificate was issued by a certification authority licensed by ... *[the enacting State specifies the organ or authority competent to license certification authorities and to promulgate regulations for the operation of licensed certification authorities]*; or

(ii) the certificate was issued by a certification authority accredited by a responsible accreditation body applying commercially appropriate and internationally recognized standards covering the trustworthiness of the certification authority's technology, practices and other relevant characteristics. A non-exclusive list of bodies or standards that comply with this paragraph may

be published by ... *[the enacting State specifies the organ or authority competent to issue recognized standards for the operation of licensed certification authorities]*; or

(iii) the certificate was otherwise issued in accordance with commercially appropriate and internationally recognized standards[.][; or]

[(iv) sufficient evidence indicates that the certificate [accurately] binds the public key to the [signer's][subject's] identity.]

"[(2) Where a data message is signed with a digital signature [created during the validity period of a certificate] that does not meet the requirements set forth in paragraph (1), the digital signature is regarded as a[n] [enhanced][secure] electronic signature if sufficient evidence indicates that [the certificate] accurately binds the public key to the identity of the [signer][subject of the certificate].]

"(3) The provisions of this article do not apply to the following: [...]."

General remarks

118. The placement of the draft article in section III was questioned, and the suggestion was made that the order of draft article 8 and draft article 9 should be reversed, with the effects of a digital signature supported by a certificate to be introduced before specifying the content of that certificate.

Paragraph (1)

Opening words

119. It was recognized, at the outset, that the meaning and purpose of draft article 9 was dependent upon which words in square brackets in the opening words of paragraph (1) were retained. The view was expressed that the words containing a reference to article 7 of the Model Law would establish legal effect, while the words relating to an [enhanced] electronic signature would result in a statement of which digital signatures could be regarded as [enhanced] electronic signatures, provided that the requirements were met. General support was expressed in favour of retaining the words [is a[n] [enhanced] electronic signature] without the square brackets in preference to the alternative words relating to article 7 of the Model Law.

Subparagraph (a)

120. The discussion focused on whether use of the word "securely" in subparagraph (a) was appropriate. In support of the retention of that word, it was recalled that it had been included in the Uniform Rules in order to reflect better the necessary trustworthiness of the digital signature process, which was essential to the concept of an [enhanced] electronic signature. It was suggested that the term "securely" could be deleted from subparagraph (a) if the opening words contained a reference to article 7 of the Model Law, because that reference to article 7 would imply the necessary level of trustworthiness. Since the Working Group had decided that the opening words of paragraph (1) should not refer to article 7 of the Model Law, the word "securely" should be retained in subparagraph (a) in

order to ensure that the digital signature was secure, since not all digital signatures verifiable with reference to a certificate were necessarily secure, especially if there was uncertainty as to the accuracy of the identification of the signer or the public key. One proposal was that the term should not only be retained in subparagraph (a), but that it should be elaborated upon by addition of the following text:

> "A digital signature is securely created and securely verified if it was generated using:
>
> (a) technical components for the generation and verification of the digital signature which would reliably reveal a forged digital signature and manipulated signed data and provided protection against unauthorized use of private signature keys;
>
> (b) technical components for the presentation of data to be signed which clearly indicate in advance the generation of digital signatures and enable identification of the data to which a digital signature applies; and
>
> (c) these technical components are adequately tested against current engineering standards."

121. In reply to that proposal, it was widely felt that the level of detail was too great for inclusion in the body of the Uniform Rules. However, explanations along the lines of the proposed text might be very useful in the context of a Guide to Enactment to the Uniform Rules.

122. Strong support was expressed in support of the deletion of the word "securely" in subparagraph (a). It was stated that use of the word introduced a new concept in relation to both creation and verification of a digital signature that was uncertain and ambiguous.

123. As a matter of drafting, a proposal was made that the text of subparagraph (a) should make it clear that both the creation of the signature and its verification should occur within the operational period of a certificate. A contrary view was that the operational period was only relevant to the verification of a digital signature and that subparagraph (a) should be revised by deleting the word "securely" in respect of verification and adding at the end of the subparagraph the words "and during the period in which verification is permitted to be made".

124. After discussion, the Working Group failed to achieve consensus with respect to the use of the word "securely" in subparagraph (a). It was decided that, in the variants of draft article 9 to be prepared for continuation of the discussion at a later session, retention and deletion of the word "securely" should be reflected as alternatives (see below, para. 133).

Subparagraph (b)

Opening words

125. The opening words of subparagraph (b) were found to be generally acceptable.

Subparagraphs (i) and (ii)

126. The substance of subparagraphs (i) and (ii) was found to be generally acceptable, although clarification as to the mandatory or other character of "licensed" and "accredited" was sought. It was stated that, while "licensed" suggested a mandatory, government-implemented scheme for regulating certification authorities, and "accreditation" suggested a non-mandatory, voluntary scheme, such schemes were not central to the creation of a secure digital signature. Security should be assessed by reference to objective, qualitative criteria, rather than by focusing upon the process of creation of a secure signature. That view was not supported and retention of subparagraphs (i) and (ii) was agreed.

Subparagraph (iii)

127. A concern was expressed that the use of the word "otherwise" in draft subparagraph (iii) might not be sufficiently clear in its application, and it was proposed that the words in subparagraph (iii) should be stated at the beginning of each of subparagraphs (i) and (ii), along the following lines: "the certificate was issued in accordance with commercially appropriate and internationally recognized standards by a certification authority licensed by ...".

128. In support of retention of subparagraph (iii) in its present form, the view was expressed that, together with subparagraph (iv), the subparagraph established what might be described as a "long form" of proof which enabled satisfaction of the requirement that a public key be bound to a person's identity in the event that the certificate was not issued in accordance with paragraph (1)(b)(i) or (1)(b)(ii) of draft article 9. In opposing the proposal to include the substance of subparagraph (iii) at the beginning of subparagraphs (i) and (ii), it was stated that that proposal would remove the "shortcuts", provided by subparagraphs (i) and (ii), to the establishment of the binding of the public key to the signer's identity, by requiring proof that the prescribed standards had been followed. If it was made clear that the process of licensing or accrediting a certification authority should be in accordance with appropriate standards of trustworthiness, it was unnecessary to restate this requirement in respect of the issue of certificates by those properly licensed or accredited bodies.

129. A concern of a drafting nature was that the reference to "commercially appropriate and internationally recognized standards" might not be appropriate and was likely to cause problems of interpretation in some languages. One proposal was that the term should be "commercially reasonable" and some reference should also be made to the origin of the standards by including the words "market-based". Another proposal was that the words "usages and practices" should be substituted for "standards". In opposing that proposal, it was pointed out that, since the word "usage" had a technical meaning in a number of legal systems which required that the usage be established over time and by means of wide use and support, it was inappropriate for use in the context of electronic commerce, where neither the Uniform Rules nor any other usage was sufficiently established to be applicable immediately. To resolve this difficulty, yet another proposal was made to include references to both "international technical standards" and "practices and usages", and to describe the latter as "commercial usages and practices".

130. With a view to reconciling the above-mentioned proposals, it was suggested that subparagraph (iii) should refer to a certificate issued "in accordance with international standards and commercial practices or usages widely known and regularly observed in the trade involved in the transaction". It was widely felt that the suggested language might constitute an acceptable basis for continuation of the discussion. However, doubts were expressed as to whether the suggested language was fully consistent

with other references to usages and practices (or to technical standards) that might exist in international texts in the field of international trade law. After discussion, it was agreed that the suggested language should be reflected between square brackets in the variants of draft article 9 to be prepared for consideration by the Working Group at a later stage.

Subparagraph (iv)

131. Support for the deletion of subparagraph (iv) was expressed on the grounds that it was unnecessary to state that the certificate binds the public key to the signer's identity if evidence could be adduced to prove that fact, as this would ordinarily be the case, irrespective of any rule in draft article 9. In support of retaining subparagraph (iv), it was pointed out that, in the event that the binding of the public key was not achieved by the application of subparagraph (i) or (ii), which prescribed only very limited methods and might not be widely applicable, or subparagraph (iii) which might, at the outset, have a limited application in the field of electronic commerce, it was necessary to state how this could otherwise be proved. The purpose of subparagraph (iv) was therefore to balance subparagraphs (i), (ii) and (iii) and to ensure the flexibility of draft article 9.

Paragraph (2)

132. Support was expressed for the retention of paragraph (2) on the same grounds as stated in respect of subparagraph (iv). It was realized, however, that it might not be necessary to retain both subparagraph (1)(b)(iv) and paragraph (2), which served essentially the same purpose.

Proposal for new draft article 9

133. In order to reflect the differing proposals and suggestions made in respect of draft article 9, the following revised draft was proposed:

"(1) *Variant A*

"In respect of all or any part of a data message, where the originator is identified by a digital signature, the digital signature is an [enhanced] electronic signature if:

(a) the digital signature was created during the operational period of a valid certificate and is [properly] verified by reference to the public key listed in the certificate;

(b) the certificate purports to bind a public key to [the signer's][a person's] identity;

(c) the certificate was issued for the purpose of supporting digital signatures which are [enhanced] electronic signatures; and

(d) the certificate was issued:

(i) by a certification authority licensed by ... *[the enacting State specifies the organ or authority competent to license certification authorities and to*

promulgate regulations for the operation of licensed certification authorities]; or

(ii) by a certification authority accredited by a responsible accreditation authority applying commercially appropriate and internationally recognized standards covering the trustworthiness of the certification authority's technology, practices and other relevant characteristics. A non-exclusive list of bodies or standards that comply with this paragraph may be published by ... *[the enacting State specifies the organ or authority competent to issue recognized standards for the operation of licensed certification authorities]*; or

[(iii) in accordance with commercially appropriate and internationally recognized standards.]

"*Variant B*

"In respect of all or any part of a data message, where the originator is identified by a digital signature, the digital signature is an [enhanced] electronic signature if:

(a) the digital signature was [securely] created during the operational period of a valid certificate and is [properly] verified by reference to the public key listed in the certificate; and

(b) the certificate binds a public key to the person's identity according to procedures established by:

(i) [*the enacting State specifies the organ or authority competent to license certification authorities and to promulgate regulations for the operation of licensed certification authorities*]; or

(ii) a responsible accreditation authority applying commercially appropriate and internationally recognized standards covering the trustworthiness of the certification authority's technology, practices and other relevant characteristics; or

(iii) [international standards and commercial practices or usages widely known and regularly observed in the trade involved in the transaction].

"(2) A digital signature that does not meet the requirements in paragraph (1) is regarded as an [enhanced] electronic signature if:

(a) sufficient evidence exists to indicate that:

(i) the certificate accurately binds the public key to the identity of the subject of the certificate; and

(ii) the digital signature was properly created and verified using a secure and trustworthy procedure; or

(b) it qualifies as an [enhanced] electronic signature under other provisions of these Rules."

134. In explanation of the proposal, it was stated that, in subparagraph (a) of Variant A, the term "properly" was intended to include the concept that the signature was created during the operational period of the certificate. Subparagraph (b) did not require proof that the certificate actually bound the public key to the signer's identity, but that it should simply purport to do so. Subparagraph (d)(iii) was included in square brackets to reflect the earlier discussion concerning the inclusion of the reference to standards, practices and usages in subparagraphs (i) and (ii).

135. A concern was expressed that the use of the word "properly" in paragraph (1)(a) of the proposal was not sufficiently clear to ensure that verification ought to occur during the operational period of the certificate. The Secretariat was requested to insert appropriate language to reflect that concern.

136. After discussion, the Working Group agreed that Variants A and B above should be reflected by the Secretariat in the revised version of the Uniform Rules to be prepared for future discussion.

137. Having completed its review of Chapter II and prior to engaging into consideration of Chapter III of the Uniform Rules, the Working Group was invited by one delegation to reconsider the purpose of the Uniform Rules. It was stated that the purpose of the Uniform Rules should be to lay down some very basic principles of law in order to create a harmonized international common platform. In view of the fact that an instrument of the international character of the Uniform Rules could not be expected to be open to frequent revision, the Uniform Rules should not be aimed at creating standards and detailed rules as to digital signatures. Such detailed regulation would not be flexible enough to adapt to the rapidly developing techniques of electronic commerce. While it was appropriate for UNCITRAL to codify certain usages and practices of international trade, it should be borne in mind, when preparing the Uniform Rules, that such usages and practices did not currently exist with respect to electronic signatures, and that it would be illusory to attempt to deal in the Uniform Rules with the wide range of technical and commercial issues that might arise in connection with emerging digital signature practice. Such issues might be better dealt with by bodies such as ISO or the ICC. The scope of the Uniform Rules should be refocused to concentrate on the preparation of the basic legal framework within which all electronic signatures could be expected to develop. To that effect, the Uniform Rules might avoid any distinction between various levels of signatures (e.g., the distinction between ordinary electronic signatures and [enhanced] electronic signatures), and be restructured in three parts as follows: (a) an introduction acknowledging the principle of party autonomy; (b) a set of rules dealing with the relationship between parties communicating with each other (based on the presumptions and liability provisions currently contained in the Uniform Rules); and (c) a set of provisions dealing with the liability of service providers that undertake to assist in the identification of parties in an electronic environment (also based on the liability provisions in the Uniform Rules). The Uniform Rules should not be concerned with certification authorities or other identification service providers, except to the extent necessary to provide basic guidance as to how such entities should perform the identification function. The Uniform Rules should avoid referring to the technical context (e.g., use of encryption techniques, reliance on a public-key infrastructure (PKI), signature dynamics or other biometric

device). Instead, the Uniform Rules should provide a very general rule to the effect that identification service providers should be liable to persons who relied on the identification to the extent that such reliance was reasonable.

138. Support was expressed in favour of the idea that the Uniform Rules might need to be somewhat simplified and that they should continue focusing on provisions of general applicability in a media-neutral framework. Nevertheless, it was generally felt that the overall structure of the Uniform Rules was appropriate and did not need to be reconsidered at the current stage. In particular, the distinction between various levels of electronic signatures was adequate. It was pointed out that, as currently drafted, the Uniform Rules already reflected the intent to deal with the complex reality of electronic authentication through simple and general provisions. It was generally felt that the approach on which the Uniform Rules were based should be pursued further.

Chapter III. Certification authorities and related issues

Article 10. Undertaking upon issuance of certificate

139. The text of draft article 10 as considered by the Working Group was as follows:

"(1) By issuing a certificate, the certification authority undertakes [to any person who reasonably relies on the certificate] that:

(a) the certification authority has complied with all applicable requirements of [these Rules];

(b) all information in the certificate is accurate as of the date it was issued, [unless the certification authority has stated in the certificate that the accuracy of specified information is not confirmed];

(c) to the certification authority's knowledge, there are no known, material facts omitted from the certificate which would adversely affect the reliability of the information in the certificate; and

[(d) that if the certification authority has published a certification practice statement, the certificate has been issued by the certification authority in accordance with that certification practice statement.]

"(2) By issuing a[n] [enhanced][secure] certificate, the certification authority makes the following additional undertakings in respect of the [signer][subject] identified in the certificate [to any person who reasonably relies on the certificate]:

(a) that the public key and private key of the [signer][subject] identified in the certificate constitute a functioning key pair; and

(b) that at the time of issuing the certificate, the private key is:

(i) that of the [signer][subject] identified in the certificate; and

(ii) corresponds to the public key listed in the certificate."

Paragraph (1)

140. Various views were expressed as to the need for, and the scope of, paragraph (1) of draft article 10. One view was that paragraph (1) (and possibly draft article 10 in its entirety) should be deleted, as it was unnecessary and went into too much detail. It was stated that, in particular, the standard of care contained in paragraph (1) with respect to all certificates was unnecessarily complex and could be summarized as a duty placed on the certification authority to act reasonably and in good faith. Thus, paragraph (1) merely stated the obvious and could be either deleted or reflected in other provisions of the Uniform Rules. It was stated in reply that, irrespective of its content and location, the provision of a standard of conduct was necessary as a logical step to allow the operation of the provisions of the Uniform Rules dealing with the liability of the certification authority. It was pointed out that the relationship between draft article 10 and draft articles 11 and 12 might need to be clarified to the effect of ensuring that failure to comply with the requirements of draft article 10 would entail liability of the certification authority. The suggestion was made that the contents of draft article 10 could be merged with draft article 12. In the context of that discussion, a further suggestion was that, alongside provisions dealing with the liability of certification authorities, the Uniform Rules might need to provide more detailed guidance as to the standard of care to be met by the relying parties. Another suggestion was that the standard of care for both certification authorities and relying parties might need to be reformulated on the basis of an obligation to act reasonably.

141. Another view was that specific elements listed under paragraph (1) were necessary with respect to all types of certificates. Paragraph (1) should thus be retained, subject to the possible deletion of subparagraphs (b) and (d), the subject matter of which could be dealt with through party autonomy. As a matter of drafting, it was suggested that, should the Uniform Rules contain requirements for all certificates, these should be made subject to international practice and established usage. Another suggestion was that the words "by issuing a certificate" should be revised in order to make it clear that the standard of conduct contained in the provision covered both the "issuing" of the certificate to its client by the certification authority and the "disclosing" of information with respect to the certificate to any relying party by the certification authority. In the context of that discussion, it was realized that the question of whether the signer or subject of a certificate was to be considered as a relying party was still unresolved. With respect to subparagraph (c), the view was expressed that the provision might need to spell out more clearly the facts which should not be omitted from the certificate. Alternatively, it was suggested that the liability of the issuer of the certificate should be limited to guaranteeing the reliability of the information relevant to the purpose for which the certificate was issued, to the exclusion of other information that might be contained in the certificate. To that effect, it was suggested that the words "for its intended use" should be inserted at the end of subparagraph (c).

142. A widely held view was that the scope of draft article 10 should be limited to cover only a limited range of certificates, and possibly only those certificates that were issued for the purposes of [enhanced] electronic signatures. It was stated that prescribing a mandatory standard of conduct for all certificates might not be appropriate in view of the numerous types (and uses) of certificates that might develop beyond those needed for enhanced electronic signatures and beyond the scope of the

Uniform Rules. It was suggested that the contents of paragraph (2) might need to be reconsidered to include in the opening words a general reference to the obligation of the certification authority to act reasonably.

Paragraph (2)

143. As a matter of drafting, it was suggested that subparagraph (b)(i) should read along the lines of "corresponds to the [signer][subject] identified in the certificate". Such a formulation would avoid the certification authority becoming inadvertently involved in issues regarding ownership of the key.

144. After discussion, the Working Group decided to postpone its decision on draft article 10 until it had completed its review of draft article 12. It was agreed that, for continuation of the discussion at a future session, the Secretariat should prepare a revised version of draft article 10, limited in scope as suggested above.

Article 11. Contractual liability

145. The text of draft article 11 as considered by the Working Group was as follows:

"*Variant A*

"(1) As between a certification authority issuing a certificate and the holder of that certificate [or any other relying party having a contractual relationship with the certification authority], the rights and obligations of the parties [and any limitation thereon] are determined by their agreement [subject to applicable law].

"[(2) Subject to article 10, a certification authority may, by agreement, exempt itself from liability for any loss [resulting from reliance on the certificate][due to defects in the information listed in the certificate, technical breakdowns or similar circumstances. However, the clause which limits or excludes the liability of the certification authority may not be invoked if exclusion or limitation of contractual liability would be grossly unfair, having regard to the purpose of the contract].]

"[(3) The certification authority is not entitled to limit its liability if it is proved that the loss resulted from the act or omission of the certification authority done with intent to cause damage or recklessly and with knowledge that damage would probably result.]

"*Variant B*

"In accordance with applicable law, the rights and obligations of a certification authority, of a [signer][subject] identified in a certificate, and of any other party shall be governed by the agreement or agreements entered into by those parties to the extent that the agreement or agreements deal with those rights and obligations and any limitations thereon.

"*Variant C*

"Where agreements are entered into by a certification authority, a [signer][subject] identified in a certificate, or any other party, the rights and obligations of those parties and any limitation thereon which are dealt with in the agreements shall be governed by the agreements in accordance with and to the extent permitted by applicable law."

General remarks

146. At the outset of the discussion, doubt was expressed as to the need for an article on contractual liability in the Uniform Rules. With specific reference to draft article 11, it was pointed out that paragraph (1) of Variant A, as well as Variant B and Variant C, referred simply to the application of domestic law, a result which would be achieved without the inclusion of a provision such as draft article 11 in the Uniform Rules. These provisions were characterized as "place holders" which simply reminded readers of the Uniform Rules that, in respect of issues of contractual liability, reference should be made to applicable law. The provisions did not attempt to establish any substantive rule or impose obligations in respect of that issue. It was also pointed out that paragraphs (2) and (3) of Variant A could not be characterized in this way and did provide substantive rules on issues of unfairness and wilful misconduct. These issues, however, were generally contentious, both domestically and internationally, as they touched upon consumer protection concerns.

147. A contrary view was that draft article 11 was of use as an introduction to draft article 12. In dealing with rules of liability other than contractual liability, draft article 12 did not provide for party autonomy or otherwise for limitation of liability by contract. In order to clarify that the Uniform Rules were not intended to exclude the possibility of parties agreeing to limit liability in their contract, it was suggested that it might be necessary to include a provision along the lines of draft article 11.

148. Another view was that, since the purpose of UNCITRAL was to harmonize and unify the rules of international trade law, it was important to seek agreement on substantive principles of liability for inclusion in the Uniform Rules. In the same context, it was pointed out that some legal systems might not recognize variation of liability by agreement, and that leaving the issue to be resolved according to domestic law therefore might not serve the interests of facilitating electronic commerce.

149. The prevailing view was that a provision along the lines of draft article 11 should be maintained in the Uniform Rules. The discussion focused on Variants A, B and C of draft article 11. A concern which applied to each variant was the use of the phrase "subject to applicable law". One view was that in legal systems that did not recognize the right of parties to vary liability by agreement, the inclusion of the words "subject to applicable law" would result in an excessively narrow application of the Uniform Rules. Conversely, deletion of those words would result in an unlimited ability to limit or exclude liability. For those reasons, it was suggested that the Working Group should carefully consider the use of those words in draft article 11. A proposal was made that contractual liability, to the extent that a provision was required, could be dealt with in the context of article 12, with the inclusion of a provision dealing with party autonomy.

Variant A

150. Variant A was widely supported, subject to general concerns expressed as to the meaning, in particular, of paragraph (2).

Paragraph (1)

151. One concern expressed in respect of paragraph (1) was that it was limited in scope to specific relationships between specified parties to a particular contract, rather than including all contracting parties. Subject to that concern, the substance of paragraph (1) was found to be generally acceptable and it was agreed that it could be adopted as the basis of further discussion.

Paragraph (2)

152. The view was expressed that, by providing a rule on grossly unfair conduct, paragraph (2) raised an issue that might be difficult to understand in the context of a number of legal systems. The Working Group was reminded that paragraph (2) was inspired by the UNIDROIT Principles on International Commercial Contracts (Article 7.1.6) as an attempt to provide a uniform standard for assessing the general acceptability of exemption clauses. The reference to the limitation or exemption of liability being "grossly unfair" suggested a flexible approach to exemption clauses, with the aim of promoting a broader recognition of limitation and exemption clauses than would otherwise be the case if the Uniform Rules were to refer merely to the law applicable outside the Uniform Rules (A/CN.9/WG.IV/WP.73, para. 64). While some support was expressed in favour of including the standard in the terms developed by UNIDROIT, which was known and understood in a number of legal systems, a number of proposals were made to improve the drafting and more clearly reflect the principle at issue. One proposal was that language that described the principle should be substituted for the words "grossly unfair". Another proposal was that the principle should be interpreted in the Uniform Rules in the same way as the UNIDROIT provision and explanatory material should be included in a Guide to Enactment. The Secretariat was requested to consider the redrafting of paragraph (2) to reflect the proposals made in respect of the standard of "grossly unfair" limitations and exclusions.

153. Another concern related to the use of the words "Subject to article 10" at the beginning of paragraph (2). It was pointed out that, since the Working Group had not reached agreement on draft article 10, it was difficult to understand what the use of those words in paragraph (2) of draft article 11 would mean. It was agreed that those words should be placed in square brackets until article 10 could be further discussed.

154. With respect to the words in square brackets in paragraph (2), there was general support for retaining the words "resulting from reliance on the certificate" without square brackets; and for deleting the words "due to defects in the information listed in the certificate, technical breakdowns or similar circumstances". There was also general agreement that the last sentence of paragraph (2) should be retained, with amendments as follows: "However, the clause which limits or excludes the liability of the certification authority may not be invoked *to the extent that* exclusion or limitation of contractual liability would be grossly unfair, having regard to the purpose of the contract *and other relevant circumstances.*" Inclusion of the words "and other relevant circumstances" was proposed on the basis that assessment of what constituted a grossly unfair limitation or exclusion would always have to be considered by reference to all of the surrounding circumstances, not simply to the contract which contained such limitation or exclusion.

155. The Working Group decided that paragraphs (1) and (2) of Variant A should be retained, subject to revision to reflect the above-mentioned suggested changes.

Paragraph (3)

156. The proposal was made that paragraph (3) could be deleted on the basis that the standard of intent to cause harm, or wilful or reckless conduct would be covered by paragraph (2). That proposal was generally accepted.

Variants B and C

157. Some support was expressed in favour of retaining Variant C as a possible alternative to Variant A. It was stated that, since Variant C was based on a mere reference to applicable law, it would not run the risk of conflicting with any applicable rule of contractual liability. After discussion, it was generally felt that, for the above-mentioned reasons, Variant A should be preferred. No support was expressed in favour of Variant B. After discussion, the Working Group decided that both Variants B and C should be deleted.

Article 12. Liability of the certification authority to parties relying on certificates

158. The text of draft article 12 as considered by the Working Group was as follows:

"(1) Subject to paragraph (2), where a certification authority issues a certificate, it is liable to any person who reasonably relies on that certificate for:

(a) errors in the certificate, unless the certification authority proves that it or its agents have taken [all reasonable] [commercially reasonable] measures [that were appropriate for the purpose for which the certificate was issued, in the light of all circumstances] to avoid errors in the certificate;

(b) failure to register revocation of the certificate, unless the certification authority proves that it or its agents have taken [all reasonable] [commercially reasonable] measures [that were appropriate for the purpose for which the certificate was issued, in the light of all circumstances] to register the revocation promptly upon receipt of notice of the revocation[; and

(c) the consequences of not following:

(i) any procedure set forth in the certification practice statement published by the certification authority; or

(ii) any procedure set forth in applicable law].

"(2) Reliance on a certificate is not reasonable to the extent that it is contrary to the information contained [or incorporated by reference] in the certificate [or in a revocation list] [or in the revocation information]. [Reliance is not reasonable, in particular, if:

(a) it is contrary to the purpose for which the certificate was issued;

(b) it exceeds the value for which the certificate is valid; or

(c) [...].]"

General remarks

159. While the substance of draft article 12 was found to be generally acceptable, some delegations expressed the view that it would be preferable not to have a specific rule on the liability of a certification authority to relying parties. The Working Group agreed that draft articles 10, 11 and 12 would need to be considered together at a future meeting to ensure that obligations imposed upon certification authorities corresponded with the liability rules established by the Uniform Rules and to ensure that issues of party autonomy were properly resolved. It was also suggested that consistency of approach between the three draft articles should be ensured, particularly as to whether the focus of the provisions should be upon the accuracy of the result to be achieved or upon the procedure to be followed.

Paragraph (1)

Subparagraph (a)

160. A number of suggestions of a drafting nature were made. It was agreed that the words "all reasonable" in square brackets should be retained without brackets and that the remaining bracketed text should be deleted. It was proposed that subparagraph (a) should include a reference to "omissions" from the certificate in addition to errors, and that the reference to the requirement that the certification authority should prove that it had taken reasonable measures to avoid errors or omissions should be deleted. The following text was proposed: "(a) errors or omissions in the certificate which result from the certification authority's failure to have taken all reasonable measures to avoid errors or omission in the certificate". Another proposal was that the order of the text should be reversed to focus upon the certification authority's failure to take reasonable care and to introduce the concept of allowing the certification authority to take remedial action to correct errors or inaccuracies in the certificate. The following text was proposed: "(a) for failure to take all reasonable measures to avoid or correct errors or inaccuracies in the certificate". One concern with that proposal was that the reference to omissions would have meaning only in the context of a duty to include specified information on the certificate, where failure to do so would give rise to liability for its omission. This would be relevant in the context of draft articles 8 and 10, and would need to be aligned with those draft articles. Another concern was that the proposal to reverse the order of subparagraph (a) and delete the words relating to the certification authority's obligation to prove that it took all reasonable measures would effectively reverse the burden of proof in the subparagraph. While addition of a reference to omissions was accepted, it was generally agreed that the burden of proof should not be reversed in this way.

Subparagraph (b)

161. It was suggested that subparagraph (b) should be deleted on the ground that it was too detailed. However, it was generally agreed that deletion of subparagraph (b) would be acceptable only if the substance of the subparagraph were included in a revised and broader version of subparagraph (a). It was agreed that, pending future discussion on the alignment of draft articles 8, 10 and 12, subparagraph (b) should be retained in the Uniform Rules. As a matter of drafting, it was decided that the words "all reasonable" should be retained without brackets and that the remaining text in square brackets should be deleted.

Subparagraph (c)

162. Concern was expressed at the inclusion of a provision along the lines of subparagraph (ii) of subparagraph (c) on the basis that it could be difficult for a certification authority to know what the applicable law might be in a given instance. In support of deletion of subparagraph (c) (ii), it was stated that the reference to "any procedure" set forth in a certification practice statement or in applicable law might be too broad, since not all such procedures were aimed at protecting relying parties, and the scope of draft article 12 should be limited to the liability of certification authorities to such relying parties. It was generally agreed that subparagraph (ii) should be deleted. It was decided that subparagraph (i), which dealt with the liability of the certification authority for failure to comply with its own certification practice statement, should be retained.

Paragraph (2)

163. Suggestions were made to clarify the drafting of paragraph (2). One proposal was that subparagraph (a) should be amended as follows: "it is for a purpose contrary to the purpose for which the certificate was issued". Similarly, subparagraph (b) should be amended as follows: "it is in respect of a transaction, the value of which exceeds the value for which the certificate is valid". Another suggestion was that the text should make it clear that reliance on a certificate would not be reasonable under paragraph (2) "to the extent" that it was not founded upon either the purpose for which the certificate was issued or the value for which the certificate was valid. It was generally agreed that the drafting of paragraph (2) would need to be revised to reflect those suggestions.

Articles 13 to 15

164. For lack of sufficient time, the Working Group had only a preliminary discussion of draft articles 13, 14 and 15. The text of draft articles 13, 14 and 15 as considered by the Working Group was as follows:

Article 13. Revocation of certificate

"(1) During the operational period of a certificate, the certification authority that issued the certificate must revoke the certificate in accordance with the policies and procedures governing revocation specified in the applicable certification practice statement or, in the absence of such policies and procedures, promptly upon receiving:

(a) a request for revocation by the [signer] [subject] identified in the certificate, and confirmation that the person requesting revocation is the [rightful] [signer] [subject], or is an agent of the [signer] [subject] with authority to request the revocation;

(b) reliable evidence of the [signer's] [subject's] death if the [signer] [subject] is a natural person; or

(c) reliable evidence that the [signer] [subject] has been dissolved or has ceased to exist, if the [signer] [subject] is a corporate entity.

"(2) The [signer] [subject] in relation to a certified key pair is under an obligation to revoke, or to request revocation of, the corresponding certificate where the [signer] [subject] knows that the private key has been lost, compromised or is in danger of being misused in other respects. If the [signer] [subject] fails to revoke, or to request revocation of, the certificate in such a situation, the [signer] [subject] is liable to any person relying on a message as a result of the failure by the [signer] [subject] to undertake such revocation.

"(3) Regardless of whether the [signer] [subject] identified in the certificate consents to the revocation, the certification authority that issued a certificate must revoke the certificate promptly upon acquiring knowledge that:

(a) a material fact represented in the certificate is false;

(b) the certification authority's private key or information system was compromised in a manner affecting the reliability of the certificate; or

(c) the [signer's] [subject's] private key or information system was compromised.

"(4) Upon effecting the revocation of a certificate under paragraph (3), the certification authority must notify the [signer] [subject] and relying parties in accordance with the policies and procedures governing notice of revocation specified in the applicable certification practice statement, or in the absence of such policies and procedures, promptly notify the [signer] [subject] and promptly publish notice of the revocation if the certificate was published, and otherwise disclose the fact of revocation upon inquiry by a relying party.

"(5) [As between the [signer] [subject] and the certification authority,] the revocation is effective from the time when it is [received] [registered] by the certification authority.

"[(6) As between the certification authority and any other relying party, the revocation is effective from the time it is [registered] [published] by the certification authority.]"

Article 14. Suspension of certificate

"During the operational period of a certificate, the certification authority that issued the certificate must suspend the certificate in accordance with the policies and procedures governing suspension specified in the applicable certification practice statement or, in the absence of such policies and procedures, promptly upon receiving a request to that effect by a person whom the certification authority reasonably believes to be the [signer] [subject] identified in the certificate or a person authorized to act on behalf of that [signer] [subject]."

Article 15. Register of certificates

"(1) Certification authorities shall keep a publicly accessible electronic register of certificates issued, indicating the time when any individual certificate expires or when it was suspended or revoked.

"(2) The register shall be maintained by the certification authority.

Variant A for at least [30] [10] [5] years

Variant B for ... *[the enacting State specifies the period during which the relevant information should be maintained in the register]*

after the date of revocation or expiry of the operational period of any certificate issued by that certification authority.

Variant C in accordance with the policies and procedures specified by the

certification authority in the applicable certification practice statement."

General remarks

165. A number of concerns were expressed about the need for including draft articles 13 to 15 in the Uniform Rules. The suggestion was made that all three articles could be deleted on the grounds that: they were too specific, detailed and limited in their application; they were based on broad assumptions as to how certain models might or might not work in practice; and they were unlikely to be widely adopted. However, it was widely accepted in the Working Group that it would be premature to delete those draft articles without further discussion.

166. A number of delegations felt that draft articles 13 and 14 dealt with issues that it might be important to include in the Uniform Rules, depending upon how issues left open by the Working Group at its current session might eventually be dealt with in the Uniform Rules. The view was generally expressed that the draft articles should be simplified and possibly reduced to a single article, or incorporated with other articles in section III of chapter II. It was proposed that, as it was clear that certification authorities were needed for digital signatures, these three articles should be limited in their application to digital signatures and the Uniform Rules rearranged to reflect that limitation. A related proposal was that it would be important to examine how commercial practices with respect to signatures other than digital signatures were developing, in order to see how the structure of the Uniform Rules should be arranged.

167. As to the substance of the draft articles, the view was expressed that draft articles 13 and 14 dealt with primary obligations of a certification authority and that it was necessary to resolve what those obligations should be before issues of liability could be resolved. In respect of draft article 13, it was suggested that the article provided an opportunity to ensure that a balance was reached in the Uniform Rules between the obligations imposed on the certification authority and those applicable to the signer or subject of the certificate.

168. The view was expressed that draft article 15 raised difficult issues of data privacy and could be deleted. Another difficulty raised was that draft article 15 might be unworkable in some certification systems. In support of retention, it was pointed out that draft article 15 was related to the liability of the certification authority under draft article 12 and would need to be further considered in the context of consideration of draft article 12.

169. The Working Group agreed that draft articles 13, 14 and 15 should be retained between square brackets for future consideration. The Secretariat was requested to review the drafting to reflect the views expressed and to explore the possibility of simplifying those draft articles.

Article 16. Relations between parties relying on certificates and certification authorities

170. The text of draft article 16 as considered by the Working Group was as follows:

"[(1) A certification authority is only allowed to request such information as is necessary to identify the [signer] [subject of the certificate].

"(2) Upon request, the certification authority shall deliver information about the following:

(a) the conditions under which the certificate may be used;

(b) the conditions associated with the use of digital signatures;

(c) the costs of using the services of the certification authority;

(d) the policy or practices of the certification authority with respect to the use, storage and communication of personal information;

(e) the technical requirements of the certification authority with respect to the communication equipment to be used by parties relying on certificates;

(f) the conditions under which warnings are given to parties relying on certificates by the certification authority in case of irregularities or faults in the functioning of the communication equipment;

(g) any limitation of the liability of the certification authority;

(h) any restrictions imposed by the certification authority on the use of the certificate; and

(i) the conditions under which the [signer] [subject] is entitled to place restrictions on the use of the certificate.

"(3) The information listed in paragraph (1) shall be delivered to the [potential] [signer] [subject] before a final agreement of certification is concluded. That information may be delivered by the certification authority by way of a certification practice statement.

"(4) Subject to a [one-month] notice, the [signer] [subject] may terminate the agreement for connection to the certification authority. Such notice of termination takes effect when received by the certification authority.

"(5) Subject to a [three-month] notice, the certification authority may terminate the agreement for connection to the certification authority. Such notice of termination takes effect when received.]"

171. There was general agreement that article 16 should be deleted on the grounds that it dealt with pre-contractual matters which should be left to the parties to a certification contract to resolve as between themselves. While some of the issues covered might be useful as a statement of best practice for certification authorities, the view was expressed that such issues were inappropriate for inclusion in the Uniform Rules, but could be included in an explanatory guide.

172. One concern related to the question of certification practice statements referred to in paragraph (3). The view was expressed that certification practice statements were an important element of the relationship between certification authorities, signers and relying parties, and that all certification authorities should be placed under an obligation to issue a certification practice statement. It was agreed that the issue should be further discussed by the Working Group at a later session in the context of draft articles 10, 11 and 12.

Chapter IV. Foreign electronic signatures

Articles 17 to 19

173. For lack of sufficient time, the Working Group postponed its consideration of draft articles 17 to 19 to a future session.

III. Proposal for future work in the field of electronic commerce

174. During the current session of the Working Group, informal consultations were held with respect to the proposal for the preparation of a draft international convention on electronic transactions (see A/CN.9/WG.IV/WP.77). [4/] A delegation described the goal of the proposal. It was explained that the proposal sought to accomplish two goals: (a) to remove paper-based obstacles to electronic transactions by adopting provisions from the Model Law; and (b) to address certain electronic authentication issues (to the extent that those issues were not already covered by the current work on the draft Uniform Rules) in a manner which, while accommodating different domestic law approaches that might be adopted, would still ensure that private contractual stipulations dealing with the authentication of electronic transactions were widely recognized and enforced. It was noted that the text of the proposal had been drafted for discussion purposes and was not cast in convention language.

175. With respect to paper-based obstacles, the proposal addressed issues concerning electronic transactions generally. It would include adoption of basic elements of the Model Law: for example, a contract formed electronically should not be denied validity or enforceability on the sole ground that it had been formed electronically. That portion of the convention would also define the characteristics of a valid electronic writing and original document and support the admission of electronic evidence. It would also recognize the acceptability of electronic signatures for legal and commercial purposes. It was felt by the proponents of the convention that there was a great deal of international consensus about these provisions, although it was reported that, in the context of informal consultations, a number of delegations had expressed interest in retaining flexibility in implementing these provisions in their own laws.

176. One delegation provided an oral report to the Working Group about various additional issues that had been informally discussed between a number of delegations. It was reported that an informal view had been expressed that the possible preparation of a convention should not involve reopening discussion as to the contents of the Model Law. The proposal for a convention should rather be regarded as a suggestion for further promoting the Model Law. It was also reported that there had been some discussion about the extent to which the provisions of the Model Law should be incorporated into the proposed convention. It was further reported that a view had been expressed that the entire Model Law should be annexed to the convention. Another view that was reported was that certain provisions of the Model Law might be less appropriate in the context of a convention. One idea that was reported was the possibility of adapting the wording of the draft convention so that States parties would undertake to implement the principles contained in the appropriate provisions of the Model Law.

177. With respect to the portion of the convention dealing with electronic authentication, it was reported that a number of issues had been discussed informally. A delegation had emphasized that, in addressing electronic authentication issues, the proposed convention should preserve the freedom of countries to adopt different approaches in domestic law. The convention should also make it clear that, notwithstanding the precise nature of any statutory framework governing electronic authentication, the terms of an agreement (including closed-system agreements) between parties should be enforced to the maximum extent possible. It was reported that the view had been expressed that the need to strike a balance between wide recognition of party autonomy, on the one hand, and the willingness of States to ensure preservation of their domestic legislative and regulatory framework, on the other hand, might be one of the crucial issues to be solved.

178. Other issues had been informally discussed in connection with the rest of the provisions concerning authentication. In addition to technology and implementation neutrality, the proposed convention provided that parties should be permitted to try to prove that their transactions were valid, whether or not the authentication technology or business method they used had been specifically addressed by legislation or regulation. Finally, the proposed convention called on States to take a non-discriminatory approach to authentication mechanisms as implemented in other countries. It was reported that there had been some discussion about this provision as a principle of commercial law and its relationship to principles of international trade policy.

179. It was agreed that informal discussions might be continued with respect to the proposed convention before and during the next session of the Working Group.

* * *

Notes

[1/] Official Records of the General Assembly, Fifty-first Session, Supplement No. 17 (A/51/17), paras. 223-224.

[2/] Ibid., Fifty-second Session, Supplement No. 17 (A/52/17), paras. 249-251.

[3/] Ibid., Fifty-third Session, Supplement No. 17 (A/53/17), paras. 209-211.

[4/] For a preliminary discussion by the Commission in relation to that proposal, see Official Records of the General Assembly, Fifty-third Session, Supplement No. 17 (A/53/17), paras. 209-211.