UNITED NATIONS

A

General Assembly

Distr.
GENERAL

A/CN.9/465
23 September 1999

ORIGINAL: ENGLISH

UNITED NATIONS COMMISSION
ON INTERNATIONAL TRADE LAW
Thirty-third session
New York, 12 June-7 July 2000

REPORT OF THE WORKING GROUP ON ELECTRONIC COMMERCE
ON THE WORK OF ITS THIRTY-FIFTH SESSION
(Vienna, 6-17 September 1999)

CONTENTS

V.99-88117 (E)

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 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). 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 no firm decision as to the form and content of such work had been reached, the Working Group 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 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 (hereinafter referred to as “the Model Law”). 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).

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. 3/

8. At its thirty-second session (1999), the Commission had before it the report of the Working Group on the work of its thirty-third (July 1998) and thirty-fourth (February 1999) sessions (A/CN.9/454 and 457). The Commission expressed its appreciation for the efforts accomplished by the Working Group in its preparation of draft uniform rules on electronic signatures. While it was generally agreed that significant progress had been made at those sessions in the understanding of the legal issues of electronic signatures, it was also felt that the Working Group had been faced with difficulties in the building of a consensus as to the legislative policy on which the Uniform Rules should be based.

9. A view was expressed that the approach currently taken by the Working Group did not sufficiently reflect the business need for flexibility in the use of electronic signatures and other authentication techniques. As currently envisaged by the Working Group, the Uniform Rules placed excessive emphasis on digital signature techniques and, within the sphere of digital signatures, on a specific application involving third-party certification. Accordingly, it was suggested that work on electronic signatures by the Working Group should either be limited to the legal issues of cross-border certification or be postponed altogether until market practices were better established. A related view expressed was that, for the purposes of international trade, most of the legal issues arising from the use of electronic signatures had already been solved in the Model Law. While regulation dealing with certain uses of electronic signatures might be needed outside the scope of commercial law, the Working Group should not become involved in any such regulatory activity.

10. The widely prevailing view was that the Working Group should pursue its task on the basis of its original mandate (see above, para. 3). With respect to the need for uniform rules on electronic signatures, it was explained that, in many countries, guidance from UNCITRAL was expected by governmental and legislative authorities that were in the process of preparing legislation on electronic signature issues, including the establishment of public key infrastructures (PKI) or other projects on closely related matters (see A/CN.9/457, para. 16). As to the decision made by the Working Group to focus on PKI issues and PKI terminology, it was recalled that the interplay of relationships between three distinct types of parties (i.e., key holders, certification authorities and

relying parties) corresponded to one possible PKI model, but that other models were conceivable, e.g., where no independent certification authority was involved. One of the main benefits to be drawn from focusing on PKI issues was to facilitate the structuring of the Uniform Rules by reference to three functions (or roles) with respect to key pairs, namely, the key issuer (or subscriber) function, the certification function, and the relying function. It was generally agreed that those three functions were common to all PKI models. It was also agreed that those three functions should be dealt with irrespective of whether they were in fact served by three separate entities or whether two of those functions were served by the same person (e.g., where the certification authority was also a relying party). In addition, it was widely felt that focusing on the functions typical of PKI and not on any specific model might make it easier to develop a fully media-neutral rule at a later stage (ibid., para. 68).

11. After discussion, the Commission reaffirmed its earlier decisions as to the feasibility of preparing such uniform rules (see above, paras. 3 and 5) and expressed its confidence that more progress could be accomplished by the Working Group at its forthcoming sessions. [4/]

12. The Working Group on Electronic Commerce, which was composed of all the States members of the Commission, held its thirty-fifth session in Vienna from 6 to 17 September 1999. The session was attended by representatives of the following States members of the Working Group: Australia, Austria, Bulgaria, Cameroon, China, Colombia, Egypt, Finland, France, Germany, Honduras, Hungary, India, Iran (Islamic Republic of), Italy, Japan, Mexico, Nigeria, Romania, Singapore, Spain, Thailand, United Kingdom of Great Britain and Northern Ireland, the United States of America and Uruguay.

13. The session was attended by observers from the following States: Angola, Bahrain, Belgium, Belize, Bolivia, Canada, Costa Rica, the Czech Republic, Denmark, Georgia, Guatemala, Indonesia, Iraq, Ireland, Kuwait, Lebanon, Malaysia, Morocco, the Netherlands, New Zealand, Philippines, Poland, Portugal, the Republic of Korea, Saudi Arabia, **Slovakia,** Sweden, Switzerland, Tunisia, Turkey, Ukraine and Yemen.

14. The session was attended by observers from the following international organizations: United Nations Conference on Trade and Development (UNCTAD), United Nations Educational, Scientific and Cultural Organization (UNESCO), African Development Bank, European Commission, Organisation for Economic Cooperation and Development (OECD), Electronic Frontier Foundation Europe, European Law Student Association (ELSA) International, International Association of Ports and Harbors (IAPH), International Bar Association (IBA), International Chamber of Commerce (ICC), Internet Law and Policy Forum (ILPF), and *Union Internationale du Notariat Latin* (UINL).

15. The Working Group elected the following officers:

Chairman: Mr. Jacques GAUTHIER (Canada, elected in his personal capacity);

Rapporteur: Mr. Pinai NANAKORN (Thailand)

16. The Working Group had before it the following documents: provisional agenda (A/CN.9/WG.IV/WP.81); a note by the Secretariat containing revised draft uniform rules on electronic signatures (A/CN.9/WG.IV/WP.82).

17. 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

18. The Working Group discussed the issue of electronic signatures on the basis of the note prepared by the Secretariat (A/CN.9/WG.IV/WP.82). The deliberations and conclusions of the Working Group with respect to those issues are reflected in section 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.

II. DRAFT UNIFORM RULES ON ELECTRONIC SIGNATURES

A. GENERAL REMARKS

19. At the outset, the Working Group exchanged views on current developments in regulatory issues arising from electronic commerce, including adoption of the Model Law, electronic signatures and public key infrastructure (referred to here as "PKI") issues in the context of digital signatures. These reports, at the governmental, intergovernmental and non-governmental levels, confirmed that addressing electronic commerce legal issues was recognized as essential for the implementation of electronic commerce and removal of barriers to trade. It was reported that a number of countries had introduced recently, or were about to introduce, legislation either adopting the Model Law or addressing related electronic commerce facilitation issues. A number of those legislative proposals also dealt with electronic (or in some cases, specifically digital) signature issues. Other countries had established policy working groups, a number in close association with private sector interests, which were working on the need for legislative change to facilitate electronic commerce, actively considering adoption of the Model Law and preparing necessary legislation, working on electronic signature issues including the establishment of public key infrastructures or other projects on closely related matters.

B. CONSIDERATION OF DRAFT ARTICLES

20. It was recalled that, for lack of sufficient time at its previous session, the Working Group had been unable to discuss the principle of non-discrimination between certificates on the basis of the place at which they were issued (A/CN.9/457, para. 120). For the same reason, the issues of cross-border recognition of certificates had not been considered at previous sessions. Prior to starting with the discussion draft article 1, the Working Group thus decided to engage in an exchange of views with respect to the provisions of draft article 13.

Article 13. Recognition of foreign certificates and signatures

21. The text of draft article 13 as considered by the Working Group was as follows:

"(1) In determining whether, or the extent to which, a certificate [signature] is legally effective, no regard shall be had to the place where the certificate [signature] was issued, nor to the State in which the issuer had its place of business.

"Variant A

"(2) Certificates issued by a foreign information certifier are recognized as legally equivalent to certificates issued by information certifiers operating under ... *[the law of the enacting State]* if the practices of the foreign information certifiers provide a level of reliability at least equivalent to that required of information certifiers under ... *[the law of the enacting State]*. [Such recognition may be made through a published determination of the State or through bilateral or multilateral agreement between or among the States concerned.]

"(3) Signatures complying with the laws of another State relating to digital or other electronic signatures are recognized as legally equivalent to signatures under ... *[the law of the enacting State]* if the laws of the other State require a level of reliability at least equivalent to that required for such signatures under ... *[the law of the enacting State]*. [Such recognition may be made by a published determination of the State or through bilateral or multilateral agreement with other States.]

"(4) Notwithstanding the preceding paragraph, parties to commercial and other transactions may specify that a particular information certifier, class of information certifier or class of certificates must be used in connection with messages or signatures submitted to them.

"Variant B

"(2) Certificates issued by a foreign information certifier are recognized as legally equivalent to certificates issued by information certifiers operating under [*the law of the enacting State*] if the practices of the foreign information certifier provide a level of reliability

at least equivalent to that required of information certifiers under ... *[the law of the enacting State]*.

"[(3) The determination of equivalence described in paragraph (2) may be made by a published determination of the State or through bilateral or multilateral agreement with other States.]

"(4) In the determination of equivalence, regard shall be had to the following factors :

(a) financial and human resources, including existence of assets within jurisdiction;

(b) trustworthiness of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records;

(d) availability of information to the [signers][subjects] identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the State, an accreditation body or the certification authority regarding compliance with or existence of the foregoing;

(g) susceptibility to the jurisdiction of courts of the enacting State; and

(h) the degree of discrepancy between the law applicable to the conduct of the certification authority and the law of enacting State."

General Remarks

22. Concern was expressed as to whether draft article 13 was intended to apply to the recognition of both certificates and signatures. One view expressed was that the draft article properly applied to certificates and that any provision dealing with the legal effect of signatures was best placed in the substantive articles dealing with signatures at the beginning of the Uniform Rules. In support of this view, it was stated that it might be difficult to formulate a single rule for the recognition of signatures, given the many different functions of signatures and the differing levels of reliability that might be encountered. It was also pointed out that, while the factors set forth in paragraph (4) of Variant B might properly be considered in respect of certificates, assessing the reliability of signatures within the meaning of Variant A would require the taking into account of different factors. An opposing view was that the draft article should address recognition of both signatures and certificates, since both were important to the question of identification in the context of commercial use and the purpose of the Uniform Rules was the development of rules on the use of electronic signatures, including in cross-border international trade. After discussion, the Working Group decided that the question should be left open until the substantive articles of the Uniform Rules had been considered.

Paragraph (1)

23. While there was general support for the principle of non-discrimination set forth in paragraph (1), doubts were expressed as to whether the provision as currently drafted properly reflected this principle and whether it was appropriate to refer to the country of origin. The view was expressed that reference to the country of origin resulted in a non-discrimination provision that was too narrow, and left open the possibility that discrimination could occur on a number of other grounds, which would be undesirable. The view was also expressed that, in fact, there might be cases where the country of origin of the signature or certificate was essential to the question of recognition. It was generally felt that the above-mentioned views and concerns should be considered when redrafting paragraph (1) for continuation of the discussion at a future session.

24. It was suggested that the principle of non-discrimination might be expressed more clearly along the following lines:

> "A determination of whether, or the extent to which, a certificate [signature] is legally effective, shall not be based solely on the place where the certificate [signature] was issued, nor solely on the State in which the issuer had its place of business."

That proposal did not receive support.

25. In terms of the relationship of paragraph (1) to Variants A and B, support was expressed for the view that only paragraph (1) was required in order to address the issue of recognition of foreign signatures and certificates. It was stated that the principles reflected in Variants A and B could not be supported as they were too restrictive, too difficult to verify and too generally drafted to provide guidance on how equivalence could be established. It was pointed out that a non-discrimination rule like paragraph (1) would have the effect of encouraging parties to look at the requirements in other jurisdictions where transactions involved foreign signatures and certificates, with a view to ascertaining what evidence might be required for signatures and certificates to be legally effective and to determine what applicable law would be desirable. An opposing view was that a rule on non-discrimination was not sufficient to enable the comparison of different certificates and signatures, which would inevitably be required to facilitate the cross-border use of electronic commerce. For that purpose, a rule on how cross-border recognition could be achieved was necessary. Support was expressed for the view that what was required internationally was guidance on the criteria on which recognition could be based, such as the reliability of certificates and signatures as set forth in Variants A and B. After discussion, the prevailing view was that paragraph (1) was not sufficient for facilitating cross-border recognition of certificates and signatures.

Variant A

26. Support was expressed for the view that Variant A, by referring to reliability, addressed the essential criterion of equivalence upon which recognition could be based. A further view was that reliability should be confined to technical reliability and that requirements such as registration of an information certifier should not be considered. Some concern was expressed, however, as to what such a rule might mean in practice. It was suggested that Variant A could give rise to reverse

discrimination, for example if it resulted in a foreign information certifier not having to comply with the law of the recognizing State, provided that its practices were determined to be equivalent, on the basis of specified factors, to the practices of a domestic information certifier. A particular concern in relation to this situation was that the foreign information certifier might gain an advantage over the domestic certifier, specifically where the basis of establishing equivalence did not take into account administrative requirements such as for registration of the information certifier. While these concerns were noted by the Working Group, particularly in view of the agreement on the importance of the principle of non-discrimination, it was generally felt that these concerns could be addressed by setting the factors to be taken into account in determining equivalence. Another concern expressed in relation to the possible introduction of a test of technical reliability (particularly in relation to certificates) was the extent to which reliability of the certificate depended upon the reliability of the information certifier, and thus upon factors not strictly relevant to technical matters.

27. In connection with the possible criterion for establishing equivalence, the view was expressed that the focus in Variant A upon reliability was too narrow and that other factors such as the contractual environment created by the parties were important to a determination of equivalence. It was also pointed out that the provisions of Variant A presupposed a level of regulation of information certifiers and certificates that might not, in practice, be universal and such provisions might prove difficult to implement. The prevailing view in the Working Group was that reliability was an appropriate criterion upon which to make a determination of equivalence for the purposes of recognition of foreign information certifiers, subject to establishing certain factors to be taken into account in making that determination.

28. Wide support was also expressed for recognizing the importance of bilateral and multilateral agreements as a means of agreeing upon recognition, along the lines set forth in paragraphs (2) and (3) of Variant A.

29. There was general support for the inclusion in draft article 13 of a provision establishing ample recognition of party autonomy as a basis for cross-border recognition. It was also agreed that the freedom of the parties to agree on the use of specific certificates or signatures along the lines of paragraph (4) of Variant A should be recognized.

Variant B

30. Various views were expressed as to the need to retain the factors set out in paragraph (4) of Variant B. In support of retaining these factors, it was repeated that a basis for establishing recognition was required and that this paragraph, in combination with paragraph (1) and Variant A, provided such a basis. An opposing view was that it was inappropriate to include, in an article on cross-border recognition of certificates and signatures, requirements in respect of information certifiers not included elsewhere in the draft Uniform Rules. The suggestion was made that if the Uniform Rules were to address the operations of information certifiers and establish factors to which reference should be had in assessing the reliability of certificates issued by such information certifiers, those provisions should be located in substantive articles, such as draft article 12. In addition, it was stated that to include these factors only in provisions addressing recognition of foreign certificates and signatures might lead to discrimination and thus run counter to the principle stated in paragraph

(1). Furthermore, some concern was expressed as to the relevance of all of these factors in each case and the need to ensure that the provision was neither drafted as a mandatory provision, nor specifically limited to those factors set forth.

31. With a view to addressing some of the views and concerns that had been expressed in the discussion, a provision on recognition along the following lines was proposed:

> "(1) In determining whether, or the extent to which, a certificate is legally effective, no regard shall be had to the place where the certificate was issued, nor to the State in which the issuer had its place of business.
>
> "(2) A determination of whether, or the extent to which, a certificate is legally effective shall be determined by reference to the laws of the recognizing State or such other applicable law as the parties may agree.
>
> "(3) A certificate shall not be held legally ineffective under the laws of the recognizing State or such other applicable law as the parties shall agree solely because a registration requirement under the applicable law has not been met.
>
> "(4) If a recognizing State has entered into a bilateral or multilateral agreement with another State, a certificate issued pursuant to that agreement shall be recognized.
>
> "(5) If the parties agree to be bound by a certificate issued by a specified information certifier that certificate shall be recognized."

32. As doubts were expressed as to how this proposal could be interpreted, particularly in relation to conflicts-of-laws issues, the proposal received limited support.

33. In the context of the discussion as to which of the factors set forth in paragraph (4) of Variant B should be retained, it was pointed out that not all of the factors included might be equally relevant to a determination of reliability or what might be required to prove a certificate. In addition, the view was expressed that the cost and ease of proof of the factors required careful consideration to ensure that they did not act as a barrier to the use of certificates and electronic signatures. The Working Group took note of these views for a discussion of paragraph (4) at a later stage.

34. After discussion, the Working Group concluded that, for the purpose of future discussion: paragraph (1) should state the principle of non-discrimination with some adjustment to the drafting to ensure that the views expressed in the discussion were reflected; paragraphs (2), (3) and (4) of Variant A should be retained as setting out an appropriate rule on recognition of foreign certificates and signatures; paragraph (4) of Variant B should set out the factors to be taken into account in considering equivalence of reliability in relation to paragraphs (2) and (3) of Variant A, but this provision should be neither mandatory nor limited to the particular factors enumerated; draft article 13 should provide for the recognition of agreement between interested parties regarding the use of certain types of electronic signatures or certificates as sufficient grounds for cross-border recognition (as between those parties) of such agreed signatures or certificates; and the question of whether draft article 13 should address both certificates and signatures should be reconsidered when decisions on

the substantive articles of the draft Uniform Rules had been made.

35. The Working Group agreed that, for continuation of the discussion at a later session, an alternative draft of article 13 should be prepared, based on the view that criteria set forth with respect to signatures or certificates should apply equally to foreign and domestic signatures or certificates. For that purpose, the substance of those criteria should be set forth in draft article 12, with a reference in draft article 13 to foreign information certifiers having to comply with the criteria set forth in draft article 12 in order to obtain recognition.

Article 1. Sphere of application

36. The text of draft article 1 as considered by the Working Group was as follows:

> "These Rules apply to electronic signatures used in the context of commercial* relationships and do not override any law intended for the protection of consumers.
>
> "* The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road."

37. At the outset, it was noted that draft article 1, which reproduced a number of provisions contained in article 1 of the Model Law, was based on the working assumption that the Uniform Rules should be prepared as a separate legal instrument and not merely as a separate chapter of the Model Law (see A/CN.9/WG.IV/WP.82, para. 16). While the view was expressed that the possible adoption of the Uniform Rules as an additional part of the Model Law might need to be reconsidered at a later stage, the Working Group agreed with that working assumption. It was also agreed that, in drafting the Uniform Rules, every effort should be made to ensure consistency with both the substance and the terminology of the Model Law. In the explanatory note, or guide to enactment of the Uniform Rules, possibly to be prepared at a later stage, explanations should be provided regarding the relationship between the Uniform Rules and the Model Law. In that context, it should be indicated that the Uniform Rules could be enacted either independently or as an addition to the Model Law.

38. General support was expressed for the substance of draft article 1. As a matter of drafting, it was agreed that, in order to ensure consistency with the terminology used in article 1 of the Model Law, the words "commercial relationships" should be replaced by the words "commercial activities". It was also agreed that the words "These Rules apply to electronic signatures used ..." did not sufficiently reflect the broad scope of the Uniform Rules and should be replaced by the words "These Rules apply where electronic signatures are used ...".

39. With respect to the reference to "commercial activities", doubts were expressed as to whether it was necessary to restrict the scope of the Uniform Rules to the commercial sphere. It was pointed out that the Uniform Rules should equally apply, for example, where electronic signatures were used in the submission of statements or other documents to public administrations. It was observed that the same discussion had taken place during the preparation of the Model Law. As indicated in the Guide to Enactment of the Model Law, it had been decided that "nothing in the Model Law should prevent an enacting State from extending the scope of the Model Law to cover uses of electronic commerce outside the commercial sphere" (Guide to Enactment of the Model Law, para. 26). It was generally agreed that the same policy should apply with respect to electronic signatures. Accordingly, it was decided that wording along the lines of footnote *** to article 1 of the Model Law should be inserted in the revised version of draft article 1 to be prepared for continuation of the discussion at a future session.

40. As regards the definition of the term "commercial" a question was raised about the relevance of the wording "relationships of a commercial nature, whether contractual or not". However, it was generally felt that, while relationships of a commercial nature might be regarded as inherently contractual in certain countries, they might also be regarded as non-contractual under the laws of other countries. In addition, it was noted that the same definition of the term "commercial" had been successfully used in other UNCITRAL texts.

41. A suggestion was made that uses of electronic signatures involving consumers should be excluded from the scope of the Uniform Rules. It was recalled that the matter of consumers had been considered by the Working Group at its previous session (see A/CN.9/457, paras. 20, 56 and 70). After discussion, the Working Group reaffirmed the decision made at that session not to displace any law intended for the protection of consumers. However, under that same decision, consumers should not be excluded from the scope of the Uniform Rules since there might be cases where the Uniform Rules might prove useful to consumers.

42. After discussing draft article 1, the Working Group decided to postpone consideration of the definitions contained in draft article 2 until it had completed its review of the substantive provisions of the Uniform Rules.

Article 3. [Non-discrimination] [Technology neutrality]

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

> "[None of the provisions of these Rules shall be applied] [The provisions of these Rules shall not be applied] so as to exclude, restrict, or deprive of legal effect any method [of signature] that satisfies the requirements of *[article 7 of the UNCITRAL Model Law on Electronic Commerce*].

44. General support was expressed in the Working Group for a principle along the lines of draft article 3 which made it clear that the Uniform Rules were not intended to give a privilege or benefit to the use of certain technologies which might result in discrimination against the use of other technologies. The Working Group reaffirmed the importance of the principle of technology neutrality

upon which the Model Law was based, and which was also an essential element of the Working Group's mandate for the preparation of the Uniform Rules.

45. Some concerns were expressed as to how the rule on non-discrimination should be formulated in the Uniform Rules, and about the relationship of that principle with article 7 of the Model Law. One issue was the role of party autonomy in draft article 3. The view was expressed that any reference to article 7 of the Model Law, since article 7 was a mandatory provision and not subject to variation by agreement, would limit the ability of the parties to agree on how to conduct their transactions between themselves and, in particular, on what might constitute a signature. Suggestions were made to address this issue by deleting the reference to article 7 and ending the draft article after the word "method" or by making draft article 3 subject to the party autonomy provisions of draft article 5. Under the first suggestion, draft article 3 would be a general statement of non-discrimination. Under the second suggestion, draft article 3 could be varied by agreement pursuant to draft article 5. An opposing view was that the focus of draft article 3 was upon the actions a State might take in legislating for the recognition (or legal effect) of different forms of technology. In that context, the issue of party autonomy was not relevant. An additional observation was that, while article 7 of the Model Law provided a means of establishing a functional equivalent for requirements of law for a signature, it did not exclude methods of signature that might still have legal effect even if they did not satisfy those form requirements. For that reason also the question of party autonomy was not relevant to a consideration of draft article 3.

46. Another concern expressed about the relationship of draft article 3 to article 7 of the Model Law was that, since the Uniform Rules could be an independent or free-standing text, draft article 3 would have little meaning to those States which did not adopt the Model Law or, at least, article 7 of the Model Law. To address this difficulty, one suggestion was that draft article 3 should refer to the provisions of the law of the State (being the State which was enacting the Uniform Rules) which dealt with signatures or electronic signatures. It was pointed out that the purpose of the reference to article 7 was to go beyond recognizing signatures which were given legal effect in national law and to offer the criterion in article 7 for those States looking to adopt new law on signatures. For that purpose, the reference in draft article 3 could be either a specific reference to article 7, a reference to the criteria set forth in article 7 or a reference to draft article 6(2) of the Uniform Rules which repeated the criteria of article 7. It was pointed out that a reference to the criteria of article 7 would have the advantage of preserving those criteria in the Uniform Rules since countries which adopted the Model Law could modify or vary article 7 to lower the effect of the criteria. If the proposal to adopt a reference to national law were followed, that reference to national law would then be a reference to something other than the criteria of article 7 of the Model Law. Support was expressed in favour of both a reference to the criteria of article 7, whether by reproducing them in the draft article directly or by a reference to draft article 6(2), and a reference to applicable law.

47. A number of suggestions of a drafting nature were made. Support was expressed for the first set of opening words "None of the provisions of these Rules ...". Support was expressed in favour of both retaining and deleting the words "[of signature]" and for adding the qualification "electronic" before "signature". The Working Group agreed that this was a question of drafting which depended upon what, if any, words were used to end the sentence. A further suggestion was made to replace "deprive of legal effect" with the words "discriminate against", but this proposal did not receive

support. Support was expressed in favour of both alternatives shown in square brackets as a heading for draft article 3. A further proposal was for the heading "Equal treatment of electronic signatures". A degree of preference was expressed for a reference to the principle of technology neutrality in the title of draft article 3.

48. After discussion, the Working Group agreed: that an article along the lines of draft article 3 was very important to ensure that the principle of non-discrimination applied as between different types of signature technology, whether that technology was currently being used or technology that might be developed in the future; that there was no connection between draft articles 3 and 5 of the Uniform Rules and, therefore, no provision for variation by agreement in draft article 3 was necessary; that the opening words of draft article 3 should be "None of the provisions of these Rules ..."; that, while there was some preference for the heading of draft article 3 to be "Technology neutrality", the Secretariat might wish to consider other possible titles to reflect the views expressed by the Working Group; that the reference to article 7 of the Model Law, although intended only to be a reference to article 7 as enacted by adopting States, should be replaced by a reference to draft article 6(2) of the Uniform Rules including the criteria set out in article 7 of the Model Law (as originally proposed and set out in A/CN.9/457 at para. 55); that, as an addition to the reference to draft article 6(2), the words "or otherwise meets the requirements of applicable law" should be included for later consideration by the Working Group.

Article 4. Interpretation

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

> "(1) In the interpretation of these Uniform Rules, regard is to be had to their international origin and to the need to promote uniformity in their application and the observance of good faith in electronic commerce.
>
> "(2) Questions concerning matters governed by these Uniform Rules which are not expressly settled in them are to be settled in conformity with the general principles on which these Uniform Rules are based."

50. There was general support for article 4 as drafted, although some doubts were expressed as to the meaning of the words "in electronic commerce" in paragraph (1). It was pointed out that electronic commerce was not a defined term. Although the meaning of the term was discussed in the Guide to Enactment of the Model Law, the view was expressed that this was not sufficient and that, should a reference to good faith "in electronic commerce" be retained, the text of the Uniform Rules should make it clear what the precise scope of these words was to be. Another view was that these words might assist in defining the sphere in which the requirement of good faith was to operate, in much the same manner as adopted in other UNCITRAL texts. These included, for example, article 7 of the United Nations Convention on Contracts for the International Sale of Goods ("The Sales Convention"), which referred to good faith "in international trade", and article 5 of the United Nations Convention on Independent Guarantees and Stand-by Letters of Credit which referred to good faith "in the international practice of independent guarantees and stand-by letters of credit". After discussion, however, it was decided that the words "in electronic commerce" should be deleted.

Article 5. Variation by agreement

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

Variant A

"[By agreement, whether express or implied, parties are free to derogate from or vary any aspect of these Rules,] [Any aspect of these Rules may be derogated from or varied by agreement, whether express or implied,] except to the extent such derogation or variation would adversely affect rights of third parties.

Variant B

"(1) These Rules do not affect any right that may exist to modify by agreement any rule of law referred to in articles 6 and 7.

"(2) Any aspect of articles 9 to 12 of these Rules may be derogated from or varied by agreement, whether express or implied, except to the extent that such derogation or variation would adversely affect rights of third parties."

General Remarks

52. In relation to the general principle of party autonomy, it was stated that the only limitation that the Uniform Rules should impose upon commercial parties in respect of regulating commercial matters as between themselves and in respect of third parties, should be the limitations imposed in the laws of enacting States.

53. In respect of both Variants A and B, there was support for the deletion of the phrases dealing with the rights of third parties. It was stated that this principle, together with the principle that parties could not affect, by agreement, provisions of mandatory law, was internationally recognized as fundamental and therefore did not need to be expressed in the Uniform Rules. Another view was that the reference to the rights and obligations of third parties would fall within the more general category of an exception to party autonomy based on public policy reasons, an exception which might usefully be stated in this article. An opposing view was that issues of public policy should be left to domestic law and not addressed in the Uniform Rules.

54. The Working Group exchanged views on the heading of draft article 5 and a number of suggestions for revision were made including "Party autonomy" and "Freedom of contract". After discussion, the Working Group requested the Secretariat to take these views into consideration when revising draft article 5.

Variant A

55. Various views were expressed in support of Variant A. One view was that, because the rule

set out in Variant B specified which articles of the Uniform Rules were to be regarded as mandatory rules, it expressed the principle of party autonomy more narrowly than the rule in Variant A. Variant B might thus have the effect of inhibiting, rather than facilitating, the development of electronic commerce. It was pointed out that an absence of regulation had greatly facilitated the development of electronic data interchange and allowed parties to develop contractual means of addressing legal issues that arose. For the same reasons, the Uniform Rules should not seek to create mandatory provisions such as those set forth in Variant B. Another view was that, in a commercial context, parties should have complete freedom to agree on how their relationships and transactions should be conducted, including on what they might agree to treat as a signature. It was acknowledged that, while commercial parties could certainly conclude such agreements "as between themselves", there was some doubt as to how such an agreement could be legally effective where form requirements applied to the commercial context.

56. It was suggested, however, that the decision on whether certain articles of the Uniform Rules should be mandatory could be taken at a later stage of the Working Group's deliberations and, if necessary, included in the relevant articles, rather than diluting the article on party autonomy. To reflect this suggestion, it was proposed that the opening words of Variant A could be amended to read "Unless these Rules provide otherwise ...".

57. As a matter of drafting, it was suggested that the reference to "express or implied" agreement should be deleted and that the word "modify" should be substituted for "derogate". In view of the subsequent decisions of the Working Group these suggested changes were not pursued.

Variant B

58. Support was expressed in favour of Variant B. It was pointed out that draft paragraphs (1) and (2) were closely modelled upon article 4 of the Model Law. Accordingly, draft articles 6 and 7 of the Uniform Rules, like articles 7 and 8 of the Model Law upon which they were based, would be mandatory provisions. Similarly, in accordance with article 4 paragraph (2), draft paragraph (1) of Variant B preserved the right of parties to modify mandatory provisions where national law would allow them to do so. Draft articles 9 to 12 of the Uniform Rules, in comparison, were provisions from which parties could freely derogate, like those provisions of chapter III of the Model Law.

59. With a view to addressing some of the views and concerns that had been expressed in relation to both Variants, a provision on party autonomy along the following lines was proposed:

> "These Rules may be derogated from or varied by agreement unless:
> (a) these Rules provide otherwise;
> (b) the law of the enacting State provides otherwise."

60. This proposal was generally supported. Some concern was expressed, however, as to paragraph (b) on the basis that it was a very broad provision which left it open to States to impose restrictive regulations on the use of electronic signatures and did not encourage adoption of a standard such as article 7 of the Model Law. It was noted by the Working Group that, while it would be impossible to prevent a State from adopting such a position, the intention that restrictive provisions should be exceptional, rather than general, could be mentioned in a guide or explanatory

report to the Uniform Rules. A further proposal was that paragraph (b) should be placed in square brackets, pending further consideration by the Working Group. After discussion, the Working Group adopted that proposal.

61. A suggestion of a drafting nature was that the provision should refer to derogation or variation of "the effect" of the Rules, rather than from the Rules themselves. It was agreed that, because this type of provision was found in a number of international instruments (e.g., the Sales Convention), the common formulation should be followed.

Article 6. [Compliance with requirements for signature][Presumption of signing]

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

"Variant A

"(1) Where, in relation to a data message, an enhanced electronic signature is used, it is presumed that the data message is signed.

"(2) Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used which 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.

"[(3) Where the law requires a signature of a person, that requirement is met in relation to a data message if an enhanced electronic signature is used.]

"(4) Paragraphs (2) and (3) apply whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

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

"Variant B

"(1) Where, in relation to a data message, [a method] [an electronic signature] is used which:

(a) is unique to the signature holder [for the purpose for][within the context in] which it is used;

[(b) can be used to objectively identify the signature holder in relation to the data message; and]

(c) was created and affixed to the data message by the signature holder or using a means under the sole control of the signature holder [and not by any other person];

it is presumed that the data message is signed.

"(2) Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used which 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.

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

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

Purpose of draft article 6

63. There was general agreement that the main purpose of draft article 6 should be to establish a degree of certainty as to the legal effects that would flow from the use of electronic signatures. As to what those legal effects might be, the discussion developed in various directions, with constant reference being made to the question of fulfilment of the signature requirements referred to in article 7 of the Model Law.

Types of electronic signatures

64. A view was expressed that (either through a reference to the notion of "enhanced electronic signature" or through a direct mention of criteria for establishing the technical reliability of a given signature technique) a dual purpose of draft article 6 should be to establish: (1) that legal effects would result from the application of those electronic signature techniques that were recognized as reliable; and (2), conversely, that no such legal effects would flow from the use of techniques of a lesser reliability. It was generally felt, however, that a more subtle distinction might need to be drawn between the various possible electronic signature techniques, since the Uniform Rules should avoid discriminating against any form of electronic signature, unsophisticated and insecure though it might appear in given circumstances. Therefore, any electronic signature technique applied for the purpose of signing a data message under article 7(1)(a) of the Model Law would be likely to produce legal effects, provided that it was sufficiently reliable in the light of all the circumstances, including any agreement between the parties. However, the determination of what constituted a reliable method of signature in the light of the circumstances could only be made under article 7 of the Model Law by a court or other trier of fact intervening *ex post*, possibly long after the electronic signature had been used. In contrast, the benefit expected from the Uniform Rules in favour of certain techniques, which were recognized as particularly reliable, irrespective of the circumstance in which they were used, was to create certainty (through either a presumption or a substantive rule), at or before the time any such technique of electronic signature was used (*ex ante*), that it would result in legal effects equivalent to those of a handwritten signature.

65. A question was raised as to whether any legal effect should result from uses of electronic signature techniques that would not fulfil all the functions described in article 7(1)(a) of the Model Law, namely those uses of electronic signatures that would not be made with the intent of indicating any approval of the information contained in the data message. It was generally felt that, by

appending a signature (whether handwritten or electronic) to certain information, the alleged signer should be presumed to have approved the linking of its identity with that information. Whether that linking should produce legal effects (contractual or other) would result from the nature of the information being signed, and from any other circumstances, to be assessed according to the law applicable outside the Uniform Rules. In that context, the Working Group agreed that the Uniform Rules should not interfere with the general law of contracts or obligations.

66. It was noted that Variants A and B, while intended to produce the same result in practice, differed as to whether they relied or not on the notion of "enhanced electronic signature". Support was expressed in favour of retaining the notion of enhanced electronic signature, which was described as particularly apt to provide certainty with respect to the use of a certain type of electronic signatures, namely digital signatures implemented through public-key infrastructure (PKI). In response, it was pointed out that the notion of "enhanced electronic signature" made the structure of the Uniform Rules unnecessarily complex. In addition, the notion of "enhanced electronic signature" would lend itself to misinterpretation by suggesting that various layers of technical reliability might correspond to an equally diversified range of legal effects. Widespread concern was expressed that an enhanced electronic signature would be considered as if it were a distinct legal concept, rather than just a description of a collection of technical criteria, the use of which made a method of signing particularly reliable. While postponing its final decision as to whether the Uniform Rules would rely on the notion of "enhanced electronic signature", the Working Group generally agreed that, in preparing a revised draft of the Uniform Rules for continuation of the discussion at a future session, it would be useful to introduce a version of the draft articles that did not rely on that notion.

Relationship with article 7 of the Model Law

67. A view was expressed that the reference to article 7 of the Model Law in paragraph (2) of draft article 6 (which was also useful as a reminder of the conceptual origin of the Uniform Rules) was to be interpreted as limiting the scope of the Uniform Rules to situations where an electronic signature was used to meet a mandatory requirement of law that certain documents had to be signed for validity purposes. Under that view, since the law contained very few such requirements with respect to documents used for commercial transactions, the scope of the Uniform Rules was very narrow. It was generally agreed, in response, that such interpretation of draft article 6 (and of article 7 of the Model Law) was inconsistent with the interpretation of the words "the law" adopted by the Commission in paragraph 68 of the Guide to Enactment of the Model Law, under which "the words 'the law' are to be understood as encompassing not only statutory or regulatory law but also judicially-created law and other procedural law". While paragraph (1) of both Variant A and Variant B contained no reference to any "requirement of law", and paragraph (2) mirrored the wording of article 7 of the Model Law, it was widely understood that there was no difference in scope between the two paragraphs, and that scope was particularly broad since most documents used in the context of commercial transactions were likely to be faced, in practice, with the requirements of the law of evidence regarding proof in writing.

Legal effect: presumption or substantive rule

68. Various views were expressed as to precisely what legal effect should result from the use of

a reliable electronic signature. One view was that the question whether the document should be regarded as "signed" should be distinguished from the question whether it should be regarded as signed by any specific person. Another view was that establishing a presumption that the information was "signed" would be inappropriate since, under the laws of a number of countries, "signature" indicated the intent of the signer to be bound, for example in a contractual environment. Presuming intent might place an excessive burden on the alleged signer, and might interfere with the existing law dealing with the formation of contracts or obligations. Accordingly, it was suggested that, instead of establishing a presumption that the data message was "signed", the Uniform Rules should merely establish the presumption of a link between the electronic signature and the alleged signer, together with a presumption as to the reliability of the signature technique being used. It was also suggested that any additional conclusion regarding the effect of the electronic signature with respect to the substance of the data message should be left to other applicable law. Some support was expressed in favour of those views.

69. A related view was that the approach taken in draft article 6 in combination with the definition of "electronic signature" in draft article 2 was acceptable. Under that approach, the use of a reliable electronic signature should result in the data message being "signed" by the holder of the signature device, on the assumption that the consequences of such a "signature", in particular as to any intent of the alleged signer regarding the information contained in the data message, would be dealt with by the law applicable outside the Uniform Rules.

70. The Working Group generally agreed that the focus of draft article 6 should be on replicating in an electronic environment the legal consequences of the use of a handwritten signature. Based on the view that the use of the verb "signed" was, in some countries, inappropriate in the context of data messages, it was suggested that the functional equivalent of the word should be assumed in the discussion, except where the context indicated a handwritten signature. The Working Group proceeded with a discussion as to whether the legal effects of the use of a reliable electronic signature device should be expressed by way of a presumption or through a substantive rule.

71. As an alternative to establishing a presumption, which might be regarded in certain legal systems as narrowly restricted to the realm of civil procedure, it was suggested that an operative provision was needed to recognize legal effects to the use of electronic signatures. It was suggested that a rule along the following lines should be adopted, based on the text of paragraph (1) of Variant A: "Where, in relation to a data message, an electronic signature is used, that electronic signature is given the same legal effect [as there would be if the information in the data message had been in writing and signed][as is given to a handwritten signature under applicable law]". It was pointed out that wording along the same lines could be prepared based on paragraph (1) of Variant B. Some support was expressed in favour of that suggestion. While a view was expressed that the principle embodied in the suggested text should apply to all electronic signatures, it was pointed out by a number of delegations that the operative provision should be limited in scope to cover only those electronic signatures which were described as "enhanced" under draft article 2.

72. A widely shared view, however, was that draft article 6 was appropriately drafted in the form of a rebuttable presumption. Support was expressed in favour of the view that a rebuttable presumption of "signature" by the alleged signer was the most appropriate effect that could result from the use of a reliable signature technique. The effect of such a presumption would be to place

on the alleged signer the burden of proving that the electronic signature should not be attributed to that person or that it should not be treated as binding. In that context, while concern was expressed as to how the alleged signer would rebut the presumption, for example in the context of contract formation, it was recalled that the Uniform Rules merely established the equivalence between certain electronic and handwritten signatures, and did not intend to interfere with the general law of contracts or obligations.

73. The view was expressed that, irrespective of whether draft article 6 established a presumption that the data was "signed" or a mere presumption that the electronic signature was technically reliable and linked to a given message, the burden of rebutting such presumptions might be too onerous in the context of consumer transactions, which might need to be excluded from the scope of draft article 6.

74. With respect to the nature of the presumption to be established, the view was expressed that, while the substance of the suggestion for a substantive rule (see above, para. 71) should be reflected in draft article 6, there was a need for establishing a presumption, which should be more reflective of the evidentiary context in which it would be used. It was pointed out that creating a presumption purely for evidentiary purposes might be less ambitious but more feasible than establishing general criteria of reliability under which data messages should be presumed to be "signed". On the one hand, technical reliability was a rapidly evolving reality. Technical criteria might thus prove extremely difficult to express in sufficiently neutral terms to stand the test of time. On the other hand, changing practices in the use of electronic signatures required a flexible criterion, such as embodied in article 7(1)(b) of the Model Law, more than an all-purpose test of reliability along the lines of draft article 6(1). With a view to illustrating the suggested approach, the following text was proposed for draft article 6:

"Article 6. Presumptions affecting electronic signatures

"(1) The legal consequences of the use of a signature shall apply equally to the use of electronic signatures.

"(2) Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used which 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.

"(3) If the requirements of paragraph (4) are met, a judicial or administrative tribunal is entitled to presume that an electronic signature proves one or more of the following matters:

(a) that the electronic signature meets the standard of reliability set out in paragraph (2);

(b) the identity of the alleged signer;

(c) that the alleged signer approved the data message to which the electronic signature relates.

"(4) The presumptions in paragraph (3) shall apply if, and only if

(a) a notice is served* on the alleged signer by the person relying on the electronic signature asserting that a specified electronic signature proves one or more of the matters set out in subparagraphs (a) to (c) of paragraph (3); and

(b) the alleged signer fails to serve* a notice which denies one or more of the matters set out in the notice under subparagraph (a) and provides the grounds of that objection.

"* Requirements as to service (including timing) are to be dealt with under the applicable law. Some States may wish to add provisions to deal with those matters."

75. Support was expressed in favour of that proposal, particularly on the grounds that it would be applicable to consumer transactions, since rebuttal of the presumption could result from a simple notice of objection. However, it was generally felt, particularly with respect to proposed new paragraphs (3) and (4) that the suggested wording might be overly geared to evidentiary practices in judicial proceedings as they were known in certain legal systems, and might be difficult to rephrase in sufficiently neutral terms to adapt to all legal systems. In general, it was found that the proposed text of paragraph (4) went too deeply into harmonizing the rules of civil procedure, an area which did not easily lend itself to treatment by international instruments. With respect to paragraphs (1) and (2), the view was expressed that the interplay of the two provisions might need to be reconsidered to avoid a possible misinterpretation under which unqualified electronic signatures would be treated more favourably than those electronic signatures that met criteria of reliability.

76. In response to the objection expressed with respect to the proposed text of new paragraphs (3) and (4), an alternative to those paragraphs was proposed in the form of a single paragraph (3) as follows:

"[(3) In the absence of proof to the contrary, reliance on an electronic signature shall be presumed to prove:

(a) that the electronic signature meets the standard of reliability set out in paragraph (2);

(b) the identity of the alleged signer; and

(c) that the alleged signer approved the data message to which the electronic signature relates.]"

77. It was felt that additional efforts should be made by the Working Group at a future session to determine whether an acceptable rule of procedure could be drafted, to the effect that, where the alleged signer intended to dispute its signature, it should promptly advise the relying party, and disclose the reasonable grounds for such a dispute. In that connection, it was suggested that inspiration might be drawn from article 16 of the UNCITRAL Model Law on Cross-border Insolvency. In response to that suggestion, however, it was pointed out that, while limited

harmonization of civil procedure was conceivable in the narrow context of cross-border insolvency, it might be more difficult to achieve with respect to the broader issues of electronic signatures,

Criteria of reliability of an electronic signature

78. In the context of the above discussion regarding the formulation of draft article 6 as a rebuttable presumption, particular attention was given to the criteria against which the technical reliability of the signature technique should be measured. With a view to expressing more objectively the criteria set forth in paragraph (1) of Variant B, the following proposal was made for draft article 6:

"Article 6. Compliance with legal requirements for signature

"(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if a method is used which is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

"(2) It is presumed that a method is reliable for the purpose of satisfying the requirement referred to in paragraph (1) if that method ensures that:

(a) the data used for the creation of an electronic signature are unique to the holder of the signature creation device within the context in which the device is used;

(b) the holder of the signature creation device has sole control of that device;

(c) the electronic signature is linked to the data message to which it relates [in a manner which guarantees the integrity of the message];

(d) the holder of the signature creation device is objectively identified within the context [in which the device is used][of the data message]."

79. Considerable support was expressed in favour of expressing draft article 6 as a presumption of technical reliability. Doubts were expressed, however, as to whether it was necessary to establish detailed technical criteria to measure such reliability. The view was expressed that, in most practical circumstances, reliability would be pre-determined, either by agreement between the parties, or through reliance on an existing public or private PKI. While there was widespread agreement with that view, it was also felt that it was desirable to offer default criteria for assessing the technical reliability of electronic signature techniques, for consideration mainly by countries that did not already have established PKI.

80. With respect to the individual criteria proposed, it was pointed out that the Uniform Rules or any guide to enactment or explanatory note that might be prepared at a later stage would need to

clarify the following issues: (1) provisions under which the signature creation device should be under the sole control of the corresponding device holder should not interfere with the law of agency or with the operation of the device holder through an electronic agent; and (2) the "objective identification" of the device holder should not imply that, in all cases, an individual person should be identified by name, since the notion of "identity" should be interpreted as referring possibly to significant characteristics of the device holder, such as position or authority, either in combination with a name or without reference to a name (see A/CN.9/WG.IV/WP.82, para. 29). In addition, questions were raised as to whether the reference to the integrity of the message should be regarded as appropriate in the context of establishing whether a data message was "signed", since the verification of "integrity" was not inherently part of any signature process (whether electronic or handwritten) and might seem more pertinent in the context of assessing whether that message should be regarded as "original".

81. More generally with respect to criteria for assessing the reliability of a signing method, the view was expressed that any such criteria should be drafted so as to support the presumption, and should not amount to proving independently the conclusion which was to be presumed. It was suggested that the criteria for recognition of foreign certificates in draft article 13, and perhaps the responsibilities of an information certifier in draft article 12, could furnish useful additional criteria against which to measure reliability. It was further suggested that the criteria in Variant B gave little or no help in deciding whether a signing method was reliable. Most if not all of them would apply to any method at all. It was stated that, in establishing criteria, the principal objective should be to determine the degree of confidence that could be derived from satisfying such criteria. Even digital signatures supported by certificates offered a range of distinct levels of assurance. It was pointed out that the Working Group had not yet agreed on the level of assurance needed for the proposed presumption.

82. After discussion, the Working Group agreed that the discussion of draft article 6 should be resumed at a future session. The Secretariat was requested to prepare a revised draft of article 6 to reflect, as possible variants, the above-mentioned views and concerns. In preparing those variants, the Secretariat should consider a version of draft article 6 that would combine the approaches suggested in paragraphs 74, 76 and 78 above, together with paragraphs (3) and (4) of Variant B.

Article 7. [Presumption of original]

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

> "(1) Where, in relation to a data message, [an enhanced electronic signature is used] [an electronic signature [a method] is used which provides a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise], it is presumed that the data message is an original.
>
> (2) The provisions of this article do not apply to the following: [...]."

84. A number of concerns were raised as to the purpose of draft article 7 and whether it was necessary to include such an article in the Uniform Rules. It was pointed out that the purpose of draft

article 7 was to establish that the criteria for reliable assurance as to the integrity of the information in a data message (in the context of an original in article 8 of the Model Law) could be met, or would be presumed to be met, by the use of a method of electronic signature. One concern was that the use of a signature as a means of satisfying the criteria of reliable assurance as to integrity in article 8 of the Model Law might not be appropriate to the concept of originality and might have the effect of imposing the use of a signature on a requirement for an original, where a signature might not otherwise be necessary. In addition, the view was expressed that it was not clear how draft article 7 would operate when what was required was a unique original. It was also suggested that the use of a particular method of signature to establish a presumption of originality might be interpreted as departing from the flexible test established in paragraph (3) of article 8 of the Model Law, and might not be technologically neutral.

85. Another concern was that, if the purpose of draft article 7 was to provide a means by which the criteria in article 8 could be satisfied, not only paragraphs (1)(a) but also paragraph (1)(b) of article 8 should be referred to in draft article 7. Similarly, it was pointed out that the establishment of a presumption of an "original" in draft article 7 was not fully consistent with article 8 of the Model Law, which referred to information in “original form”. Since the idea of an “original” was difficult to understand in the context of electronic commerce, the presumption in draft article 7 should refer to the data message as having the value of an original or as being the equivalent of an original. A further view was that the focus of draft article 7 in relation to the integrity of the data message should be to establish that, by the use of a method of signature, the data message could be presumed not to have been altered; the issue should not be whether the data message satisfied a requirement for an original, since this was addressed in article 8 of the Model Law.

86. On the issue of how draft article 7 would function in practice, it was pointed out that there was an element of circularity in the current drafting. It was suggested that, in essence, draft article 7 provided that, where a method could demonstrate integrity by reference to certain technical criteria and that method was used, the benefit of a presumption of integrity was obtained. In that case, however, integrity would be proven by the use of the method and was therefore a matter of fact, not a matter to be presumed. Similarly, if draft article 7 were to refer to the use of an enhanced electronic signature, use of such a signature would lead to a presumption of integrity. When considered in the light of the definition of enhanced electronic signature in draft article 2, however, draft article 7 would have little meaning because integrity was potentially a feature of an enhanced electronic signature.

87. In support of retaining draft article 7, it was pointed out that, if the Uniform Rules were to be a text independent of the Model Law, draft article 7 might serve a useful function, especially in situations where the Model Law, or at least article 8, was not adopted. To reflect this concept more clearly, and address a concern about repeating only a part, rather than the whole, of article 8 of the Model Law in draft article 7, it was proposed that the text should be amended as follows, and should be accompanied by a note in a guide explaining that, where it was not already adopted, States could enact article 8 of the Model Law in full:

> “A data message shall be presumed to be original information for the purposes of [*the law of the enacting State*] if it complies with the requirements of *[article 8 of the Model Law as enacted in the enacting State*].”

That proposal was not widely supported. A view was expressed, however, that the effect of all four paragraphs of article 8 of the Model Law should not be ignored.

88. Another view was that draft article 7 was useful in providing a means for establishing a guarantee of the integrity of the data message, especially where an enhanced electronic signature was used. A related view was that, if the issue of integrity was not to be addressed in the context of draft article 7, it might need to be considered for inclusion in draft article 6 as one of the criteria for a signature, along the lines proposed in the definition of "enhanced electronic signature" in draft article 2.

89. After discussion, the Working Group agreed that, for the purposes of further consideration, the Uniform Rules should include, in square brackets, a draft article 7 under which, where a method within draft article 6 was used and that method satisfied paragraphs (1)(a) and (b) of article 8 of the Model Law (these paragraphs were to be repeated in full in the draft article), a presumption would be established that the data message was in original form. Such a provision would add to the Model Law by establishing a method of generating a signature which could establish a presumption of original form. In connection with that decision, it was also agreed that, while the revised version of draft article 7 to be prepared by the Secretariat would no longer mention the notion of "enhanced electronic signature", it should not be interpreted as preempting the final decision of the Working Group, to be made at a later stage, as to whether the draft Uniform Rules would refer to that notion or not.

Article 8. Determination of [enhanced] electronic signature

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

> (1) *[The organ or authority specified by the enacting State as competent]* may determine [that an electronic signature is an enhanced electronic signature] [which [methods][electronic signatures] satisfy the requirements of articles 6 and 7].
>
> (2) Any determination made under paragraph (1) should be consistent with recognized international standards.

91. Support was expressed in favour of retaining draft article 8. One view was that, while the draft article was not an enabling provision that could, or would, necessarily be enacted by States in its present form, it nevertheless gave a clear message that certainty and predictability could be achieved by determining which signature techniques satisfied the reliability criteria of draft articles 6 and 7, provided that such determination was made in accordance with international standards. It was further emphasized that what was required to facilitate the development of electronic commerce was certainty and predictability at the time when commercial parties might use a signature technique, not at the time when there was a dispute before the courts. Where a particular signature technique could satisfy requirements for a higher degree of reliability and security, there should be a means for assessing that technical aspects of reliability and security and according the signature technique some form of recognition, such as provided by the mechanism of draft article 8.

92. On the issue of satisfaction of the reliability criteria of draft article 6, a proposal was made that

what should be considered was not the satisfaction of those criteria in absolute terms, but the extent to which a particular technology could satisfy those criteria. That proposal was supported.

93. Concern was expressed, however, that the draft article should not be interpreted in a manner that would either prescribe mandatory legal effects for the use of certain types of signature techniques, or would restrict the use of technology to those techniques determined to satisfy the reliability requirements of draft articles 6 and 7. Parties should be free, for example, to use techniques which had not been determined to satisfy draft articles 6 and 7, if that was what they had agreed to do. They should also be free to show, before a court or arbitral tribunal, that the method of signature they had chosen to use did satisfy the requirements of draft articles 6 and 7, even though not the subject of a prior determination to that effect. A related concern was that the draft article should not be seen as making a recommendation to States as to the only means of achieving recognition of signature technologies, but rather as indicating the limitations that should apply if States wished to adopt such an approach. It was suggested that these points should be clearly explained, possibly in a guide to the Uniform Rules.

94. Doubts were expressed as to the role of the State in making the determinations referred to in paragraph (1). One view was that any organ or authority set up to assess technical reliability of signature techniques should be industry-based. Another view was that the draft article should not focus on the question of who or what might be authorised to make the determination, but rather on the matters to be considered if any determination was to be made. Concern was also expressed as to the meaning of the words "recognized international standards". It was pointed out that reference to "recognized" standards might raise questions as to what would constitute a recognized standard and of whom recognition was required. It was also suggested that the word "standard" needed to be interpreted in a broad sense which would include industry practices and trade usages, texts emanating from such organizations as the International Chamber of Commerce, as well as the work of UNCITRAL itself (including these Rules and the Model Law); it should not be limited to official standards developed, for example, by the International Standards Organization (ISO) and the Internet Engineering Task Force (IETF). To address these concerns, it was suggested that the reference to "recognized standards" could be replaced with "relevant standards" and an explanation of these matters included in a guide to the Uniform Rules.

95. To reflect some of the above doubts and concerns, the following proposals were made as possible substitutes for the text of draft article 8:

> "(a) Any determination by [*the State*] as to which electronic signatures satisfy the requirements of article 6 shall be consistent with recognized international standards.
>
> "(b) The enacting State may appoint an organ or authority to make a determination as to what technologies or electronic signatures, in accordance with international standards, would satisfy articles 6 and 7.
>
> "(c) In making a determination that electronic signatures are entitled to the presumptions of articles 6 and 7 due regard shall be had to recognized international standards.
>
> "(d) One or more methods of electronic signature [provided such methods conform with

recognized international standards] may be determined as satisfying *a priori* the requirements of articles 6 and 7."

96. Considerable support was expressed in favour of the principles set forth in these various options. It was observed that the first two proposed paragraphs included a reference to the body that might make the determination, while the second two proposed paragraphs focused on the determination itself.

97. As a matter of drafting, with respect to paragraph (1) of draft article 8, support was expressed in favour of the alternative words "which methods satisfy the requirements of articles 6 and 7". With respect to paragraph (2), it was suggested that the word "shall" should replace the word "should".

98. After discussion, the Working Group agreed that: (1) the revision of draft article 8 should reflect, possibly as two variants, the proposals set forth above; (2) a guide or explanatory note to the Uniform Rules should make it clear that the mechanism referred to in draft article 8 for making a determination as to satisfaction of the requirements of draft articles 6 and 7 was not the only means of achieving certainty and predictability in signature techniques; (3) it should also be made clear that less emphasis should be placed on the role of the State in making this determination and more on the establishment of some other organ or authority; (4) the draft article should only refer to the use of electronic signatures and references to enhanced electronic signatures should be deleted, however without preempting the final decision of the Working Group, to be made at a later stage, as to whether the Uniform Rules would refer to that notion or not; (5) any determination made within the meaning of this draft article should be in accordance with international standards; and (6) any determination made should take into account not only whether certain methods satisfied the requirements of draft articles 6 and 7 but also the degree or extent to which those requirements were met.

Article 9. [Responsibilities] [duties] of the signature holder

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

"(1) A signature holder [has a duty to] [shall]:

(a) Exercise due diligence to ensure the accuracy and completeness of all material representations made by the signature holder which are relevant to issuing, suspending or revoking a certificate, or which are included in the certificate.

(b) Notify appropriate persons without undue delay in the event that [it knew its signature had been compromised] [its signature had or might have been compromised];

(c) Exercise due care to retain control and avoid unauthorized use of its signature, as of the time when the signature holder has sole control of the signature device.

"(2) If [there are joint holders][more than one person has control] of the [key][signature device], the [obligations] [duties] under paragraph (1) are joint and several.

"(3) A signature holder shall be [responsible][liable] for its failure to [fulfil the obligations [duties] in][satisfy the requirements of] paragraph (1).

"(4) [Liability of the signature holder may not exceed the loss which the signature holder foresaw or ought to have foreseen at the time of its failure in the light of facts or matters which the signature holder knew or ought to have known to be possible consequences of the signature holder's failure to [fulfil the obligations [duties] in][satisfy the requirements of] paragraph (1).]"

Title

100. It was generally agreed that, in order not to create confusion by using either the words "obligations" or "duties", which might connote different types of responsibilities and sanctions, in the various legal systems, the title of draft article 9 should refer merely to "conduct" or "responsibilities" of the signature holder. With respect to the notion of "signature holder", the view was expressed that the term "signature device holder" would be more appropriate, since it would clarify the distinction to be made between the legal notion of "signature" on the one hand, and the technical concept of "signature device" on the other. While no decision was made by the Working Group in that respect, it was generally felt that the issue might need to be further considered in the context of draft article 2.

Paragraph (1)

101. For the same reasons as expressed regarding the title of draft article 9 (see above, para. 100), it was decided that the opening words of paragraph (1) should read "A signature holder shall" (for continuation of the discussion, see below, para. 105).

102. General support was expressed for the substance of subparagraph (a). However, with respect to the verbs "issuing, suspending or revoking a certificate", it was generally felt that broader wording should be used to cover the entire life-cycle of the certificate. That life-cycle might begin before the certificate was actually issued, for example at the time when the information certifier received an application for issuance of the certificate. Similarly, the life-cycle might be extended beyond the time of expiry initially stipulated for a given certificate, for example in case of renewal or extension of the certificate. In view of the wide range of possible factual situations to be covered, it was agreed that a flexible formulation should be used to avoid the need to specify each event that might occur in relation to the certificate during its life-cycle. It was also agreed that the wording used in subparagraph (a) was not sufficiently neutral in that it might be read as implying that the signature device would necessarily involve the use of a certificate. With a view to making it clear that not all signature devices might rely on certificates, it was decided that the opening words of subparagraph (a) should read along the following lines: "Where the signature device involves the use of a certificate ...". For the same reason, it was decided that subparagraph (a) should be relocated after subparagraphs (b) and (c). As a matter of drafting, it was agreed that the words "or which are included in the certificate" should be replaced by the words "or which are to be included in the

certificate".

103. With respect to subparagraph (b), wide support was expressed in favour of retaining words along the lines of "it knew that its electronic signature had or might have been compromised". A concern was expressed, however, that the rule might place excessive emphasis on a subjective determination of what the signature holder "knew". It was suggested that a more objective reference to what the signature holder "ought to have known" should be added to the current text. In response, it was recalled that the words "or ought to have known" had not been included in draft article 9 on the basis that it would be difficult for the signature holder to satisfy a duty of notification that was based on something it ought to have known, but did not in fact know. With a view to alleviating the expressed concern, the following text was proposed for subparagraph (b):

> "Notify appropriate persons without undue delay if
> (i) the signature holder knows that the signature device has been compromised; or
> (ii) the circumstances known to the signature holder give rise to a substantial risk that the signature device may have been compromised".

The Working Group accepted that proposal.

104. While the substance of subparagraph (c) was found to be generally acceptable, it was decided that no reference to the time when the signature holder had acquired sole control of the signature device was necessary. As a matter of drafting, it was decided that, to avoid any ambiguity as to the meaning of the notion of "control" of the signature device, the provision should read along the following lines: "Exercise due care to avoid unauthorized use of its signature". With a view to ensuring consistency in terminology, the Secretariat was invited to consider whether a single term could be used instead of the two concepts of "due diligence" in subparagraph (a) and "due care" in subparagraph (c). The term "reasonable care" was suggested as a possible substitute.

Paragraph (2)

105. The discussion focused on the issue whether, in a case where the signature device was held jointly by more than one holder, the liability for failure to meet the requirements in paragraph (1) should be joint and several. It was widely felt that paragraph (2) might inappropriately interfere with the law governing liability outside the Uniform Rules. As to the substance of the rule, it was stated that there were situations where it might be unfair to provide that each holder of the device was liable for the entire loss that might have resulted from unauthorized use of the device, e.g., in case of unauthorized use of a corporate signature device held by a number of employees. It was decided that each holder should only be liable to the extent that it had personally failed to meet the requirements in paragraph (1). To that effect, it was decided that paragraph (2) should be deleted, and that the opening words of paragraph (1) should read along the lines of: "Each signature device holder shall".

Paragraph (3)

106. The Working Group found the substance of paragraph (3) to be generally acceptable as a general statement of liability of a signature holder who failed to satisfy the requirements of paragraph

(1). As a matter of drafting, a suggestion was made that the provision should read: "A signature holder shall assume the legal consequences for its failure to satisfy the requirements of paragraph (1)". After discussion, the Working Group decided that, in order not to suggest that the Uniform Rules dealt in any detail with the legal consequences of misconduct by the signature holder, paragraph (3) should read as follows "A signature holder shall be liable for its failure to satisfy the requirements of paragraph (1)".

Paragraph (4)

107. It was recalled that paragraph (4) was based upon article 74 of the Sales Convention. It established a rule based upon a test of foreseeability of damage, but was limited to breach of the obligations of the signature holder in paragraph (1). Concerns were expressed by the Working Group that the liability which might arise in the context of a contract for the sale of goods was not the same as the liability that might arise from the use of a signature, and could not be quantified in the same way. It was also stated that a test of foreseeability might not be appropriate in the context of the contractual relationship between the signature holder and the information certifier, although such a test might be appropriate in the context of the relationship between the signature holder and a relying party (for previous discussion, see A/CN.9/457, paras. 93-98). It was explained, in response, that establishing a test of foreseeability in the context of draft article 9 would merely amount to restating a basic rule which would apply under readily applicable law in many countries. Where that basic rule did not readily apply, paragraph (4) would provide useful guidance to courts and tribunals when assessing the liability of the signature holder, and avoid in practice the application of consequential or punitive damages that might largely exceed the amount of any damage reasonably foreseeable by the signature holder at the time when the electronic signature was applied.

108. The prevailing view, however, was that it might be difficult to achieve consensus as to what consequences might flow from the liability of the signature holder. Depending on the context in which the electronic signature was used, such consequences might range, under existing law, from the signature holder being bound by the contents of the message to a mere liability to pay damages. It was stated that the Uniform Rules should not embark on the preparation of any provision that might interfere with the general law of obligations. Accordingly, that matter was left to paragraph (3), which established the principle that the signature holder should be held liable for failure to meet the requirements of paragraph (1), and to the law applicable outside the Uniform Rules in each enacting State, with respect to the legal consequences that would flow from such liability. After discussion, the Working Group decided to delete paragraph (4).

Article 10. Reliance on an enhanced electronic signatures

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

"(1) A person [is] [is not] entitled to rely on an enhanced electronic signature to the extent that it [is] [is not] reasonable to do so.

"(2) In determining whether reliance [is][is not] reasonable, regard shall be had, if

appropriate, to:

(a) the nature of the underlying transaction that the signature was intended to support;

(b) whether the relying party has taken appropriate steps to determine the reliability of the signature;

(c) whether the relying party knew or ought to have known that the signature had been compromised or revoked;

(d) any agreement or course of dealing which the relying party has with the subscriber, or any trade usage which may be applicable;

(e) any other relevant factor."

110. Support was expressed both for and against the retention of draft article 10. In support of retention, it was pointed out that draft article 10 served a useful purpose in setting forth conduct that the relying party should follow, along the lines of a code of conduct. A further view was that, since electronic signatures were a new phenomenon and raised issues relevant to reliance that were not raised by handwritten signatures, draft article 10 could provide courts and tribunals with useful guidance. In addition, it was pointed out that, since draft article 11 focused upon certificates, draft article 10 could address types of signatures that did not rely upon certificates and assist the efforts of the Working Group to formulate rules that achieved a satisfactory degree of technology neutrality.

111. A number of views were expressed in support of the deletion of the draft article. One view was that draft article 10 introduced a new concept, that of reliance, which related both to the message and the signature, and which might raise difficult questions when confronted with the law of obligations and the need to assign risk. It was suggested, in relation to assignment of risk, that the draft article raised issues which it did not explicitly settle, and therefore was likely to lead to confusion and uncertainty. If the draft article were to be retained, its relationship to questions of risk allocation would need to be clarified.

112. Concern was expressed as to the relationship between draft articles 10 and 6. One view was that a provision dealing the question of whether or not a signature could be relied upon was tantamount to addressing the reliability of the signature method, an issue dealt with in draft article 6. In response, it was pointed out that the focus of draft article 10 was conduct that would make reliance possible, not the reliability of a signature method within the meaning of draft article 6. Another view was that, where issues of reliance were covered by contract, these should be left to draft article 6 and the determination of what signature technique satisfied the criteria of reliability. In the case of third parties, where contract was not relevant, mere reliance would not be sufficient to establish an obligation on the part of the signature holder. Since draft article 10 did not address anything beyond the question of mere reliance, it added very little to the Uniform Rules and therefore could be deleted. It was further suggested that what was required was a provision which addressed something in addition to the reliability of the signature and this was provided in draft article 11, which addressed reliance on certificates.

113. As a matter for drafting, some support was expressed in favour of a negative formulation of draft article 10, since this would be consistent with an approach under which draft articles 9 to 12 would establish a code of conduct, without addressing the consequences of failure to follow the conduct indicated. As a substantive point, however, it was noted that the criteria set forth in paragraph (2) were not really rules of conduct, with the possible exception of subparagraph (b). While a code of conduct might be a useful means of addressing the issues set forth in draft article 10, it was pointed out that draft article 10, as currently drafted, did not achieve this aim. Another drafting suggestion was to add a further criterion to paragraph (2) to the effect that it should be ascertained whether the electronic signature was the subject of a certificate.

114. After discussion, the Working Group decided that, before reaching a final conclusion on draft article 10, it would be necessary to consider draft article 11, and the responsibilities that might attach to information certifiers under draft article 12.

Article 11. Reliance on certificates

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

> "(1) A person [is] [is not] entitled to rely on a certificate to the extent that it [is] [is not] reasonable to do so.
>
> "(2) In determining whether reliance [is][is not] reasonable, regard shall be had, if appropriate, to:
>
> (a) any restrictions placed upon the certificate;
>
> (b) whether the relying party has taken appropriate steps to determine the reliability of the certificate, including reference to a certificate revocation list where relevant;
>
> (c) any agreement or course of dealing which the relying party has with the information certifier or subscriber or any trade usage which may be applicable;
>
> (d) [any] [all] other relevant factor[s]."

116. At the outset of the discussion on draft article 11, concern was expressed that the emphasis of the draft article should be upon reliance on the information contained in the certificate, not on the certificate as such. Although it was acknowledged that this could be addressed in draft article 2 in the definition of "certificate", a preference for making this point expressly in the substance of draft article 11 was stated. A question was raised as to whether draft article 11 should focus upon the conduct required to establish that reliance was reasonable, or address the criteria by which the quality or reliability of a certificate could be ascertained. Support was expressed in favour of draft article 11 addressing issues of reliance on, not reliability of, the certificate.

117. Concerns were expressed that draft article 11, like draft article 10, introduced a new concept

of reliance. While draft article 11 set out criteria to be followed before reliance could be determined to be reasonable, it did not address what would occur where some of those matters were not properly considered or where the certificate was relied upon, notwithstanding that it might not have been reasonable to do so. In other words, it did not address the consequences of failure to comply with what was set forth in paragraph (2). Support was expressed in favour of draft article 11 addressing the consequences for the relying party in those situations. As to the content of a provision on such consequences, two approaches were suggested. One suggestion was to include a formulation along the lines of the draft provisions quoted following para. 58 of document A/CN.9/WG.IV/WP.82, which would provide that, in the event of failure to follow the conduct in paragraph (2), the relying party would bear the risk that the signature was not valid as a signature. Another suggestion was that failure to follow the prescribed conduct would result in the relying party having no claim against either the information certifier or the signature holder. While support was expressed in favour of both of the above-suggested approaches, doubts were expressed as to whether rules along these lines would be appropriate in all cases. Several examples were cited in which it was suggested that the result should not be that the relying parties bore the risk of the signature being invalid simply because they did not follow the conduct set forth in draft article 11 (e.g., where the relying party failed to check a certificate revocation list but checking that list would not have revealed that the signature had been compromised). In support of that view, it was suggested that the purpose of draft article 11 was not to override contractual terms and conditions, not was it intended to remove the ability to decide each case on its merits from the relevant court or tribunal.

118. The view was expressed that draft article 11 should not specify consequences, but should be more along the lines of a code of conduct, a view already noted in respect of draft article 10. A related view was that the negative formulation of draft article 11 was preferable because it did not create legal effect and supported the notion of a code of conduct. In support of the view that draft article 11 should establish a code of conduct, it was pointed out that different jurisdictions adopted different rules on liability, for example, on the application of comparative negligence, and it would be very difficult to reach agreement on how consequences could be addressed. A further view expressed was that, as the law of electronic commerce was not a discrete area of law, rules proposed by the Working Group to deal with concepts which already existed in national law (even if in slightly different contexts and even if the specific application of these concepts to electronic commerce issues might be uncertain) could not ignore the manner in which those concepts were treated. This was especially true in relation to issues of liability and the consequences of liability. It was suggested that the Working Group should focus upon setting forth relevant factors that would assist courts and tribunals to extend these existing concepts to electronic commerce.

119. Doubts were expressed about the use of the word “entitlement” and the appropriateness of establishing an entitlement to rely upon a certificate in draft article 11. The view was expressed that the word “entitlement” might suggest that some benefit was being conferred upon the relying party in addition to what might otherwise be applicable. To address this difficulty, an article along the following lines was proposed:

> “In determining whether it was reasonable for a person to have relied on the information in a certificate, regard shall be had to: [insert paragraph 2(a) to (d)]”

120. Support was expressed in favour of the substance of the criteria set forth in paragraph (2),

with a suggestion for the addition of a further factor along the lines of paragraph 2(c) of draft article 10, but in relation to the signature device. As a matter of drafting , it was suggested that, for reasons of completeness, reference to a suspension list, in addition to a revocation list, should be added to paragraph 2(b).

121. As to the location of draft article 11 in the Uniform Rules, it was proposed that draft articles 9 and 12 should appear before draft articles 10 and 11, since those articles established the responsibilities of signature holders and information certifiers, both of which were relevant to the question of reliance and the scope of the responsibility of the relying party. A related suggestion was that draft articles 10 and 11 should be merged into a single article dealing with both signatures and signatures supported by certificates. It was pointed out, however, that this suggestion reflected a previous draft of this article, which had been separated into two articles for the reasons that different considerations applied to the concepts of reliance on signature and reliance on signatures supported by certificates (A/CN.9/WG.IV/WP.82, para. 56).

122. After discussion, the Working Group decided, in respect of both draft articles 10 and 11, that: (1) although the discussion on draft article 10 had not been completed, the Secretariat should prepare a revised draft of article 10 to reflect the deliberations in the Working Group; (2) the Secretariat should prepare a revised draft of article 11 to reflect (possibly as two variants or, alternatively, as two consecutive paragraphs) the proposal set out in paragraph 119 above and the two types of consequences discussed in paragraph 117 above; (3) draft articles 10 and 11 should be located in the Uniform Rules after draft article 12; and (4) draft articles 10 and 11 should not be merged on the basis of the reasons discussed in the Working Group.

Article 12. [Responsibilities] [duties] of an information certifier

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

"(1) [An information certifier is [obliged to [shall]] [*inter alia*]:

(a) act in accordance with the representations it makes with respect to its practices;

(b) take reasonable steps to ascertain the accuracy of any facts or information that the information certifier certifies in the certificate, [including the identity of the signature holder];

(c) provide reasonably accessible means which enable a relying party to ascertain:

(i) the identity of the information certifier;

(ii) that the person who is [named][identified] in the certificate holds [at the relevant time] the [private key corresponding to the public key][signature device] referred to in the certificate;

[(iii) that the keys are a functioning key pair];

(iv) the method used to identify the signature holder;

(v) any limitations on the purposes or value for which the signature may be used; and

(vi) whether the signature device is valid and has not been compromised;

(d) provide a means for signature holders to give notice that an enhanced electronic signature has been compromised and ensure the operation of a timely revocation service;

(e) exercise due diligence to ensure the accuracy and completeness of all material representations made by the information certifier that are relevant to issuing, suspending or revoking a certificate or which are included in the certificate;

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

"Variant X

"(2) An information certifier shall be [responsible][liable] for its failure to [fulfil the obligations [duties] in][satisfy the requirements of] paragraph (1).

"(3) Liability of the information certifier may not exceed the loss which the information certifier foresaw or ought to have foreseen at the time of its failure in the light of facts or matters which the information certifier knew or ought to have known to be possible consequences of the information certifier's failure to [fulfil the obligations [duties] in][satisfy the requirements of] paragraph (1).

"Variant Y

"(2) Subject to paragraph (3), if the damage has been caused as a result of the certificate being incorrect or defective, an information certifier shall be liable for damage suffered by either:

(a) a party who has contracted with the information certifier for the provision of a certificate; or

(b) any person who reasonably relies on a certificate issued by the information certifier.

"(3) An information certifier shall not be liable under paragraph (2):

(a) if, and to the extent, it included in the certificate a statement limiting the scope or extent of its liability to any person; or

(b) if it proves that it [was not negligent][took all reasonable measures to prevent the damage]."

General remarks

124. It was noted, at the outset, that the scope of draft article 12 should be understood as covering the activities of information certifiers only in connection with those electronic signature that were intended to produce legal effect under draft articles 6 and 7. Other activities of information certifiers, including the possible issuance of certificates of lesser reliability were not dealt with by the Uniform Rules.

125. As a matter of drafting, it was suggested that the notion of "information certifier" might be replaced appropriately by the more descriptive term "supplier of certification services". It was agreed that the question might need to be further discussed in the context of draft article 2.

Title

126. It was generally agreed that the title of draft article 12 should parallel the title of draft article 9 (see above, para. 100).

Paragraph (1)

127. For reasons of consistency, it was also agreed that the opening words of paragraph (1) should mirror those of draft article 9(1) (see above, paras. 101 and 105) . A suggestion was made that the words "which enable a relying party to ascertain" should be replaced by the words "which enable a relying party to ascertain any of the following, that the information certifier is capable of disclosing". That suggestion was objected to on the grounds that the factors listed in subparagraph (c) did not address what the information certifier was capable of disclosing or not, but should be regarded as establishing a prescriptive list of cumulative factors to be made available in any event by the information certifier.

Subparagraph (a)

128. The substance of subparagraph (a) was found to be generally acceptable. As a matter of drafting, a suggestion was made that the reference to the information certifier's "practices" should be replaced by a reference to its "activities". However, it was felt that, in view of the widespread use of concepts such as that of "certification practices statement", the reference to "practices" should be maintained.

Subparagraphs (b) and (e)

129. The substance of both subparagraphs was found to be generally acceptable. In view of the similarities in their contents, it was agreed that they should be merged into one subparagraph, which would read along the following lines: "exercise due diligence to ensure the accuracy and completeness of all material representations made by the information certifier that are relevant to the life-cycle of the certificate, or which are certified in the certificate".

Subparagraph (c)

130. The substance of subparagraphs (c)(i) and (c)(iv) to (vi) was found to be generally acceptable.

131. It was noted that subparagraph (c)(ii) referred both to a "key pair" and to a "signature device". To reflect the technology-neutral approach taken in the Uniform Rules, the Working Group agreed that a technology-neutral formulation such as "signature device" or "signature creation device" should be used as an alternative to the words "key pair", since "key pair" referred specifically to digital signatures. Use of the phrase "key pair" in relation to the definition of "certificate" might be appropriate in situations where certificates were only used in a digital signature context.

132. With respect to subparagraph (c)(ii), a suggestion of a drafting nature was that, consistent with the approach taken in the context of draft article 6 (see above, para. 80), the word "identified" should be used instead of the word "named". Under that approach, the concept of identity was to be interpreted more broadly than a mere reference to the name of the signature holder, since it might refer to other significant characteristics, such as position or authority, either in combination with a name or without reference to the name (see A/CN.9/WG.IV/WP.82, para. 29). After discussion, the Working Group agreed that subparagraph (c)(ii) should read along the following lines: "that the person who is identified in the certificate holds, at the relevant time, the signature device referred to in the certificate".

133. It was generally agreed that subparagraph (c)(iii) should be deleted. If the public key referred to in the certificate corresponded to the private key held by the signature holder and there was, therefore, a mathematical correspondence between the two keys, it was not clear what additional functionality would be achieved by a requirement that the key pair be "a functioning key pair". It was also uncertain whether the information certifier could provide information, in addition to what was required by paragraph (c)(ii), that would indicate that additional functionality.

Subparagraphs (d) and (f)

134. The substance of subparagraphs (d) and (f) was found to be generally acceptable.

Proposals for additional provisions

135. In the context of the discussion of subparagraph (c), the view was expressed that draft article 12 should establish an additional rule setting out the minimum contents of a certificate (see A/CN.9/WG.IV/WP.82, para. 61). It was suggested that such a rule might be based on elements of subparagraph (c) and on paragraph (3)(a) of variant Y along the following lines:

> "A certificate shall state
> (a) the identity of the information certifier;
> (b) that the person who is identified in the certificate holds, at the relevant time, the signature device referred to in the certificate;
> (c) that the signature device was effective at or before the date when the certificate was issued;

(d) any limitations on the purposes or value for which the certificate may be used; and

(e) any limitation on the scope or extent of liability which the information certifier accepts to any person".

136. Another proposal was made, in relation to an proposal made earlier in connection with draft article 13 to the effect that the characteristics of an information certifier as described in draft article 13 should not be taken into account only in respect of foreign entities but should equally apply to domestic information certifiers (see above, paras. 30 and 35). Accordingly, it was suggested that a subparagraph (g) should be added at the end of paragraph (1) along the following lines:

"(g) In determining whether and the extent to which any systems, procedures and human resources are trustworthy for the purposes of subparagraph (f), regard shall be had to the following factors: [subparagraphs (a) to (h) of draft article 13(4), Variant B]".

137. Those two proposals were met with considerable interest. It was agreed that the issues they raised might need to be further discussed at a future session on the basis of a revised draft of paragraph (1) to be prepared by the Secretariat to reflect the above discussion.

Paragraph (2)

138. While the desirability of establishing basic rules regarding liability of information certifiers was noted, it was widely felt that consensus might be difficult to achieve in respect of what those rules might be. For reasons already expressed in the context of draft article 9 (see above, paras. 107-108), a strong body of opinion was that the Uniform Rules could do little more than adopting paragraph (2) of Variant X, thus stating a general principle that failure by the information certifier to comply with the requirements of paragraph (1) should entail liability. As to precisely what that liability might be (e.g., contractual or tortious liability, liability for negligence or strict liability), no attempt should be made in the Uniform Rules to establish any provision that might conflict, or otherwise interfere, with existing legal doctrines regarding liability under applicable law.

139. An equally strong feeling was that the authors of the Uniform Rules should not miss the opportunity of establishing guiding principles and minimum standards as to liability and allocation of risk in the field of electronic signatures. Such guidance was needed by legislators and courts that would be confronted with the practical issues of liability in electronic commerce. Internationally recognized liability standards were also needed by practitioners of electronic signatures, including information certifiers themselves. Examples were given of national laws specifically geared to electronic signatures, which dealt with the issue of liability of information certifiers simply by establishing that contractual clauses limiting the liability of such information certifiers should be treated as null and void. In the absence of minimal harmonization at the international level, national laws applicable through conflicts rules might thus impose extremely harsh standards that could potentially affect the growth and the global availability of electronic commerce techniques.

140. Various suggestions were made as to how minimal liability provisions could be drafted. One suggestion was to adopt paragraph (3) of Variant X. However, while it was generally agreed that

the liability of the information certifier might need to be treated differently from the liability of the signature holder, doubts were expressed as to whether the criterion of foreseeability was more likely to achieve consensus in draft article 12 than it had been in the context of draft article 9 (see above, para. 107). Another suggestion was that the Uniform Rules, without interfering with the operation of domestic law, might provide a list of factors to be taken into consideration when applying domestic law to information certifiers. Wording along the following lines was suggested:

"In assessing the loss, regard shall be had to the following factors:
(a) the cost of obtaining the certificate;
(b) the nature of the information being certified;
(c) the existence and extent of any limitation on the purpose for which the certificate may be used;
(d) the existence of any statement limiting the scope or extent of the liability of the information certifier; and
(e) any contributory conduct by the relying party."

141. The suggestion was met with considerable interest. It was stated that such wording might provide useful guidance, while preserving the necessary flexibility to avoid interfering with the operation of local law regarding, for example, a differentiated measure of damages, or a differentiated assessment of contributory negligence, according to whether liability was in contract or in tort.

142. For lack of sufficient time, the Working Group did not pursue the discussion and decided that it should be resumed at its next session. The Secretariat was requested to prepare a revised draft of paragraph (2) taking into account the above discussion. It was noted that, in accordance with the decision made by the Commission at its thirty-second session, the thirty-sixth session of the Working Group would be held in New York from 14 to 25 February 2000. [5/]

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. 207-211.

[4/] Ibid., Fifty-fourth Session, Supplement No. 17 (A/54/17), paras. 308-314.

5/ Ibid., para. 434.