UNITED
NATIONS

A

General Assembly

Distr.
GENERAL

A/CN.9/457
25 February 1999

ORIGINAL: ENGLISH

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

REPORT OF THE WORKING GROUP ON ELECTRONIC COMMERCE ON THE WORK OF ITS THIRTY-FOURTH SESSION (Vienna, 8-19 February 1999)

CONTENTS

V.99-81356

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. The Working Group continued revision of the Uniform Rules at its thirty-third (July 1998) session on the basis of a note prepared by the Secretariat (A/CN.9/WG.IV/WP.76). The report of that session is contained in document A/CN.9/454.

9. The Working Group on Electronic Commerce, which was composed of all the States members of the Commission, held its thirty-fourth session in Vienna from 8 to 19 February 1999. The session was attended by representatives of the following States members of the Working Group: Argentina, Australia, Austria, Brazil, Burkina Faso, Cameroon, China, Colombia, Egypt, Finland, France, Germany, Honduras, Hungary, India, Iran (Islamic Republic of), Italy, Japan, Mexico, Nigeria, Paraguay, Romania, Russian Federation, Singapore, Spain, Thailand, United Kingdom of Great Britain and Northern Ireland, and the United States of America.

10. The session was attended by observers from the following States: Angola, Belarus, Belgium, Bolivia, Canada, Croatia, Cuba, the Czech Republic, Georgia, Guatemala, Indonesia, Ireland, Kuwait, Lebanon, Morocco, the Netherlands, New Zealand, Poland, Portugal, the Republic of Korea, Saudi Arabia, Slovakia, South Africa, Sweden, Switzerland, Turkey, and Uruguay.

11. The session was attended by observers from the following international organizations: United Nations Conference on Trade and Development (UNCTAD) United Nations Economic Commission for Europe (UN/ECE), United Nations Educational, Scientific and Cultural Organization (UNESCO), United Nations Industrial Development Organization (UNIDO), African Development Bank, European Commission, Organisation for Economic Cooperation and Development (OECD), Asian Clearing Union, European Law Student Association (ELSA) International, International Association of Ports and Harbors (IAPH), International Bar Association (IBA), International Chamber of Commerce (ICC), International Telecommunications User Group (INTUG), Internet Law and Policy Forum (ILPF), Society for Worldwide Interbank Financial Telecommunications (S.W.I.F.T), and *Union internationale des avocats* (UIA).

12. The Working Group elected the following officers:

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

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

Rapporteur: Mr. Louis-Paul ENOUGA (Cameroon).

13. The Working Group had before it the following documents: provisional agenda (A/CN.9/WG.IV/WP.78); two notes by the Secretariat containing revised draft uniform rules on electronic signatures (A/CN.9/WG.IV/WP.79 and 80); and the note by the Secretariat prepared for the thirty-third session of the Working Group (A/CN.9/WG.IV/WP.76), for continuation of the discussion on the issues of recognition of foreign electronic signatures (draft articles 17 to 19).

14. 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

15. The Working Group discussed the issue of electronic signatures on the basis of the notes prepared by the Secretariat (A/CN.9/WG.IV/WP.76, 79 and 80). 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

16. At the outset, the Working Group exchanged views on current developments in regulatory issues arising from electronic commerce, including adoption of the UNCITRAL Model Law on Electronic Commerce, electronic signatures and public key infrastructure (hereinafter referred to as "PKI") issues in the context of digital signatures. These reports, at the governmental, inter-governmental and non-governmental levels, confirmed that addressing electronic commerce legal issues had become increasingly recognized as important for the facilitation and implementation of electronic commerce and the removal of barriers to trade. It was reported that several 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 these 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 changes 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.

17. The Working Group commenced its consideration of the Uniform Rules by recalling the desirability and feasibility of preparing rules on electronic signatures and the need to work towards harmonization of the law in that area (see above, para. 7). It was pointed out that a number of references had been made to work being undertaken on specifically digital signatures and the diversity of laws appearing on this particular signature technique underlined the importance of harmonization. It was also pointed out that while the principles of technology neutrality and media neutrality underpinned the Model Law, in the draft Uniform Rules which addressed a number of different signature techniques, following these principles created a tension. While there was general agreement that consistency between the Model Law and the Uniform Rules should be ensured, it was recognized that drafting provisions which attributed specific legal effects to these various types of signature techniques required a balance which might be difficult to achieve. It was suggested that the Uniform Rules should focus upon: uses of signatures, which might include looking specifically at issues of functional equivalence for an "enhanced" or high-level signature; the consequences of the use of various signature techniques on the parties involved, including the conduct of those parties (rather than trying to establish a link between any specific legal consequence and the use of any specific electronic signature technique); and issues of cross-border recognition.

18. The view was expressed that the relationship between article 7 of the Model Law and the draft Uniform Rules needed to be further clarified. The necessity and desirability of building upon article 7 were questioned and it was pointed out that providing a single shortcut to satisfaction of the very flexible requirement in article 7(1)(b) that the method of identification used be "as reliable as appropriate for the purpose for which it was used" might prove difficult. Reference was made to the diversity of the matters listed in the Guide to Enactment (see para. 58 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce) as relevant to any consideration of the purpose for which the method was used. It was recalled that the Working Group had considered this issue on a number of occasions in its previous deliberations and the current draft of the Uniform Rules left this issue to be resolved. A further concern was expressed that considering a rule on what types of signature techniques might satisfy the requirement in article 7 might lead to a rule which could be construed as having a very narrow sphere of application in relation to commercial transactions (which generally were not required to satisfy any particular rules of law as to form of transactions).

19. The question of what form the draft Uniform Rules might take was raised and the importance of considering the relationship of the form to the content was noted. Different approaches were suggested as to what the form might be, which included contractual rules, legislative provisions, or guidelines for States considering enacting legislation on electronic signatures. The relationship of the Uniform Rules, as legislative provisions, to the Model Law was also raised in the context of the consideration of form. It was recognized that the discussion in the Working Group on the use of various signature techniques had been particularly helpful in advancing understanding of the relevant issues and that the Working Group documents provided a good outline of the basic concepts. Pending a final decision as to the relationship between the Uniform Rules and the Model Law, overall preference was

expressed in the Working Group for dealing with the Uniform Rules as a separate instrument.

20. With respect to the scope of the Uniform Rules, it was generally felt that consumers should not be dealt with specifically in the Uniform Rules. Nevertheless, since there might be cases where the Uniform Rules might prove to be useful to consumers, the suggestion was made that the formulation set out in footnote ** to article 1 of the Model Law could be adopted. A further suggestion was that, in any event, the scope of consumer transactions covered by the Uniform Rules should be limited to commercial transactions as described in footnote *** to article 1 of the Model Law (for continuation of the discussion, see below, paras. 56 and 70).

21. The Working Group was of the view that the draft of the Uniform Rules contained in document A/CN.9/WG.IV/WP.80 (in this report referred to as WP.80) constituted a more acceptable basis for discussion than that contained in document A/CN.9/WG.IV/WP.79 (in this report referred to as WP.79). It was pointed out that it might be helpful for the Working Group to consider WP.79 once it had completed its consideration of WP.80 in order to gauge whether there were any further issues which might need to be addressed.

B. CONSIDERATION OF DRAFT ARTICLES

Article A. Definitions

22. The text of draft article A as considered by the Working Group was as follows:

"For the purposes of these Rules:

"(a) 'Electronic signature' means data in electronic form in, affixed to, or logically associated with, a data message, and [that may be] used to [identify the signature holder in relation to the data message and indicate the signature holder's approval of the information contained in the data message].

"(b) 'Enhanced electronic signature' means an electronic signature which [is created and] can be verified through the application of a security procedure or combination of security procedures that ensures that such electronic signature:

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

(ii) can be used to identify objectively the signature holder in relation to the data message;

(iii) was created and affixed to the data message by the signature holder or using a means under the sole control of the signature holder.

"(c) 'Signature holder' means a person by whom, or on whose behalf, an enhanced electronic signature can be created and affixed to a data message.

"(d) 'Information certifier' means a person or entity which, in the course of its business, engages in [providing identification services] [certifying information] which [are][is] used to support the use of enhanced electronic signatures".

Subparagraph (a) - Definition of "electronic signature"

23. Approaching the issue of the definition of electronic signature from a broad perspective, it was suggested that such a definition was superfluous, since the concept of electronic signature was well known and understood. Another view was that the term "signature" should not be used, since it suggested that a definition of the legal concept of a signature was being provided, whilst the Uniform Rules were merely aimed at regulating the use of certain types of technology. Electronic signature, like digital signature, was a technical concept and should not be used as a legal term indicating legal effect. Yet another view was that no definition was needed since the notion of "electronic signature" was sufficiently explained in article 7 of the Model Law.

24. In response, it was pointed out that "electronic signature" could not be merely a technical term, since it did not refer to any particular signature technique, but was intended to provide a link between a variety of techniques and the legal notion of a signature. As to whether article 7 of the Model Law sufficiently covered the matter of the definition of a "signature" in an electronic environment, it was pointed out that article 7 did not contain a definition. Article 7 was geared towards providing a functional-equivalence rule for a range of situations where technical devices were used to produce substitutes for traditional hand-written signatures. It was widely felt that the need for the definition of "electronic signature" should be addressed in terms of the structure of WP.80. It was pointed out that a definition was needed both because an electronic signature was given legal effect in draft article B, and in order to be able to construct a definition of enhanced electronic signature. After discussion, it was generally agreed that a definition of "electronic signature" should be included. However, a view was expressed that a definition was not necessary because no legal effect would be attached to it see below, para. 48).

25. Various suggestions were made as to how the definition of "electronic signature" might be improved. One suggestion, which was widely supported, was that the square brackets should be removed from the words "that may be". It was generally felt that the definition should not cover only the case where an electronic signature was effectively used, but also point to its availability as a technical signing device.

26. Another suggestion was that the use of the term "approval" was too subjective and conducive to uncertainty as it depended on the intentions of the signer at the time of signing. It was suggested that a more objective wording should be used and the following text was proposed as an alternative, based upon a draft directive of the European Parliament and Council on a common framework for electronic signatures:

"Electronic signatures means data in electronic form attached to, or logically associated with, other electronic data and which serves as a method of authentication."

27. In response to that suggestion, it was pointed out that the use of the word "approval" did not necessarily imply any assessment of the subjective intent of the signer with respect, for example, to the

contractual or other legal effects of the message. Instead, it was limited to associating the signer with the message, which was a necessary element of most existing definitions of any type of signature, as illustrated by the use of the notion of "approval" in article 7 of the Model Law. The suggested alternative was not adopted by the Working Group.

28. With a view to reflecting some of the views and concerns that had been expressed in the discussion, it was suggested that the elements necessary to define an electronic signature might be expressed more clearly along the following lines:

"Electronic signature" means data in electronic form which:

(a) is included in, attached to or logically associated with a data message;

(b) is provided by a signer as a means of identifying himself;

(c) is used by a signer to indicate his approval of the information in the date message; and

(d) can be used to verify that identification".

29. It was pointed out that the suggested changes were intended to clarify: firstly, that while the data constituting the electronic signature should be provided as a means of identifying the signer, the actual use of the data for that purpose might not occur until some time after the signature had been created; and secondly, that verification could be done by the recipient, the signer or by a third party, but that verification of the means of identification had to be possible. However, in the light of earlier comments about the word "approval", a suggestion was made to delete subparagraph (c).

30. While some support was expressed in favour of the suggested text, doubts were expressed about the need for subparagraph (d). Subparagraph (d) implied the possible involvement of third parties in the verification of the signature and was thus outside the scope of the actual signature. In addition, subparagraph (d) might not be needed in the context of the general category of electronic signature, since that category might include types of signature where verification would have little meaning.

31. It was suggested that, in order to align the definition in WP.80 with article 7 of the Model Law, the words "electronic form in, affixed to, or logically associated with, a data message, and" should be replaced with "any method in relation to a data message" as follows:

"Electronic signature means any method in relation to a data message that may be used to [identify the signature holder in relation to the data message and indicate the signature holder's approval of the information contained in the data message]".

32. After discussion, the Working Group decided that the definition contained in subparagraph (a) should be retained with all square brackets removed. It was also decided that, for continuation of the discussion at a later stage, an alternative draft should be prepared, based on the above-suggested wording (see above, para. 31), which referred to the use of a "method" along the lines of article 7 of the Model Law.

Subparagraph (b) - Definition of "enhanced electronic signature"

33. It was suggested that the notion of "enhanced electronic signature"should be replaced by that of "certified electronic signature", which was said to be more in line with digital signature practice. While support was expressed in favour of the proposal, it was generally felt that the notion of "enhanced" signature was preferable since the intervention of a third party to certify the signature would not be necessary in all instances.

34. With a view to better expressing the idea that the enhanced electronic signature should be both unique as a signature and singular to the signer, a proposal was made to replace subparagraph (b) by the following:

> "Enhanced electronic signature" means an electronic signature in respect of which it can be shown, through the use of a security procedure, that:
>
> (i) it was unique in the context in which it was used; and
>
> (ii) it was not used by any person other than the signer".

35. Some support was expressed in favour of the proposal. However, doubts were expressed as to whether the elements of the definition contained either in the new proposal or in the original subparagraphs (i) to (iii) did create any difference in substance between an "electronic signature" and an "enhanced electronic signature". With a view to expressing the specific character of an "enhanced electronic signature", it was suggested that additional language should be introduced in subparagraph (b) along the lines of subparagraph (b)(iv) contained in WP.79 as follows:

> "(iv) was created and is linked to the data message to which it relates in a manner such that any change in the data message would be revealed".

36. Strong support was expressed in favour of the suggested addition, which was said to provide a necessary (and otherwise missing) link between the enhanced signature and the information contained in the data message. It was stated that applying an "enhanced electronic signature" should make any subsequent alteration of the message more difficult, much in the same way as the use of a handwritten signature made it more difficult to alter the contents of a paper document. In addition, it was pointed out that, although the function described in subparagraph (iv) was similar to the "hash function"offered by digital signatures, any other signature technique (e.g., authentication techniques based on signature dynamics) should be capable of offering the same level of reliability as to the integrity of the message. A guarantee as to the integrity of the message was needed, particularly in view of the ease with which undetectable changes could be made to documents in electronic form.

37. It was objected, however, that not all electronic signatures providing a high degree of security would perform the function referred to in subparagraph (iv), which was said to be typical of certain types of digital signatures only. As to a possible parallel between the hash function and the handwritten signature, it was pointed out that a handwritten signature as such did not offer much certainty as to the non-alteration of the document. With respect to the difference between an "electronic signature" under subparagraph (a) and an "enhanced" signature under subparagraphs (b)(i) to (iii), it was stated that only the "enhanced" signature inherently involved the use of security procedures which could provide highly objective assurances as to the identity of the signer. The view was expressed that such an identification

function should be considered separately from the function of verifying the integrity of the message, which might be needed only where the law required an original document. As a matter of drafting, it was stated that the wording of subparagraph (iv) might lend itself to misinterpretation, particularly if the provision that any alteration in the data message should be "revealed" were to be read as implying that the exact nature of the alteration would be spelled out. It was proposed that, should subparagraph (iv) be retained, language based on the text of article 8(1)(a) of the Model Law (e.g., "provides reasonable assurance as to the integrity of the message") should be used.

38. A concern was expressed that introducing subparagraph (iv) in the definition of "enhanced electronic signature" might raise questions as to the consistency of the Uniform Rules with article 8 of the Model Law. While article 8 provided that integrity should be guaranteed "from the time when [the information] was first generated in its final form", subparagraph (iv) would require integrity only as of the time when the signature was applied. It was stated in response that the definition of "enhanced electronic signature" was not aimed at dealing with the functional equivalence between a data message and an original document for all legal purposes. Rather, that definition was meant to ensure that an enhanced electronic signature could reliably identify a given message as the message which had been sent.

39. After discussion, the Working Group decided that a text along the lines of the suggested subparagraph (iv) should be added between square brackets to the text of subparagraph (b) or, as an alternative, to the text proposed in para. 34 above, for continuation of the discussion after the Working Group had reviewed the substantive provisions of the draft Uniform Rules. It was felt that the definition of "enhanced electronic signature" might need to be reconsidered, together with the general architecture of the Uniform Rules, once the purpose of dealing with two categories of electronic signatures had been clarified, particularly as regards the legal effects of both types of electronic signatures. It was suggested that it might be justified to deal with electronic signatures offering a high degree of reliability only if the Uniform Rules were to provide a functional equivalent to specific uses of handwritten signatures (e.g., deeds under seal, signatures certified by witnesses, and other types of certified signatures). However, it was also suggested that international unification or harmonization of such specific uses of handwritten signatures might be particularly difficult, while presenting little relevance to the vast majority of international commercial transactions. If, for those reasons, such specific form requirements were to remain outside the scope of the Uniform Rules, the additional benefit to be expected from using an "enhanced electronic signature" as opposed to a mere "electronic signature" might need to be further clarified, possibly in the context of draft article B. The Working Group agreed that discussion as to that issue might need to be reopened at a later stage.

Subparagraph (c) - Definition of "signature holder"

40. While general support was expressed for the substance of subparagraph (c), a question was raised as to whether the definition of "signature holder"should simply replace the definition of "signer" as contained in WP.79. It was suggested that, while the signature holder and the signer would, in most instances, be the same person, the two concepts might need to be used for distinguishing the act of signing from the mere possession of a signature device. While the discussion focused on the definition of "signature holder", it was widely felt that the discussion might need to be reopened at a later stage regarding the possible definition of "signer".

41. Various views were expressed as to the exact formulation of subparagraph (c). One view was

the definition should not cover only situations where an "enhanced electronic signature" was used but should extend to situations where signature devices were used in the context of mere "electronic signatures". To the extent the "signature holder" might be granted rights and obligations under draft articles E, F and G, there was no reason why the same rights and obligations should not be attributed to users of "electronic signatures" in general. A note of caution was struck, however, about burdening all users of electronic signatures with the obligations created for the signature holder under those articles. For example, under the laws of certain countries, the mere typewriting of the name of the signer at the bottom of an electronic mail message might be sufficient as a "signature". However, it might not be appropriate to provide that the signer should protect such "signatures" to the same extent the "signature holder" should protect the "signature device" containing a private key in a public-key infrastructure (PKI) environment. It was generally agreed that the matter would need to be further discussed in the context of draft articles E to G.

42. A widely shared view was that subparagraph (c) should apply only to the "rightful" holder of the signature device, as a person whose rights and obligations were being dealt with in subsequent articles of the Uniform Rules. Any person coming into possession of a signature device through fraud should not be protected by the Uniform Rules.

43. A concern was expressed that the words "on whose behalf" might raise questions regarding the law of agency and representation of legal entities, which the Uniform Rules should not interfere with. In response, it was observed that similar wording had been introduced in the definition of "originator" under the Model Law, on the assumption that any implication concerning agency should be settled by reference to the law applicable outside the Model Law. It was generally felt that the same assumption should be made under the Uniform Rules (see below, para. 90).

44. Another concern was that the notion of "signature holder" might be inconsistent with the notion of "originator" under the Model Law. It was stated in response that, while the signature holder and the originator might be the same person, it was still justified to maintain two definitions, in view of their distinct purposes. The notion of originator was used to determine the person to whom the message was attributable, whereas the signature holder had to be identified to determine who owed obligations for managing a signature device.

45. As a matter of drafting, it was suggested that the notion of "signature device holder" would be more appropriate, although admittedly more cumbersome, than the notion of "signature holder".

46. With a view to addressing some of the views and concerns that had been expressed, it was suggested that alternative wording for subparagraph (c) might be considered along the following lines:

> "Signatory" means a person who rightfully holds a signature creation device and acts either for himself or the entity he represents".

47. The Working Group did not conclude its deliberations with respect to subparagraph (c). In the context of the discussion of the definition of "signature holder" the view was expressed that the scope of the definition (as the scope of the draft Uniform Rules in general) was too broad and that, as a consequence, the individual rules contained therein were too general to provide any meaningful answer to the difficulties that were encountered in practice with respect to public-key infrastructures (PKI) in

the context of which digital signatures were used (for continuation of the discussion, see below, para. 66).

48. The Working Group engaged in a general discussion of the scope of the Uniform Rules. In view of various remarks and concerns expressed at earlier stages in the discussion, it was suggested that the concepts of both electronic signature and enhanced electronic signature should not be used in the Uniform Rules since they were not in fact "signatures", but rather techniques that enabled the identification of the sender of a data message and identification of the message that was sent. Accordingly, there was no rationale for using the term "signature" to describe such techniques, and in fact to do so could create confusion as the term "signature" carried with it meanings closely associated with its use in the paper environment and with the legal effects of its use in that environment (see above, paras. 23-24). It was suggested that article 7 of the Model Law provided a rule which dealt sufficiently with the functional equivalent of signatures in the paper and electronic environments in so far as such a rule was needed. Formulating a rule which indicated which signature techniques would satisfy the test in article 7 was not appropriate in view of these factors and in view of the difficulties associated with trying to ensure that technologies which had not yet been developed might be brought within the scope of such a provision. In addition, a view was expressed that adopting a single rule to indicate which signature technique would satisfy article 7 of the Model Law would be inappropriate in the light of the diversity of the concept of "signature" in the different legal traditions.

49. Another suggestion was that the Working Group should consider technologies which had been developed and which were being used in commercial transactions, such as digital signature techniques within a public key infrastructure (PKI). Once rules on PKI had been agreed, it would be possible to consider whether such rules could have a wider application. On that basis, it was proposed that the Working Group should not proceed to consider draft A to D of WP.80, but should focus upon draft articles F to H of WP.80 in the context of PKI (see above, para. 4).

50. That suggestion was widely supported, although some concerns were expressed that the focus on PKI might be too narrow and likely to discriminate against technologies other than PKI. It was suggested that draft articles A to D should not be dismissed without further consideration, but that discussion could be deferred until after draft articles F to H had been reviewed. It was pointed out that draft article B, in particular, might serve an important function in defining the scope of application of articles F to H. In addition , it was suggested that article E, which dealt with the principle of party autonomy, would be important to any consideration of the obligations of the parties in articles F to H. A further suggestion was that the question of cross-border recognition of foreign digital signatures and certificates, as discussed in draft articles 17 to 19 of document A/CN.9/WG.IV/WP.76 should also be considered in the context of rules on PKI. It was also noted that WP.79 could serve as a useful reference in determining whether there were other issues (in addition to draft articles E to H and issues of cross-border recognition) that could be considered in the context of rules on PKI.

51. The Working Group generally agreed to continue its consideration of these issues on the basis that it would focus first upon rules for PKI as reflected in draft articles E to H of WP.80, with the possibility of considering the extension of those rules once they were agreed; that issues of media neutrality and the legal effects of PKI would not be further pursued at this stage but kept in mind for continuation of the discussion at a later stage; and that cross-border recognition issues would be added to the topics to be considered. It was recognized that since WP.80 had not been drafted with this focus in mind, the document should only be viewed as a starting point for discussion. As to the form of the

Uniform Rules, while no final decision could be made at this stage, the Working Group adopted as a working assumption that the provisions being prepared would be legal rules with commentary, and not merely guidelines (for continuation of the discussion, see below, para. 72).

52. The Working Group proceeded next with a discussion of the substance of draft articles E to G.

Article E. Freedom of contract

53. The text of draft article E as considered by the Working Group was as follows:

> "A signature holder and any person who may rely on the electronic signature of the signature holder may determine that as between themselves the electronic signature is to be treated as an enhanced electronic signature".

54. As the Working Group was to consider the question of party autonomy in the context of PKI, it was felt that the focus of draft article E might be too narrow and that a broader consideration of the issue was required. While it was generally agreed that commercial parties should have the freedom to contract and allocate risk between or among themselves, some limits might need to be stated, for example, in relation to consumer protection or other public policy issues.

55. To facilitate discussion of a broader concept of party autonomy, the following text was proposed:

> "(1) These Rules are intended only for commercial relationships and shall not be applied so as to conflict with any law concerned with the protection of consumers.
>
> "(2) By agreement, whether express or implied, commercial parties are free to deviate from or modify any aspect of these Rules.
>
> (Commentary would say that 'None of the provisions of these Rules is mandatory'.)
> (Commentary would say that this autonomy provision relates only to these Rules, it does not affect *ordre public* or mandatory laws applicable to contracts such as provisions relating to unconscionable contracts.)
>
> "(3) None of the provisions of these Rules shall be applied so as to exclude, restrict, or discriminate against any alternative form of electronic signature [that meets the requirements of article 7 of the Model Law on Electronic Commerce] [that is applied to a data message and 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.]."

56. There was general support for an article along the lines of the proposal. As a matter of drafting, it was suggested that the reference to consumers in paragraph 1 of the draft article should be aligned with the language of footnote** to article 1 of the Model Law as follows: "This Law does not override any rules of law intended for the protection of consumers" (see above, para. 20, and below, para. 70). Another drafting suggestion was that the second square-bracketed language in proposed paragraph (3)

should be deleted, as the reference to article 7 of the Model Law was the more appropriate alternative and, in order to align the drafting to article 7, the words "electronic signature" should be deleted and the word "method" substituted. A further suggestions was that the heading "Party Autonomy" should replace the heading of draft article E. There was general support for these drafting proposals.

57. It was suggested that the reference to agreement between the parties did not address the issue of possible detriment to third parties not involved in the agreement with sufficient clarity. To ensure that any agreement between the parties could not have effects on third parties, it was proposed that words to the effect that the parties were free to agree to certain effects "as between themselves" should be adopted from draft article E. That suggestion was widely supported.

58. Some concern was expressed as to the meaning of paragraph (3) and its relationship to paragraphs (1) and (2). It was pointed out that while paragraphs (1) and (2) clearly related to the issue of party autonomy, paragraph (3) introduced a different principle, i.e., that of non-discrimination. Without further considering the content of such a provision at this stage, it was proposed that paragraph (3) should be included as a separate article. That proposal was widely supported. As to the meaning of paragraph (3), it was suggested that such a provision was not needed, since the purpose of the draft rules would not be to give a benefit to any particular technique, even though focusing upon PKI. It was widely felt, however, that, pending a final decision by the Working Group as to whether the Uniform Rules would deal with any specific legal consequence of using digital and other electronic signatures, a provision along the lines of the proposed paragraph (3) was useful.

59. A further concern with the proposed article was that, when considered in the context of draft article F which covered obligations in both contract and tort, the proposed article on party autonomy might allow the parties to agree to modify the law of tort. It was pointed out in response that, in commercial relationships, the parties should be free to modify those obligations and, for example, accept higher or lower levels of liability than would otherwise be the case under the general law of tort.

60. In order to reflect the various views and concerns expressed in the discussion, an amended proposal was made as follows:

> "(1) These Rules shall apply only to commercial relationships and shall not be applied so as to override any law intended for the protection of consumers.
>
> "(2) By agreement, whether express or implied, among themselves commercial parties are free to deviate from or modify any aspect of these Rules.
>
> (Commentary would say that 'None of the provisions of these Rules is mandatory.')
> (Commentary would say that this autonomy provision relates only to these Rules, it does not affect *ordre public* or mandatory laws applicable to contracts[, such as provisions relating to unconscionable contracts].)
> (Commentary may address significance of phrase 'among themselves'.)
>
> "(3) None of the provisions of these Rules shall be applied so as to exclude, restrict, or discriminate against any alternative method [of signature] that meets the requirements of article 7 of the Model Law on Electronic Commerce."

61. There was wide support for the substance of the revised proposal. However, a suggestion was

made that the principle of party autonomy could be expressed more succinctly. Some doubt was also expressed as to whether the rules should be limited to commercial relations, as indicated in paragraph (1) of the proposal, or whether draft articles F to H might also be useful in the context of consumers. One suggestion was that the rules should apply equally to consumers and commercial parties, provided mandatory law for the protection of consumers was not affected. A view was expressed that the reference to mandatory law or *ordre public* should be transferred from the commentary and set out explicitly in the text of the proposed rule.

62. With a view to addressing some of the concerns raised in connection with proposed paragraphs (1) and (2), language along the following lines was proposed:

> "These Rules shall only apply insofar as parties have not agreed otherwise, and they shall not override any mandatory law or *ordre public*."

Some support was expressed for the substance of that proposal.

63. It was observed that, in order to reach a proper understanding of the scope of an article on party autonomy, it might be important to consider the nature of draft articles F to H. One view was that the draft articles were intended to be default or gap-filling rules which would apply when the parties had not made any agreement on the issues covered. Another view was that the draft articles would apply unless the parties agreed otherwise. Strong support was expressed in favour of the view that draft articles F to H should perform the function of gap-filling rules.

64. After discussion, the Working Group concluded that both the detailed proposal and the concise proposal for a new article on party autonomy addressed the same principle. The Working Group agreed that, for continuation of the discussion at a future session, the revised article on party autonomy should: address the preservation of consumer protection laws; focus on commercial relationships as defined in footnote **** to article 1 of the Model Law; ensure the freedom of parties to agree between themselves; and preserve mandatory laws. The Working Group agreed that these principles on party autonomy would form a satisfactory basis for considering draft articles F to H and that the discussion on party autonomy could be resumed at a later stage in the light of the discussion on those draft articles. As to the need for a provision on non-discrimination, which had been raised in the proposal for a more detailed article on party autonomy, no decision was made. It was agreed that further consideration of that principle should be deferred until after draft articles F to H had been reviewed.

Article F. Obligations of signature holder

65. The text of draft article F as considered by the Working Group was as follows:

> "(1) A signature holder is obliged to:
>
> (a) Exercise due care to avoid unauthorized use of its signature;
>
> (b) Notify [appropriate persons] [as soon as possible] in the event its signature is compromised and could be used to create unauthorized enhanced electronic signatures;

(c) Ensure that all material representations or statements made by the signature holder to information certifiers and relying parties are accurate and complete to the best of the signature holder's knowledge and belief.

"(2) A signature holder shall be responsible for the consequences of its failure to fulfill the obligations in paragraph (1)".

General remarks

66. As a provisional conclusion of its deliberations over the definition of "signature holder" in draft article A (see above, paras. 40-47), the Working Group considered whether the "signature holder" should be the subject of the obligations stated in draft article F. It was recalled that, since the notion of "signature" was used as a reference to a technical device and not to the legal notion of a signature, the use of the term "signature holder" might lend itself to misinterpretation. It was suggested that the term "device holder" should be preferred. It was also recalled that, in view of the decision of the Working Group to consider first the issues of PKI before possibly extending the scope of the Uniform Rules to cover also other electronic signature techniques, the use of established PKI terminology might be more appropriate. It was thus suggested that terms such as "subscriber" or "key holder" might be preferable. While there was general agreement for replacing the term "signature holder" by more suitable wording, no final decision was made as to what such a more suitable wording might be. It was decided that the use of the terms "device holder", "signature device holder", "key holder" and "subscriber", all of which were used as synonymous during the discussion, might need to be reconsidered, and defined at a later stage.

67. In the context of that discussion, it was pointed out that the notions of "key holder" and "subscriber" might correspond to different periods in the life-cycle of a key pair. It was suggested that, while the key pair would typically be created prior to application for a certificate, the Uniform Rules should only apply to keys and key holders as of the time an identity certificate was issued (or requested) to allow for the practical use of the keys. Support was expressed in favour of that suggestion. The prevailing view, however, was that, while the duties of the key holder should only arise with respect to those key pairs that were effectively protected by a certificate (i.e., at the time when the certificate was issued), the duty of the key holder to protect such certified keys against misuse should retroact to the time of creation of the key pair.

68. With respect to the general reference to PKI and PKI terminology, the view was expressed 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. That view was generally accepted by the Working Group. It was generally felt, however, that 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 the 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 (for continuation of the discussion, see below, para. 109).

69. The Working Group then discussed who the subject of the obligations stated in draft article F might be. It was widely felt that only the "rightful" holder of the key should be considered. In addition, it was generally agreed that only a key holder who was aware that it was in possession of a key pair, and who had shown an intent to use the key should be made subject to obligations. Reference was made to the holding of a credit card as similar to the holding of a key pair. However, it was realized that other types of situations also needed to be considered. For example, a prospective buyer might receive from a merchant a key pair to be used for securing possible transactions with that merchant. Such a key pair could be sent through electronic messaging, without the recipient of the message being aware of the issuance and attribution of that key pair. There was general agreement that, in such a case, the recipient of the key pair should not fall under any definition of "key holder" and that it should be subject to no obligations under the Uniform Rules. It was pointed out that the notion of "reasonable care" might sufficiently address this situation since no "reasonable care" could be expected as to the key pair from the unaware holder.

70. In the context of the discussion as to who the subject of the obligations stated in draft article F might be, the Working Group examined the consequences of its earlier decision to deal with the issues of consumer protection laws by way of a provision similar to footnote ** to article 1 of the Model Law. The view was expressed that (at least under the laws of a limited number of countries),
even where a key holder had expressed an intent to use a key pair, the obligations established in draft article F might be regarded as too harsh if the key holder were to be regarded as a consumer. While it was generally felt that, in a large number of countries, the general duty of care expressed in draft article F would also apply to consumers, the Working Group reaffirmed its decision not to embark on the preparation of specific consumer law for electronic commerce. It was recalled that, under that decision, however, consumers were not be excluded from the scope of the Uniform Rules, and it would be for each enacting State to make a determination as to the need for exclusion of specific categories of key users from the application of the Rules (for previous discussion, see above, paras. 20 and 56).

71. The Working Group proceeded with a discussion concerning the person or persons to whom the various obligations established in draft article F were owed by the key holder. The view was expressed that those obligations were owed to either the certification authority or any other party who might rely on a digital signature in the context of contractual relationships with the key holder. The prevailing view, however, was that the obligations of the key holder were owed to any party who might reasonably rely on a digital signature, irrespective of whether or not that party was linked to the key holder by a contractual relationship. While the relationships between the key holder and either a certification authority or an independent key issuer would typically be contractual in nature, the relationship between the key holder and relying parties might be either contractual in the context of a commercial transaction, or based on tort. In view of their general nature, it was suggested that the "obligations" spelled out in draft article F would be more accurately described as "duties" of the key holder. The Working Group took note of that suggestion. It was generally agreed that the text of the Uniform Rules should make it clear that the obligations of the key holder should be owed to any party who reasonably relied on the use of a key and suffered a loss as a result of the keyholder's failure to fulfil its obligations. It was also agreed that, for the purpose of draft article F, the notion of "party who reasonably relied" on the use of a key should include certification authorities.

72. In the context of the general discussion of draft article F, a view was expressed that the current focus of the Uniform Rules on the establishment of a set of prescriptive provisions of a legislative nature was overly ambitious (see above, paras. 19 and 51). Accordingly, it was suggested that issues currently addressed in the Uniform Rules might be more easily solved if the purpose and nature of the entire project was reconsidered. Two possible alternatives to the current project were proposed. One alternative was to limit the contents of the Rules to a general model legislative provision, the effect of which would be to provide the broadest possible recognition of party autonomy. The remainder of the issues currently dealt with under the Uniform Rules might then be dealt with by way of a legal guide geared towards assisting parties with the structuring of their contracts regarding the issues of electronic signatures. Another alternative was to deal with the entire set of issues addressed in the Uniform Rules by way of a legislative guide, possibly accompanied by illustrative provisions. While it was pointed out that the current working assumption regarding the preparation of model legislative provisions accompanied by a legislative guide might, in practice, differ little from the latter proposed alternative, the greatly prevailing view was that the Working Group should pursue its task (the importance of which was reaffirmed, although some delegations questioned its feasibility) on the basis of the current working assumption (see above, para. 51). It was observed that, where appropriate, the Working Group might consider introducing optional formulations in the text of the Uniform Rules.

Paragraph (1)

Subparagraph (a)

73. It was widely felt that additional elements should be inserted alongside the notion of "avoiding unauthorized use of the key". It was suggested that the key holder should be under an obligation to: avoid misuse of the key; and exercise due care in retaining control of the key and control of the information contained in the signature device or used in conjunction with the signature device to create the digital signature. It was generally agreed that the notion of "control" of the key and of the information contained therein was essential, particularly for determining the time as of which the key holder should come under the obligations spelled out in draft article F. In particular in those situations where the control of the key was transferred among several successive holders of the key, draft article F should make it clear that only the person who was in control of the key was under an obligation to protect that key.

74. In connection with the discussion as to who was in control of the key, a question was raised as to whether, at any given point in time, there could be more than one holder of the same key. It was proposed that wording might be added to paragraph (1) along the following lines: "If [there are joint holders][more than one person has control of the key], the duties under paragraph (1) are joint and several". The Working Group took note of the proposal and decided that it should be reflected in the revised draft of the Uniform Rules to be prepared for continuation of the discussion at a later session.

75. With respect to the words "exercise due care", it was observed that draft article F reflected the assumption that the responsibility of the key holder was based on a standard of due diligence (also referred to as "liability for negligence") rather than on the notion of strict liability.

Subparagraph (b)

76. There was general support for a rule along the lines of subparagraph (b). It was pointed out that the words in square brackets indicated two important matters to be clarified: the persons to be notified and the time at which notification should occur.

77. On the first issue, one suggestion was that any reference to the parties to be notified should not be included, or at least that they should not be specified, as a number of different bodies might be relevant where certification authority functions were distributed. It was proposed that this issue should be further considered at a later time when it would be clear what the scope of the duties covered in the rules and the persons to whom they applied was resolved. At that time, a specific reference to the relevant persons could be included in this article. For the same reasons, it was suggested that the term "appropriate persons" should be maintained.

78. On the question of the time at which notice was required to be given, it was suggested that "without undue delay" should be adopted, as it was well understood and widely used in a number of jurisdictions and provided an appropriately flexible standard.

79. A related question was raised as to the time at which the duty to notify arose. One possibility expressed was that it arose at least as early as the time at which there was actual knowledge of the compromise of the key, but it was suggested that it could arise before that time if it could be established that the key holder ought to have known or should have known that the key was compromised. Another view was that the duty to notify arose when the key holder had "adequate grounds for suspicion" or a "reasonable suspicion" that the key was compromised or that the key was or might have been compromised. It was questioned whether there was a difference between the knowledge test in the first proposal and the question of the fact of compromise in the second. Differing views were expressed as to whether these standards were the same or achieved the same result, or whether the result in each case was desirable. In regard to the latter point, one view was that apportioning responsibility on the basis that the key "might have been compromised" placed too heavy a burden on the key holder and might discourage use of the technology. After discussion, the Working Group generally agreed that both of these standards should be included in a revised draft of subparagraph (b) for future consideration.

80. It was suggested that the rule contained in subparagraph (b), if it essentially dealt with a question of negligence, should be supplemented by a rule dealing with apportionment of risk. If risk were to be considered, it would be necessary to decide when the risk was transferred from the key holder – when notice was given, when the notice was received or when action was taken on the notice. It was pointed out in response that issues of transfer of risk were different from rules on proper and reasonable conduct, which were based on the concept of fault. The concept of risk was important where there was no question of fault. The two types of rules should be kept separate, as liability could not be equated with risk. It was noted that subparagraph (a) established a duty to take care of the key which, under paragraph (2), could lead to liability in the event that care had not been taken. Subparagraph (b) was important in that event, as it provided a means by which the key holder could mitigate the effects of the failure to take care by giving notice of the compromise of the key. In the context of liability, it was also pointed out that it might be important to consider the basis of any relationship between the parties, whether contractual or not and the content of that contract. There was general support for the formulation of a rule based on fault.

81. The question was raised as to whether the Working Group might want to consider dealing with

the legal effects of the failure to take care of the key. One view was that as this issue had proven very difficult to reach consensus on in the past, it should not be considered here. Another suggestion was that WP.79 dealt with issues of effects in greater detail and would provide a useful starting point for considering these questions further. A further view was that the detail of liability should not be dealt with beyond the content of paragraph (2), which had yet to be discussed.

82. As a matter of drafting, it was suggested that the words "and could be used to create unauthorized enhanced electronic signatures" was not needed, since it was clear what the signature device could be used for and it did not need to be stated.

83. The Working Group agreed that a future draft of subparagraph (b) should reflect the changes discussed: notice should be given "without undue delay"; the two standards of "knew or ought to have known" and "is or might have been compromised" should be included in square brackets as alternative texts; and the words "and could be used to create unauthorized enhanced electronic signatures" should be deleted.

Subparagraph (c)

84. It was suggested that the words "to information certifiers and relying parties" should be deleted on the grounds that while representations to these parties were probably the ones which should be covered, it was conceivable that there might be representations to other relevant parties. The focus of the article should be upon the obligation for the information be accurate and complete, regardless of to whom the information was provided. In response to this suggestion, it was pointed out that removing the words referring to information certifiers and relying parties might mean that the obligation was unlimited, when the focus should actually be upon representations which related to the process of identification. It was proposed that the words "and that are material to the issuance of the certificate" be added after "representations and statements".

85. Another suggestion on the issue of an objective test was that the words "which are relevant in the process of issuing a certificate or which are included in the certificate" should be added after "representations or statement". It was pointed out that such a test limited subparagraph (c) to statements made by the key holder or the person who applied for a certificate, and would not be relevant in cases where a key holder did not apply for a certificate. It was not intended, however, that those words should be interpreted in such a way as to make the person applying for a certificate liable for representations which might be stated incorrectly in the certificate, or which otherwise were not based upon information provided by the applicant for a certificate. In such cases, the information certifier would have a corresponding obligation under draft article H with respect to the content of the certificate. A key holder would be liable, however, on a narrow construction of the obligation, to a relying party where the relying party suffered loss or damage as a result of misleading or false information provided by the key holder and included in the certificate. Opposing the limitation of the subparagraph to the certification process, the view was expressed that the obligation in subparagraph (c) should be general and include the provision of information under subparagraph (b).

86. A further proposal on the scope of subparagraph (c) was that the subparagraph should be divided into two parts. Representations made to a relying party could be covered by the general obligation as to completeness and accuracy, while representations which were made to an information certifier for the purposes of obtaining a certificate could form a separate subparagraph. In the case of the information provided to the information certifier, the connection between the obligation in this draft

article and that in draft article H(1)(b) (which imposed an obligation in respect of information to be certified) was highlighted.

87. Some concern was expressed as to the persons to whom the obligations in paragraph (1) should apply. It was pointed out that it might not be appropriate to consider the whole of article F as establishing duties for the same person, as the subparagraphs of the current draft referred to different concepts. Subparagraph (a), for example, referred to both information and the device on which that information was stored and the way in which it was used. It may be that the obligation applied to a wider class of persons than just the key holder. Subparagraph (c), on the other hand, referred to information in the form of representations made to certain persons for the purpose of obtaining a certificate. These differences might need to be treated separately in any revision of the obligations in paragraph (1) of draft article F.

88. In relation to the knowledge and belief of the key holder at the time of making representations, it was pointed out that such a test was unnecessarily subjective and weak, and might result, for example, in a reduced level of responsibility where the key holder was reckless or stupid. What was required was objective language which made it clear that this was not an intended consequence of the subparagraph. One suggestion was that the words "to the best of the signature holder's knowledge and belief" should be replaced by a reference to a due diligence standard; the opening words of the subparagraph could be "Exercise due diligence in ensuring that ...". With respect to the words "accurate and complete", a view was expressed that the reference to a "complete" statement was superfluous since, in some jurisdictions, the concept of "completeness" was already included in the concept of "accuracy". That view was noted by the Working Group.

89. On the issue of terminology, the Working Group again discussed the meaning of a number of different terms, including signature holder, device holder, key holder and signature device, signature creation device, signature verification device (see above, paras. 40-47). It was proposed, in terms of a definition, that "key holder" should refer to the person by whom, or on whose behalf, the signature was attached to the data message, adopting the drafting of subparagraph (c) of article A of WP.80, a definition which recognized the concept of agency. As to the device or signature being used, the Working Group generally agreed that it was not the device that was used to create the key that was being discussed, but rather the device that was used to create the signature.

90. The Working Group considered the desirability of including agency within the concept of a key holder (for previous discussion, see above, para. 43). The general view was that agency should not be covered in the Uniform Rules, as it would be difficult to reach agreement on principles of agency and inclusion of that concept would make the scope of draft article F too broad. Where a situation of agency might be involved, such as in an employee using a signature device for a corporation, this article would have the effect that, without prejudice to corporation law, the signature of the employee would be regarded as that of the corporation, which was effectively the "key holder". The Working Group reaffirmed its earlier decision that issues of agency should be resolved under applicable law.

91. A suggestion of a drafting nature was that the term "material" was not appropriate in some jurisdictions and should therefore not be used. Another suggestion of a drafting nature was that, since the obligation under subparagraph (c) preceded the obligation under subparagraph (a) in time, the order of these two subparagraphs should be reversed.

92. After discussion, the Working Group agreed that the scope of subparagraph (c) should be limited to looking at the key holder's obligations in the context of the certification process; the key holder should ensure that representations were accurate and complete; the reference to "knowledge and belief" should be replaced by the opening words "exercise due diligence in ensuring"; the words "which are relevant in the process of issuing a certificate or which are included in the certificate" should be introduced to qualify "representations and statements", but it should be made clear that the key holder would only be liable for such statements when they were properly included in the certificate and not for mistakes or inaccuracies introduced by the information certifier; the reference to the "information certifiers and relying parties" should be removed; the order of subparagraphs (a) and (c) should be reversed; the concept of agency should not be dealt with in this article.

Paragraph (2)

93. Some support was expressed in favour of retaining draft paragraph (2) in its present form without amendment. Concerns were expressed, however, that the Uniform Rules should refer to the legal consequences of failure to fulfil the obligations set forth in draft paragraph (1). One means of addressing these consequences was to include a specific reference to national or applicable law, while a second solution was to promote harmonization by exploring possible consequences and drafting a uniform rule which should address the issue of damages, but not bind the key holder to the consequences of use of the signature device, particularly since questions of authorisation and intention might arise. However, another view was that the data message should be attributed to the key holder (see below, paras. 97 and 104). In order to place the focus of paragraph (2) on damages rather than upon consequences, it was proposed that the words "The key holder is responsible for damage and injury resulting from the failure to fulfil the obligations in paragraph (1)" should be adopted. As another means of addressing the legal consequences of failure to fulfil the obligations set forth in draft paragraph (1), it was proposed that draft article 7 of WP.79 should be considered, or perhaps an article along the lines of article 74 of the United Nations Convention on the International Sale of Goods. For the purposes of considering this proposal further, the following wording based on article 74 was suggested:

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

94. In response to this proposal based on article 74 of the United Nations Sales Convention, concern was expressed that the liability which might arise in the context of a contract for the sale of goods was not the same as liability that might arise from the use of a signature and could not be quantified in the same way. While it might be possible to foresee the damage that could arise from the breach of a contract for sale of goods, the same test could not apply in the case of the use of a particular signature technique. It was stated in that context that, under the Uniform Rules, the use of a particular signature technique should not result in any particular limitation of liability (or in any other competitive advantage over users of traditional hand-written signatures) being established to the benefit of users of electronic technology Another view was that the test of foreseeability of damage was an internationally accepted standard which might prove to be useful in the context of signatures and facilitate the drafting of a uniform rule. A further view was that if an article on damages was to be considered, it may be necessary

to distinguish between damage which arose as the result of action by the key holder which failed to meet the standard required by draft paragraph (1) and damage which arose because the key holder failed to take any action, that is between direct and indirect damage.

95. It was suggested that the duties of the key holder in article F should be analysed in terms of the parties or classes of parties to whom the duty was owed; the information certifier on one hand and a group of potential relying parties on the other. It was clear that the relationship between the key holder and the information certifier would be a contractual relationship which would be governed by the applicable law. Some doubt was expressed as to the appropriateness of applying a rule on foreseeability or remoteness of damage to such a contractual relationship. In terms of the group of relying parties, it was suggested that it might be appropriate to establish a rule which determined which relying parties might foreseeably suffer damage and the type of damage for which the key holder would be liable. Doubts were expressed as to whether article 74 of the United Nations Sales Convention captured both of these concepts and whether, in any event, it would be appropriate to have a single foreseeability rule which covered the obligations set forth in subparagraphs (a) to (c) of draft paragraph (1). It was also pointed out that draft article G dealt with issues relating to the relying party and would have to be taken account of in any article dealing with the consequences of failure on the part of the key holder to observe the obligations in draft article F.

96. To clarify the scope of application of draft paragraph (2), it was proposed that the reference to the "consequences of failing to fulfil the obligations in paragraph (1)" should be deleted, in order to avoid any uncertainty as to what the inclusion of those words might mean and to avoid considerations of whether the obligation being breached was contractual. It was also pointed out that the phrase "the consequences" might suggest that all possible consequences were under consideration and did not convey any idea as to the remoteness of those possible consequences. Deletion of these words was widely supported.

97. A further concern was expressed that if draft articles F and G were read together they could lead to a legal effect other than liability, namely attribution. It was suggested that, at the very least, a rule or a rebuttable presumption on attribution of the signature was required in order to remove uncertainty. While there was some agreement that such an article might be useful and would add to the level of trust in electronic commerce, it was pointed out that difficulties were certain to arise in the context of article 13 of the Model Law which dealt with attribution of a data message. It was generally agreed that attribution should not be considered in the context of draft article F (see below, para. 104).

98. After discussion, the Working Group agreed that, as there was both support for retaining paragraph (2) in its present form, with suggested amendments and for exploring a rule on consequences, possibly based on article 74 of the United Nations Sales Convention, a revised draft of paragraph (2) dealing with both possibilities should be included in future working papers for consideration by the Working Group. Such a provision should be limited in its application to the duties to be included in a revised version of paragraph (1) of draft article F.

Article G. Reliance on enhanced electronic signatures

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

"A person is entitled to rely on an enhanced electronic signature, provided it takes reasonable steps to determine whether the enhanced electronic signature is valid and has not been compromised or revoked".

100. Some concerns were expressed that the form in which the article was drafted was not appropriate. It was pointed out that the question that should be considered was not whether the relying party was entitled to rely upon the signature, but rather what anyone seeking to rely on the signature might have to do before reliance could be regarded as reasonable. In that regard, it would be important to indicate the situations where it would be unreasonable to rely upon the signature. In order to reflect that change of emphasis, the following words were proposed:

"(1) A person is not entitled to rely on a certificate or a signature supported by a certificate to the extent that it is not reasonable to do so.

"(2) In determining whether reliance is reasonable, regard shall be had to:

(a) any restrictions placed upon the certificate;

(b) the nature of the underlying transaction that the certificate or signature was intended to support;

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

(d) any agreement or trade usage or course of dealing which the relying party has with the information certifier or subscriber".

101. Support was expressed in favour of that proposal. To clarify what was intended by the reference to the underlying transaction in subparagraph (b), it was observed that situations might arise where it might not be sufficient to rely only on the use of a technique of identification and some other form of identification or checking might be needed. The example was given of a situation where a bank might want further confirmation that a transaction that might be considered unusual for a particular customer was in fact that customer's transaction, in addition to the use of an appropriate identification technique. Some concern was expressed that the factors stated in subparagraphs (a) to (d) might be too general and, in the context of the Working Group's assumption that PKI was being addressed, it might be helpful to make a specific reference to the need to check the validity or reliability of the certificate. For that purpose, it was suggested that the words "including reference to a certificate revocation list where relevant" could be added to subparagraph (c).

102. It was suggested that in addition to the factors set forth in subparagraphs (a) to (d) of the proposal, reference also should be made to whether the relying party knew or ought to have known that the key had been compromised or revoked or, as an alternative, that it was not reasonable to rely on the signature or the certificate. To introduce additional flexibility in the proposed text, a further suggestion was made to add the words "if appropriate" in paragraph (2) after the words "regard shall be had". Both of those proposals received some support.

103. Some support was also expressed for retaining draft article G in its current formulation or

deleting it altogether. It was pointed out that constructing an article along the lines of the proposed text would suggest the establishment of requirements or conditions for reliance on enhanced signatures. The consequences of such requirements, when considered in the context of article 13 of the Model Law, might create a situation in which it would be easier to rely on a relatively insecure electronic signature than on the more secure enhanced signature. This might have the effect of making the more secure form of signature more difficult to use. Another view was that some connection should be drawn between reliance upon the signature and article 13 of the Model Law, in particular paragraphs (3) and (4). A further view was that the current formulation of draft article G expressed a more positive policy as to whether relying parties were entitled to be confidant in the use of this type of signature. Nevertheless, it was felt that some precautions might need to be taken by a relying party and a further proposal along the following lines was made:

> "A person is entitled to rely on an enhanced electronic signature provided it takes reasonable measures to verify the validity of the signature according to the standards agreed with the key holder or to verify the information provided by the information certifier."

That proposal did not receive support.

104. Concern was expressed that the Working Group might be trying to build into draft article G legal effects that were included in draft articles B and C, but which it had been decided should not be considered at this stage. Formulating draft article G as an entitlement to rely might presume certain legal effects, while establishing what ought to be done in order to rely avoided addressing the issue of what legal effect the signature might have. It was stated that, since draft articles F, G and H focused upon rules of conduct for parties within a PKI, it was not appropriate for legal effects to be included. As to the question of attribution as raised by article 13 of the Model Law (see above, para. 97), it was observed that, while article 13 was generally limited in its scope to the situation where there was a contractual relationship between the originator and addressee of the data message, these Uniform Rules were intended to have a broader sphere of reference. It was also pointed out that formulating draft article G as a series of steps that should be considered in order to determine whether reliance was reasonable was not inconsistent with the requirement in article 13 for reasonable care, nor did it establish legal effect in terms of the validity of the signature. On the latter point, it was noted that draft article F as revised by the Working Group also did not address legal effect or validity of the signature and the form of these two draft articles was therefore consistent.

105. An opposing view was that formulating draft article G as an entitlement added a benefit that was not available under the Model Law, regardless of whether the specific legal effect was spelled out in other articles. It was proposed that the approach of establishing an entitlement to rely could be combined with the steps to be considered in determining whether reliance was reasonable as follows: "(1) A person is entitled to rely on a certificate or a signature supported by a certificate to the extent that it is reasonable to do so". A second paragraph would then set out the matters to be considered as previously proposed, with an additional category covering "all other relevant factors".

106. As a matter of drafting, it was noted that the words "reliance" and "enhanced" were not commonly used in some languages or legal systems and a more appropriate word might need to be sought.

107. After discussion, the Working Group agreed that both formulations of draft article G (see above, paras. 100 and 105) should be included in a revised article G for future consideration; that the references to "all other relevant factors" and to whether the relying party knew or ought to have known that the key had been compromised or revoked or, as an alternative, that it was not reasonable to rely on the signature or the certificate should be included; and that the words "if appropriate" should be added to paragraph (2) as discussed.

Article H. Obligations of an information certifier

108. The text of draft article H as considered by the Working Group was as follows:

"(1) An information certifier is obliged to:

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

(b) take reasonable steps to determine accurately the identity of the signature holder and any other facts or information that the information certifier certifies;

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

(i) the identify of the information certifier;

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

(iii) any limitations on the purposes for which the signature may be used; and

(iv) whether the signature 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.

(e) Ensure that all material representations or statements the information certifier makes are accurate and complete to the best of it's knowledge and belief;

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

"(2) An information certifier shall be responsible for the consequences of its failure to fulfill the obligations in paragraph (1)".

General remarks

109. The view was expressed that the possibility of stating opinions regarding the duties and liability of a certification authority was largely conditioned by the definition of a certification authority. In particular, a decision would need to be made as to whether the functions of a certification authority could be performed by a person or entity that was also a party to the underlying transaction for the

purpose of which a certificate might be used (a working assumption currently adopted by the Working Group) or whether the certification authority should, in all instances, be independent from the parties (a situation akin to that of a notary public in a number of civil law countries). After discussion, the Working Group decided to continue its deliberation of the matter on the basis of the working assumption made at that session (see above, para. 68). While the Working Group did not discuss the definition of "certification authority" as such, it was generally agreed that the words "in the course of its business" in the definition of "information certifier" in draft article A, should not be interpreted as implying that certification-related activities should be the exclusive business activities of a certification authority. A view was also expressed that there might be a need to differentiate between an entity that issued certificates merely as an incidental part of its business and an entity that engaged in the business of issuing certificates (whether exclusively or in addition to other business activities which the entity might carry on). A further view was that, given the important role played by certification authorities and the responsibilities that might flow from that important role, both for certification authorities and for relying parties, the Uniform Rules should clarify the status of certification authorities. After discussion, it was agreed that the issues of the definition, role and status of certification authorities would need to be discussed further at a future session.

Paragraph (1)

110. The discussion focused on whether the list of duties contained in paragraph (1), irrespective of what those specific duties might be, should be exhaustive or not. Strong support was expressed in favour of the view that paragraph (1) should be worded in terms of an open-ended, illustrative, list of duties. Language along the following lines was suggested as opening words for paragraph (1): "Without limiting the generality of the certification authority's obligation of due diligence, a certification authority is obliged, *inter alia*, to ...". It was stated that, while such a formulation might appear to be burdensome for the certification authority, it would in fact be consistent with the general rule that would currently apply to certification authorities in many legal systems. It was also stated that a broad statement regarding the obligations of the certification authority in paragraph (1) might be compensated by exemptions from liability, to be established under paragraph (2) or under draft article E. In that respect, it was suggested that the attention of the Working Group might appropriately focus on the ways in which contractual clauses exempting the liability of the certification authority might be extended beyond the contractual sphere. In response, it was stated that, even within the contractual sphere, limitations should be placed on the ability of certification authorities to limit their liability, for example where such limitation would be grossly unfair. The Working Group agreed that the question of contractual and other limitations to the liability of the certification authority would need to be further discussed at a future session.

111. Another view was that paragraph (1) should be phrased in terms of an exhaustive list of duties. It was stated that, under the law of certain countries, the certification authority might not be under a general duty of due diligence. The various obligations of the certification authority should thus be spelled out in detail to determine the exact scope of its liability. A further justification for that view was that the Uniform Rules should deal only with the performance of certification authority functions and should not restate general principles of tort law which might be applicable to all persons engaging in whatever types of activities. Under that view, since "certification-authority function" was an ascertainable concept, the Uniform Rules should only deal with activities within such certification-authority functions, and should not be open-ended. It was agreed that both views should be reflected

in the revised text that would be prepared for continuation of the discussion at a future session.

112. As to the substance of the specific duties listed in subparagraphs (a) to (f), general support was expressed. Various suggestions were made as to how the expression of those duties might be improved. One suggestion was that the duty to identify the signature holder under subparagraph (b) might be superfluous, as a mere illustration of the more general duty to ensure the accuracy of material representations under subparagraph (e). It was generally felt, however, that subparagraph (b) was useful to enhance clarity. Another suggestion was that subparagraph (b) should contain an additional obligation to state in the certificate the identity of the key holder.

113. Yet another suggestion was that, among its basic duties, the certification authority should be under an obligation to operate a certificate revocation list (CRL). It was suggested that the following words should be added to subparagraph (d): "and ensure the operation of a prompt and immediate revocation service". Support was expressed in favour of that suggestion. It was pointed out, however, that the obligation to operate a CRL might be appropriate for high-value transactions and certificates (i.e., for those "enhanced electronic signatures" that were intended to produce legal effect) but would be overly burdensome (and contrary to existing practice) if it were to be imposed with respect to all certificates (including "cheap certificates" used in the context of significant numbers of digital signatures). In that connection, it was recalled that one of the main difficulties of the current project was to establish a workable criterion for distinguishing between the higher level of transactions (for which a high level of security was sought, through stringent requirements on certificates and certification authorities, possibly with the view of producing specific, pre-determined, legal effects) and the bulk of lower-level uses of digital signatures and certificates (where the production of legal effects as to "signature" was largely irrelevant, and the main policy requirement was not to interfere with party autonomy). The view was expressed that, while no such workable criterion might be found, limiting the scope of the Uniform Rules to the commercial sphere (i.e., excluding consumer transactions) might provide an acceptable solution.

114. Further suggestions were made for reflecting additional elements in the list of duties established under paragraph (1) as follows: an obligation to provide information as to the revocation and suspension of certificates; in subparagraph (e), language mirroring a similar provision in draft article F; and in subparagraph (f), language expressing the obligation of the certification authority to utilize trustworthy human resources in performing its services. The following text was proposed for insertion in paragraph (1)(c): "that the person who is named in the certificate holds [held at the relevant time] the private key corresponding to the public key"; and "that the keys are a functioning key pair".

Paragraph (2)

115. With respect to the general provision concerning the liability of the certification authority for failure to fulfil the duties established under paragraph (1), it was widely felt that it would be appropriate to create a uniform rule beyond merely referring to the applicable law. As to what the contents of such a rule might be, it was suggested that it should establish a general liability for negligence, subject to possible contractual exemptions, and subject to the certification authority exonerating itself from liability by demonstrating that it had fulfilled the obligations under paragraph (1). The following text was proposed as a substitute for paragraph (2):

> "(2) Subject to paragraph (3), a certification authority shall be liable for damage suffered by

either:

(a) a party who has contracted with the certification authority for the provision of a certificate; or

(b) any person who relies on a certificate issued by the certification authority, if the damage has been caused as a result of the certificate being incorrect or defective.

"(3) A certification authority shall not be liable under paragraph (2):

(a) if, and to the extent, it included in the certificate's information 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]".

116. While support was expressed in favour of the proposal, strong objections were raised on the grounds that adopting the proposed language would amount to establishing a strict liability standard for "any damage", and that imposing a strict liability standard on certification authorities might significantly jeopardize the increased use of electronic commerce. With respect to the text of proposed subparagraph (3)(a), doubts were expressed as to whether information included in the certificate to the effect of limiting the liability of the certification authority with respect to that certificate could apply equally to contractual and tortious liability. In that context, the Working Group was urged not to attempt to base any meaningful distinction in the Uniform Rules on the notions of contractual and tortious liability, since the contents of those notions might vary significantly from country to country. Furthermore, a view was expressed that the clause limiting the liability of the certification authority ought not to be invoked to the extent that exclusion or limitation of liability would be grossly unfair. That view was supported by some delegations.

117. Support was also expressed in favour of maintaining the current structure of paragraph (2), in connection with an exhaustive list of duties under paragraph (1).

118. In connection with the discussion of the duties of the certification authority, a question was raised as to who would bear the risk of a loss resulting from reliance on an unreliable (e.g., a compromised or revoked) certificate when all parties had been diligent under draft articles F, G and H of the Uniform Rules. One suggestion was that, through the suggested negative formulation of draft article G, the relying party would bear that residual risk. It was pointed out that, in practice, reliance on means of communication such as telephone or telecopy already placed the residual risk on the relying party. Another suggestion was that provisions should be introduced in draft article H to the effect that the residual risk should be borne by the certification authority. Yet another suggestion was that the Uniform Rules should be silent on that point and leave it to the courts to determine which party should bear that risk, in view of all relevant circumstances.

119. After discussion, the Working Group did not adopt a final decision on the contents of draft article H. The Secretariat was requested to prepare variants reflecting the various views expressed, for continuation of the debate at a later session.

C. FURTHER ITEMS TO BE CONSIDERED

120. The Working Group proceeded to list the items which, for lack of time, had not been considered at that session but should be further discussed in the context of possible additions to the Uniform Rules. The view was expressed that, in its future deliberations of the Uniform Rules, the Working Group might wish to give consideration to introducing an article to establish that certificates should not be discriminated against on the basis of the place at which they were issued. The following text was proposed: "In determining whether, or the extent to which, a certificate is legally effective, no regard shall be had to where the certificate was issued, nor in which State the issuer had its place of business". The Working Group took note of that proposal.

121. Other items for future consideration included the following issues: cross-border recognition of certificates; legal effect of electronic signatures; attribution of electronic signatures; relationship between the Uniform Rules and the Model Law; definition and minimum qualities of certification authorities; possible incompatibility of functions of certification authorities with the performance of any other function in the same transaction; and revocation and suspension of certificates.

122. It was noted that the next session of the Working Group was scheduled to take place at Vienna from 6 to 17 September 1999, those dates being subject to confirmation by the Commission at its thirty-second, to be held at Vienna, from 17 May to 4 June 1999. A suggestion was made on behalf of a number of delegations that the duration of future sessions of the Working Group should be limited to one week and that this matter should be fully discussed at the thirty-second session of the Commission. The suggestion was noted by the Working Group as a matter that could only be decided upon by the Commission.

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.