United Nations A/CN.9/1045

General Assembly

Distr.: General
13 November 2020

Original: English

United Nations Commission on International Trade Law
Fifty-fourth session
28 June–16 July 2021

Report of Working Group IV (Electronic Commerce) on the work of its sixtieth session (Vienna, 19–23 October 2020)

Contents

V.20-06570 (E) 171120 181120

I. Introduction

1. Background information on the work of the Working Group on legal issues related to identity management (IdM) and trust services may be found in A/CN.9/WG.IV/WP.161/Rev.2, paragraphs 4–16.

II. Organization of the session

2. The Working Group, composed of all States members of the Commission, held its sixtieth session in Vienna from 19 to 23 October 2020. The session was held in accordance with the decision on the format, officers and methods of work of the UNCITRAL working groups during the coronavirus disease (COVID-19) pandemic, as adopted by States members on 19 August 2020 and contained in A/CN.9/1038. Arrangements were made to allow delegations to participate in person and remotely.

3. The session was attended by representatives of the following States members of the Working Group: Algeria, Argentina, Austria, Belgium, Brazil, Canada, Chile, China, Colombia, Côte d'Ivoire, Czechia, Dominican Republic, France, Germany, Ghana, Honduras, Hungary, India, Indonesia, Iran (Islamic Republic of), Israel, Italy, Japan, Kenya, Lebanon, Libya, Malaysia, Mexico, Nigeria, Pakistan, Peru, Philippines, Poland, Republic of Korea, Romania, Russian Federation, Singapore, Spain, Sri Lanka, Switzerland, Thailand, Turkey, Ukraine, United Kingdom of Great Britain and Northern Ireland, United States of America, Venezuela (Bolivarian Republic of), Viet Nam and Zimbabwe.

4. The session was attended by observers from the following States: Angola, Bhutan, Bolivia (Plurinational State of), Botswana, Burkina Faso, Cambodia, El Salvador, Lao People's Democratic Republic, Madagascar, Malta, Morocco, Norway, Paraguay, Qatar, Sierra Leone, Sudan, Sweden, Tunisia, Turkmenistan and Uruguay.

5. The session was attended by observers from the Holy See and from the European Union.

6. The session was attended by observers from the following international organizations:

(a) *United Nations system*: United Nations Industrial Development Organization and World Bank;

(b) *Intergovernmental organizations*: Caribbean Community, Eastern and Southern African Trade and Development Bank, Economic Commission for Latin America and the Caribbean and Mexican Section of the TMEC Secretariat;

(c) *International non-governmental organizations*: Alumni Association of the Willem C. Vis International Commercial Arbitration Moot, Asociación Americana de Derecho Internacional Privado, China International Economic and Trade Arbitration Commission, Council of the Notariats of the European Union, Grupo Latinoamericano de Abogados para el Derecho del Comercio Internacional, Institute of Law and Technology, International and Comparative Law Research Center, International Association of Young Lawyers, International Federation of Freight Forwarders Associations, International Union of Notaries, Kozolchyk National Law Center and Law Association for Asia and the Pacific.

7. According to the decision by States members (see para. 2 above), the following persons continued their office:

Chair: Ms. Giusella Dolores FINOCCHIARO (Italy)

Rapporteur: Mr. Paul KURUK (Ghana)

8. The Working Group had before it the following documents:

(a) An annotated provisional agenda (A/CN.9/WG.IV/WP.161/Rev.2);

(b) A note by the Secretariat containing draft provisions on the cross-border recognition of IdM and trust services (A/CN.9/WG.IV/WP.162) ("draft provisions");

(c) Comments on the draft provisions submitted by the World Bank (A/CN.9/WG.IV/WP.163);

(d) Comments submitted by States, international governmental organizations and invited international non-governmental organizations in response to an invitation by the Secretariat to facilitate progress of work during the COVID-19 pandemic (A/CN.9/WG.IV/WP.164 and Add.1); and

(e) A paper submitted by the United States of America (A/CN.9/WG.IV/WP.165).

9. The Working Group adopted the following agenda:

1. Opening of the session and scheduling of meetings.
2. Adoption of the agenda.
3. Draft instrument on the use and cross-border recognition of identity management and trust services.
4. Other business.

III. Deliberations and decisions

10. The Working Group continued its consideration of legal issues related to IdM and trust services on the basis of the documents listed in paragraph 8 above. The Working Group approved the draft provisions with the agreed modifications for its further consideration. The deliberations and decisions of the Working Group are found in chapter IV of this report.

11. The Working Group considered whether to adopt its report during the session. It was reminded of the decision adopted by the States members of UNCITRAL on 19 August 2020 (see Annex I of document A/CN.9/1038) according to which the Chair and the Rapporteur would prepare a draft summary reflecting the deliberations and any conclusions reached during the session. Having reviewed the draft summary circulated by the Chair and the Rapporteur, the Working Group agreed to adopt it for transmission to the Commission as its own report. The Working Group also agreed to possibly hold informal consultations to discuss topics included in the provisional agenda for this session that were not discussed.

IV. Draft instrument on the use and cross-border recognition of identity management and trust services

12. The Working Group was invited to proceed on the basis of the tentative schedule for the session that was set out in the letter of the Chair dated 15 September 2020.

A. General remarks

13. The Working Group received a presentation on the paper submitted by the United States of America (A/CN.9/WG.IV/WP.165). The Working Group heard that the paper set out a conceptual framework for adapting the draft provisions to address multi-party private sector IdM systems. It was noted that those IdM systems employed a wide variety of structures and technologies but shared the need for operating rules specifying (a) how IdM processes and identity transactions[1] were to be conducted,

[1] The term "identity transaction" is defined in paragraph 23 of A/CN.9/WG.IV/WP.165 as "a communication whereby a relying party receives some identity information about an individual

and (b) the rights and responsibilities of the various parties. Those rules were typically placed on a contractual footing.

14. It was explained that the legal framework for private sector IdM systems consisted of three tiers (see figure 1 of A/CN.9/WG.IV/WP.165). It was suggested that the role of UNCITRAL should be to develop a "tier 2" law for private sector IdM systems which would address (a) the legal recognition of identity transactions, (b) the requirements for determining whether identity transactions satisfied applicable legal requirements to identify a person, and (c) the applicability of laws that could not be modified by operating rules. It was observed that, while the draft provisions detailed in A/CN.9/WG.IV/WP.162 addressed some of those issues, they did not accommodate the complexity and variety of IdM systems. Moreover, the draft provisions addressed matters that would typically be governed by the operating rules and did not clarify whether they were designed to establish minimum standards for IdM systems from which operating rules could not deviate.

15. It was foreshadowed that substantial modifications would need to be made to articles 6, 7, 8, 10, 11, 12 and 26 of the draft provisions, and that additional provisions would need to be discussed on (a) the application of existing "tier 1" laws to IdM systems (e.g., tort law, negligent misrepresentation, implied warranties) and (b) the use of government-issued identifiers or information from such identifiers. One delegation welcomed the paper and supported consideration of these issues during the discussions on the IdM provisions.

B. Chapter III – trust services

1. Article 13 – legal recognition of trust services

16. With regard to the subject of non-discrimination, the Working Group considered the two options presented in the chapeau of article 13 of the draft provisions, as well as a third option to refer to "the result deriving from the use of a trust service".[2] The Working Group expressed a preference for the third option.

17. It was noted that, while article 13 enshrined the principle of "non-discrimination", its title referred to "legal recognition". It was suggested that the title should be amended to more closely reflect its content. However, it was also noted that the reference to "legal recognition" was contained in the title of corresponding provisions in other UNCITRAL texts,[3] and that departing from that established practice could affect legal uniformity.

2. Article 14 – obligations of trust service providers

18. The Working Group expressed a preference not to reformulate article 14(1)(b) along the lines of article 6(f). It was noted that the policies and practices of the trust service provider were relevant to a relying party in deciding whether to accept the result deriving from the use of a trust service (e.g., an electronic signature). It was therefore proposed that the trust service provider should be required to make its policies and practices accessible to "third parties" (in addition to "subscribers") or to "the public" (instead of "subscribers"). The observation was made that both proposals essentially covered the same range of persons, and that the requirement reflected the practice of trust service providers. Another proposal was to refer to "relying parties", noting that this term would need to be defined. After discussion, the Working Group decided to insert the words "and third parties" after "subscribers".

(identification), along with verification that the person purporting to be that individual is, in fact, that individual (authentication)".

[2] See proposal in the comment accompanying footnote 7 of A/CN.9/WG.IV/WP.164/Add.1.

[3] UNCITRAL Model Law on Electronic Commerce, article 5; United Nations Convention on the Use of Electronic Communications in International Contracts, article 8; UNCITRAL Model Law on Electronic Transferable Records, article 7.

19. With respect to article 14(2), it was proposed to insert the words “consistent with applicable contractual obligations and otherwise applicable law” at the end of the chapeau, and to omit the words “in accordance with applicable law” in subparagraph (c). It was explained that the proposal was based on the recognition that trust services were governed by contractual agreements that set obligations for trust service providers and that the relationship between the rule in article 14 and those contractual obligations and existing national law should be made clear. The prevailing view of the Working Group was that article 14(2) established a minimum standard of mandatory application and therefore that there was no room for contractual deviation. The Working Group expressed a preference to retain article 14(2) as contained in A/CN.9/WG.IV/WP.162.

20. The Working Group was invited to provide guidance in explanatory materials or similar documents on the meaning of “significant impact” in article 14(2).

21. It was suggested that an additional obligation should be imposed on the trust service provider to make publicly available the means that the subscriber should use to satisfy the obligation to notify security breaches under article 15. It was added that the policies and practices of the trust service provider would further specify those means. After discussion, the Working Group agreed to amend article 14 to impose the additional obligation and asked the Secretariat to revise the provision accordingly.

3. Article 15 – obligations of subscribers

22. The Working Group confirmed its support for the definition of “subscriber”, as contained in article 1(l). It was added that, for example, the signatory of an electronic signature would fall within that definition.

23. It was explained that the contract concluded between the trust service provider and the subscriber (referred to in the definition of “subscriber”) typically provided details on the obligations listed in article 15. It was further explained that, absent such contractual provision, those obligations would apply on the basis of legislation enacting the draft provisions and that the consequences of a failure to comply would be determined by applicable national law. In this respect, it was added that, while trust service providers were a core component of the trust service infrastructure and necessitated dedicated liability rules, subscribers were not and that general liability rules should therefore apply to subscribers.

24. It was suggested that, in order to better capture its intended operation, article 15 should require the subscriber to notify in accordance with (a) the policies and practices of the trust service provider, or (b) applicable law, which included contractual agreements.

25. It was indicated that, in the absence of a contractual relationship, imposing the obligation in article 15 on third parties might not be desirable.

26. After discussion, the Working Group decided to retain the text of article 15 as contained in A/CN.9/WG.IV/WP.162.

4. Article 16 – electronic signatures

27. Different views were heard on whether the method referred to in article 16 should be qualified as being “as reliable as appropriate”.

28. It was indicated that article 16 was clearly related to article 24, on the ex ante designation of reliable trust service providers, and that the reliability of the method would be addressed in the designation process and did not need to be qualified “as appropriate”. It was added that article 16, while related also to the ex post determination of reliability under article 23, already reflected a careful balance between the two approaches that should not be disturbed.

29. At the same time, it was indicated that UNCITRAL texts containing rules on the functional equivalence of electronic signatures qualified the method to be used as being “as reliable as appropriate” to better reflect the various uses of electronic

signatures, and that it would be desirable not to depart from well-established, broadly adopted formulations.

30. Moreover, it was noted that article 16 diverged from article 9(3) of the United Nations Convention on the Use of Electronic Communications in International Contracts (ECC)[4] in two respects. Firstly, it did not contain the qualification that the method should be "as reliable as appropriate"; secondly, it did not contain a safety clause similar to that contained in article 9(3)(b)(ii) ECC. It was added that the modified version of that safety clause contained in article 23(2) of the draft provisions was also not compliant with the ECC. It was added that this divergence created issues of treaty compliance for those States which were a party, or intended to become a party, to the ECC.

31. A question was also raised with respect to the relationship between article 16 and existing laws on electronic signatures.

32. It was noted that, although the ECC did not provide for an ex ante determination of reliability of electronic signatures, that approach was generally consistent with the ECC. It was explained that the presumption of reliability, as provided for in article 16(2) and (3) of the draft provisions, complemented article 9(3) ECC.

33. Different views were expressed with respect to the relationship between article 16(1) of the draft provisions and article 9(3) ECC. The point was made that, if the draft provisions were to take the form of a model law, each State would have the flexibility to enact them in line with its treaty obligations.

34. After discussion, the prevailing view within the Working Group was to retain the text of article 16 as contained in A/CN.9/WG.IV/WP.162 for further consideration. The Working Group asked the Secretariat to explore ways to coordinate the language of article 16(1) of the draft provisions with that of article 9(3) ECC, and to provide information on the relationship of the draft provisions with (a) existing UNCITRAL texts, and (b) existing laws on electronic signatures for its consideration to inform further discussion on this provision.

5. Article 17 – electronic seals

35. It was noted that domestic laws adopted different approaches to the trust services covered by the draft provisions or did not cover the same range of trust services. In particular, it was added that several jurisdictions did not distinguish between electronic signatures and electronic seals.

36. After discussion, the Working Group agreed to retain article 17 as contained in A/CN.9/WG.IV/WP.162.

6. Article 19 – electronic archiving

37. It was noted that, unlike draft article 20 set out in A/CN.9/WG.IV/WP.160, article 19 of the draft provisions did not require the trust service provider to retain the data message. It was added that retention was an important component of electronic archiving, and therefore it was proposed to insert the following words at the beginning of article 19(1)(b)(ii):

> "Retain the data message in the format in which it was generated, sent or received, or in another format which can be demonstrated to".

38. Some caution was expressed about referring to "format" lest the revised provision prejudice the principle of technology neutrality or fail to reflect current practices. In response, it was noted that the proposed insertion allowed for data to change format and therefore safeguarded against technological obsolescence.

[4] United Nations, *Treaty Series*, vol. 2898, No. 50525, p. 3.

39. After discussion, the Working Group agreed for article 19(1)(b)(ii) to be amended to refer to retention and asked the Secretariat to revise the provision accordingly.

40. A concern was also raised that the term “data message” could be interpreted so as to apply only to data that was sent or received. It was therefore proposed that the words “or electronic record” should be inserted after “data message” in the chapeau of article 19(1). In response, it was noted that the term “data message” was defined in article 1(c) to include not only data sent and received but also data generated and stored. The view was expressed that the term should be interpreted so as to apply to data that was generated or stored but not necessarily sent or received. It was also noted that the same definition was used in UNCITRAL texts on electronic commerce, and that in the ECC the term “electronic communication” was employed to represent the notion of data being sent and received.

41. After discussion, the Working Group agreed to retain the chapeau of article 19(1) as contained in A/CN.9/WG.IV/WP.162 and to clarify in the explanatory materials that the term “data message” included data that was not sent or received.

7. Article 20 – electronic registered delivery services

42. It was recalled that the comments synthesized in A/CN.9/WG.IV/WP.164/Add.1 supported the view that article 20 should specify that assurance of the integrity of the data message and identification of the sender and recipient were additional functions of an electronic registered delivery service.

43. Further support was expressed during the session for that view. It was explained that assurance of integrity and identification were core functions of electronic registered delivery services. It was indicated that those services enabled fundamental rights such as the right to communicate and the right to privacy, and that they were key to mitigating and overcoming the effects of the COVID-19 pandemic. It was further said that the article or the explanatory materials should specify that the identification of the recipient should take place before the recipient had access to the data message.

44. After discussion, the Working Group agreed to add the words “(c) to assure the integrity of the data message; and (d) to identify the sender and the recipient” in article 20(1), and to clarify in the explanatory materials that the identification of the recipient should take place before the recipient had access to the data message.

8. Article 21 – website authentication

45. It was recalled that the comments synthesized in A/CN.9/WG.IV/WP.164/Add.1 favoured the insertion in article 21 of a reference to the presumption and proof of reliability that was already present in other provisions on trust services.

46. It was said that, while the assurance of the qualities of a data message was an element of the definition of “trust service” in article 1(m), website authentication did not provide that assurance but rather information on the identity of the domain name holder. Hence, it was added, website authentication pertained to identification and not to trust services. It was also indicated that the reference to websites alone, and not to other digital objects, could pose challenges to technology neutrality and that a broader approach would make the instrument more future-proof.

47. In response, it was indicated that website authentication comprised two elements: identification of the domain name holder and linking that person with the website. Hence, the object of the trust service was the trustworthiness of the website and not the identity of the owner. It was emphasized that website authentication aimed to identify persons, not objects.

48. After discussion, the Working Group agreed to add the following paragraphs to article 21:

"2. A method is presumed to be reliable for the purposes of paragraph 1 if a website authentication designated pursuant to article 24 is used.

3. Paragraph 2 does not limit the ability of any person:

a. To establish in any other way, for the purpose of paragraph 1, the reliability of a method pursuant to article 23; or

b. To adduce evidence of the non-reliability of a designated website authentication."

9. Article 22 – object authentication

49. Recalling previous deliberations on the topic (see, e.g., A/CN.9/971, paras. 148-149), support was expressed for the view that the draft instrument should not deal with the authentication or identification of objects. It was indicated that any discussion on objects should be limited to their traceability to a person.

50. The view was also expressed that object authentication was a necessity of trade, as evidenced by the provision on website authentication. In that line, it was suggested that articles 21 and 22 could be merged.

51. After discussion, the Working Group agreed to delete article 22.

10. Article 23 – reliability standards for trust services

52. It was observed that the scope of "recognized international standards and procedures" referred to in paragraph 1(b) was unclear and it was proposed that the paragraph should be deleted. The point was made that, if the draft provisions were to take the form of a model law, article 23 would address in domestic law the reliability of trust services, for which the industry standards referred to in paragraph 1(c) were more relevant. It was also suggested that paragraph 1(c) could be amended to refer to any "recognized" industry standard.

53. The Working Group engaged in a detailed discussion on paragraph 1(h). It was noted that the comments synthesized in A/CN.9/WG.IV/WP.164/Add.1 supported an explicit reference to any relevant agreement "between the parties". The point was made that this provision recognized party autonomy in the determination of reliability as between the parties. The importance of party autonomy in this context was stressed and support was expressed for retaining paragraph 1(h) with the additional reference.

54. However, concerns were raised as to whether it was appropriate to take into account an agreement between the parties in determining the reliability of trust services, given that (a) a relying party might not have access to the terms of the agreement, and (b) all trust service providers should be assessed against the same requirements. It was therefore proposed to delete paragraph 1(h) in its entirety.

55. In response to these concerns, it was recalled that an agreement between the parties was only one item in a non-exhaustive list of factors to be taken into account in determining reliability, and that the chapeau of article 23(1) required "all relevant circumstances" to be taken into account. It was also observed that, in practice, the aspects of the agreement relevant in determining the reliability of a trust service were limitations on the service, which were ordinarily prescribed in the policies and practices that the trust service provider was required to make accessible to third parties (see para. 18).

56. It was recalled that article 23 set out in A/CN.9/WG.IV/WP.160 provided that the reliability standard to be met by the trust service was to use a method "as reliable as appropriate for the fulfilment of the function for which the method is being used". It was further observed that, by omitting this standard, as agreed by the Working Group (A/CN.9/1005, para. 67), article 23 of the draft provisions assumed an absolute level of reliability. It was proposed that, in order to acknowledge that reliability was relative, the factors listed in article 23(1) should be amended to include "the function

for which the trust service is being used". The Working Group agreed to list this factor in article 23(1).

57. A further observation was made that (a) policies and practices of the trust service provider ordinarily formed part of the "operational rules governing the trust service" referred to in paragraph 1(a), and (b) transparency as to the limitations on the service was addressed in article 9(1)(d)(ii) of the UNCITRAL Model Law on Electronic Signatures (MLES)[5], which required the certification service provider to provide reasonably accessible means to ascertain "any limitation on the purpose or value" for which the certificate might be used. It was therefore proposed that (a) paragraph 1(a) should be amended to refer to the "operational rules, policies and practices of the trust service provider", and (b) paragraph 1(h) should be amended to specify that any relevant agreement between the parties included any limitation on the purpose or value of the transactions for which the trust service might be used. The Working Group agreed for article 23(1) to be amended accordingly.

11. Article 24 – designation of reliable trust services

58. It was suggested that the obligation contained in paragraph 2(b) could be satisfied by publication in a centralized supranational repository. Regional examples of that practice were mentioned.

59. It was indicated that both paragraph 2(a), which specified "all relevant circumstances", and paragraph 3, which specified "recognized international standards and procedures", referred to determining reliability. It was noted that the interaction between those provisions could pose issues. It was added that those standards and procedures could not be easily identified, and that the draft provisions did not provide guidance on how they were recognized. Accordingly, it was suggested that paragraph 3 should be deleted.

60. In response, it was explained that, while paragraph 2(a) referred back to standards and procedures relevant for determining reliability, paragraph 3 should instead refer to standards and procedures relevant for designation, such as conformity assessments and audits. Accordingly, it was suggested that the words "for determining the reliability of trust services, including level of reliability frameworks" should be deleted or replaced with "for designating reliable trust services".

61. It was also suggested that the words "for determining the reliability of trust services, including level of reliability frameworks" in paragraph 3 should be replaced with "for performing the designation process". It was also suggested that the words "relevant for the provision of trust services" should be inserted in article 23(1)(b) to provide additional clarity. However, it was also said that the effect of those amendments required further consideration. After discussion, the Working Group agreed to amend articles 23 and 24 according to those suggestions.

12. Article 25 – liability of trust service providers

62. The Working Group engaged in an intense discussion of the options presented for article 25 in A/CN.9/WG.IV/WP.162. It was observed that most of the comments on article 25, as synthesized in A/CN.9/WG.IV/WP.164, supported option C. During discussion, delegations were split with some expressing a preference for option A and others for option C. No support was expressed for option B.

63. It was observed that option A provided more flexibility for enacting States. In response, it was noted that the reference to domestic law in paragraph 2 of option C still provided flexibility for enacting States to apply existing law, including on matters of evidence and burden of proof. It was added that option C provided greater clarity and predictability, and, by limiting liability in paragraph 3, might also promote the provision of trust services.

[5] United Nations publication, Sales No. E.02.V.8.

64. It was noted that the standards of intention and negligence in paragraph 1 of option C were well known to most legal systems, and therefore that the differences between option A and option C were a matter of form not substance. In response, it was observed that option C established a liability regime that departed in substance from existing law in some jurisdictions. In particular, concern was raised that the standards in option C could make it more difficult to hold a trust service provider liable for failure to comply with its obligations under the instrument. On this point, it was explained that the standard of "negligence" in the English language was a lower standard than gross negligence, and it was further suggested that the Secretariat should review the French and Spanish language versions of the draft provisions in particular to ensure that they reflected the same standard.

65. It was noted that option C only applied to a failure by the trust service provider to comply with its obligations under the draft provisions, as set out in article 14 (as amended). It was observed that, since existing domestic law would impose additional obligations on trust service providers, the liability of trust service providers for failure to comply with those obligations would continue to be determined according to existing law even if option C was adopted. A suggestion was made that, to avoid doubt, paragraph 1 of option C could be amended to clarify that it was without prejudice to liability for non-compliance with other obligations under applicable law.

66. After discussion, the Working Group agreed (a) to retain option A and option C for article 25 for further consideration and to delete option B, (b) to amend paragraph 1 of option C to clarify that it is without prejudice to liability for non-compliance with other obligations under applicable law, and (c) to ask the Secretariat to illustrate the difference between the two options and to review the different language versions of paragraph 1 of option C to ensure that they reflected the same standards.

C. Chapter IV – international aspects

1. Article 26 – cross-border recognition of IdM and trust services

67. It was stressed that article 26 was a core article that allowed cross-border legal recognition of IdM and trust services to be achieved, which was one of the main goals of the instrument. Thus, it was added, the instrument would fill an important gap in the global legal landscape.

68. A question was raised regarding the feasibility of providing for cross-border recognition in the way that it was presented in article 26, given the complexity and wide variety of IdM systems and trust services.

69. Different views were expressed on the notion of equivalent level of reliability. It was indicated that the term "substantial equivalence" was not appropriate as it was vague, and that reference should be made to "same or higher" or "at least equivalent" level of reliability to indicate that higher levels of reliability would also suffice.

70. However, it was also indicated that the term "substantial equivalence" was appropriate because it facilitated cross-border recognition in circumstances where the level of reliability defined in different jurisdictions did not match exactly, which was a likely situation given that the draft instrument did not contain agreed definitions of specific levels of reliability. It was also noted that defining specific levels of reliability was a time-consuming and challenging task. It was recalled that the term "substantial equivalence" was used in article 12 MLES.

71. It was explained that article 26 operated in conjunction with other provisions, namely articles 10, 11, 23 and 24 of the draft provisions. It was suggested that the following words should be inserted at the end of paragraph 2 to indicate the link between articles 24 and 26: "Equivalence shall be presumed if a person, organ or authority designated by the enacting jurisdiction according to article 24 has determined the equivalence for the purposes of this paragraph".

72. It was said that reference should be made in paragraph 2 to IdM systems since it was more appropriate to determine the properties of a system. Alternatively, it was said that paragraph 2 should refer to identity credentials as in practice those were recognized across borders. Yet another suggestion was to refer to IdM services. It was also suggested that reference to IdM in the title of the article should be aligned with the content of the article.

73. It was suggested that the word "State" should be replaced with the word "jurisdiction".

74. After discussion, the Working Group agreed to continue its deliberations on article 26 on the basis of a revised text incorporating the various drafting suggestions.

2. Article 27 – cooperation

75. It was emphasized that article 27 played an important role in implementing article 26, in particular by facilitating the definition of levels of assurance and levels of reliability that could support a determination of equivalence. After discussion, the Working Group agreed to retain article 27 as set out in A/CN.9/WG.IV/WP.162.

D. Chapter I – general provisions

1. Article 2 – scope of application

76. It was suggested that article 2(4) should refer to "data protection and privacy" (rather than "privacy and data protection") to acknowledge that the notion of privacy was limited to data and not concerned with privacy in other contexts.

77. In response to a query, it was explained that article 2(2)(a) clarified that the instrument did not establish any new obligation to identify, while article 3 clarified that the instrument did not establish any obligation to use an IdM service (or trust service). It was added that a similar provision on voluntary use was contained in article 8(2) ECC with respect to electronic communications.

78. It was recalled that support had been expressed for the draft instrument not to deal with the identification of objects, and that the Working Group had agreed to delete article 22 (see paras. 49-51). Accordingly, it was proposed that article 2(3) should be amended to refer only to a "person", and that similar amendment would need to be made to other provisions that offered the option to refer to "subject" or "person" (see also para. 138). The Working Group agreed to amend article 2(3) accordingly. No further amendments were agreed.

2. Article 3 – voluntary use of IdM and trust services

79. It was noted that the comments synthesized in A/CN.9/WG.IV/WP.164 expressed a variety of views on whether article 3(1) should be redrafted to refer to the voluntary acceptance of electronic identification and trust services. The view was expressed during the session that article 3 had a role to play in the draft instrument and should apply for the benefit of both the subscriber and the relying party.

80. The Working Group agreed to retain article 3 as contained in A/CN.9/WG.IV/WP.162.

3. Article 4 – interpretation

81. Article 4 did not elicit comments.

E. Chapter II – identity management

1. Article 5 – legal recognition of IdM

82. It was acknowledged that the scope of article 5 depended on the definitions of "identity proofing" and "electronic identification". It was also acknowledged that the

title of article 5 raised the same issue that had been discussed in relation to article 13 (see para. 17).

83. It was proposed that the words “Subject to article 2, paragraph 3,” should be inserted at the beginning of article 5. A question was raised as to the need for and desirability of doing so, given that (a) on its own terms, article 2(3) already qualified article 5 (and all other provisions of the draft instrument), and (b) by extension, the same words would need to be inserted in every other provision of the draft instrument. In response, it was noted that, unlike other provisions of the draft instrument, article 5 was susceptible to encroaching on the matters covered in article 2(3) (i.e., the legal requirements that a person be identified in accordance with a procedure defined or prescribed by law), and therefore that the insertion of the words in article 5 was justified.

84. After discussion, the Working Group agreed to insert the words “Subject to article 2, paragraph 3,”, or words to similar effect, at the beginning of article 5.

2. Article 6 – obligations of IdM service providers

85. The Working Group considered a proposal to amend article 6 in A/CN.9/WG.IV/WP.162 by:

(a) Including a new paragraph (a) that read “Have in place operational rules, procedures and practices to”;

(b) Recasting existing paragraphs (a) to (d) as subparagraphs (i) to (iv) of new paragraph (a); and

(c) Recasting existing paragraphs (e) and (f) as paragraphs (b) and (c).

86. It was explained that those amendments acknowledged that the functions listed in existing paragraphs (a) to (d) would ordinarily be governed by contract-based operating rules for private sector IdM systems.

87. It was observed that the suggested amendments could be interpreted as no longer establishing an obligation to perform those functions by making the functions optional at the choice of the IdM service provider according to what was regarded as the design of the IdM system. Accordingly, it was suggested to add an obligation for the IdM service provider to “act according to those operational rules, procedures and practices”. It was also suggested that article 6 should incorporate the obligation imposed on trust service providers in article 14(1)(a) to act in accordance with representations with respect to policies and practices.

88. It was noted that not all of the functions listed in article 6 may be relevant to all IdM systems and therefore that an IdM service provider might not perform each listed function. Accordingly, it was suggested that new paragraph (a) should refer to operational rules, procedures and practices “as appropriate to the structural design, technology and purpose of the IdM system, to address requirements”. It was also noted that the new paragraph (a) would make the words “as appropriate for the IdM service” and “according to the rules governing the IdM system” redundant.

89. Concern was expressed that the amendment to new paragraph (a) might jeopardize technology neutrality. It was therefore proposed to replace “structural design, technology and purpose” with “purpose and design”.

90. Concern was also expressed that the wording of the new paragraph (a) might allow an IdM service provider to disclaim responsibility for carrying out functions related to the IdM service that were carried out by a subcontractor on the provider’s behalf. It was observed that the draft provisions needed to ensure that the IdM service provider remained responsible for the full suite of IdM services provided to the subscriber. In response, it was explained that the intention of the amendment was to allow flexibility in system design and not to make compliance with obligations with respect to relevant functions optional. To address the concern, it was suggested that

the words “at a minimum” could be inserted in new paragraph (a) to qualify the requirements to be addressed.

91. It was recalled that article 6 did not prevent the service provider from outsourcing any of the listed functions under contract (see A/CN.9/1005, para. 89), or from allocating risk among its contractors.

92. As a general remark, it was observed that the functions listed in article 6 were too prescriptive, and that the Working Group should consider revising the list. With respect to the function of updating attributes (existing para. (b)), it was noted that it was ordinarily the role of the subscriber to update attributes, such that the function of the IdM system was rather to support the subscriber in doing so. It was proposed to amend the text accordingly.

93. A view was expressed that the obligation in existing paragraph (f) did not go far enough, and that the IdM service provider should provide information that was clear and comprehensible. In response, it was suggested that this concern might be addressed by recasting the paragraph in terms of article 14(1)(b).

94. It was noted that article 6 could be amended to include a new obligation to make available reasonable means for a subscriber to notify a security breach under article 8 (see also para. 21).

95. The Working Group agreed to continue its consideration of the draft provisions on the basis of the following revised article 6, bearing in mind (a) the importance of respecting technology neutrality, (b) the need to ensure that IdM service provider remained responsible for the overall operation of IdM system provided, and (c) the relevance of article 9 for the operation of other provisions in chapter II of A/CN.9/WG.IV/WP.162 that had not yet been discussed (particularly arts. 10–12):

“An IdM service provider shall [at a minimum]:

(a) Have in place operational rules, procedures and practices as appropriate to the purpose and design of the IdM system to address [at a minimum] requirements to:

(i) Enrol persons, including by:

a. Registering and collecting attributes;

b. Carrying out identity proofing and verification; and

c. Binding the identity credentials to the person;

(ii) Update attributes;

(iii) Manage identity credentials, including by:

a. Issuing, delivering and activating credentials;

b. Suspending, revoking and reactivating credentials; and

c. Renewing and replacing credentials;

(iv) Manage the electronic identification of persons, including by:

a. Managing electronic identification factors; and

b. Managing electronic identification mechanisms;

(b) Act according to the operational rules, procedures and practices;

(c) Ensure the online availability and correct operation of the IdM system;

(d) Provide reasonable access to the operational rules, procedures and practices; and

(e) Make available reasonable means for the subscriber to give notice pursuant to article 8.”

3. Article 7 – obligations of IdM service providers in case of data breach

96. It was suggested to reformulate article 7 to oblige the IdM service provider to "have in place operational rules, procedures and practices" to perform the actions listed in paragraphs 1 and 2. As a reason for that proposal, it was explained that such language would clarify that contractual agreements would be relevant for discharging the obligations under article 7, in line with the relevant language inserted in article 6. It was added that the article would set a minimum standard to be completed by contractual agreements. One delegation expressed strong support for the proposal.

97. However, other delegations expressed the view that, while the IdM service provider might not perform all of the functions listed in article 6 by virtue of the purpose and design of the IdM system, the actions listed in article 7 applied regardless of purpose and design of the IdM system. Accordingly, it was suggested that article 7 should not be reformulated. Broad support was expressed for that suggestion.

98. There was general agreement that contractual agreements could deal with those matters related to data breach that were not covered by privacy and data protection law of mandatory application. It was also said that article 6 recognized the possibility to have operational rules, procedures and practices dealing with data breaches.

99. It was indicated that several actions listed in article 7 could fall under privacy and data protection law, and that all actions listed should be performed "in accordance with applicable law" and not just the action listed in article 7(1)(c). It was recalled that article 2(4) explicitly preserved the operation of privacy and data protection law and that article 7 would effectively find application only in jurisdictions that did not have such law.

100. It was suggested that the notion of "significant breach" should be further clarified. It was also suggested that the word "potential" should be deleted.

101. After discussion, the Working Group decided to retain article 7 as set out in A/CN.9/WG.IV/WP.162.

4. Article 8 – obligations of subscribers

102. It was suggested that the chapeau of article 8 should be amended to oblige the subscriber to "make use of the means made available by the IdM service provider" under article 6 to notify the breach (see para. 94 above). A concern was raised that the amendment could have the effect of limiting the notification channels available to the subscriber, and it was therefore suggested to add a provision that the subscriber could notify using "other reasonable means" or by otherwise using reasonable efforts (see article 8(1)(b) MLES). Preference was expressed for the latter formulation.

103. It was suggested that the chapeau of article 8 should be replaced with: "The operational rules, procedures and practices shall require, at a minimum, that a subscriber notify the IdM service provider if". As a reason for this proposal, it was explained that, besides establishing minimum requirements for notification, the reformulation reflected the reality that notification requirements were ordinarily set out in a contract between the IdM service provider and subscriber. It was further noted that the reformulation could be used in article 7 both to establish minimum legal rules and to reflect the reality that those rules were typically set by contract. In response, some delegations took the view that the reformulation effectively shifted the obligation from the subscriber to the IdM service provider.

104. A concern was raised that paragraphs (a) and (b) imposed too high an expectation on the subscriber as to its knowledge of actual or potential security breaches. Several proposals were put forward to address that concern. First, it was proposed that both paragraphs should be amended so as to refer only to the subscriber's identity credentials. That proposal received broad support of the Working Group. Second, it was proposed that paragraph (b) should be deleted and instead that paragraph (a) should be amended so as to apply both if the subscriber "knows or reasonably should have known" that its identity had been compromised, and if the

subscriber had the requisite knowledge that the credentials "have been or may have been" compromised. In response, the Secretariat explained that paragraph (b) was based on article 8(1)(b)(ii) MLES and that that formulation might be easier to apply as it provided additional guidance. The Secretariat noted that it could be useful to use formulations in existing UNCITRAL texts as a means to promoting legal uniformity.

105. The Working Group agreed to continue its consideration of article 8 on the basis of the following text:

> "The subscriber shall utilize means made available by the IdM service provider pursuant to article 6, or otherwise use reasonable means, to notify the IdM service provider if:
>
> a. The subscriber knows that the subscriber's identity credentials have [or may have] been compromised; or
>
> [b. The circumstances known to the subscriber give rise to a substantial risk that the subscriber's identity credentials may have been compromised.]"

5. Article 9 – identification of a person using IdM

106. It was explained that article 9 aimed at providing a functional equivalence rule for identification in those cases where the law required identification but did not specify a procedure to identify, or where the parties agreed to identify. It was also explained that the functional equivalence rule would, in line with established principles in UNCITRAL texts, complement the rule on legal recognition set out in article 5. It was added that the instrument did not affect requirements to identify according to a specific method, as set out in article 2(3). Finally, it was said that the rule operated only when an offline equivalent existed, since the goal of the rule was to establish requirements for equivalence between offline and online identification.

107. It was indicated that option A for paragraph 1 better achieved the purpose of article 9 and was more closely aligned to the provisions on functional equivalence contained in the chapter of the instrument on trust services. Broad support was expressed for retaining that option.

108. It was suggested that the word "services" should be inserted after the word "IdM" in paragraph 1 to indicate that the rule referred to identity credentials and not to IdM systems or to identity itself.

109. It was also suggested that the words "Subject to article 2, paragraph 3," should be inserted at the beginning of paragraph 1 to emphasize that article 9 did not affect requirements to identify according to a specific procedure. Questions were again raised as to the need for and desirability of inserting those words (see para. 83).

110. It was recalled that article 9 as set out in A/CN.9/WG.IV/WP.160 had referred to laws requiring identification "in accordance with a certain method". It was further recalled that the Working Group had agreed to delete those words out of concern to avoid conflict with requirements to identify according to a specific procedure under national law (A/CN.9/1005, para. 97). It was explained that inserting now an explicit reference to article 2(3) would fully address that concern, and that therefore the Working Group should consider reinserting the words or words to similar effect.

111. It was added that, without those words, article 9 would be difficult to apply in practice. Scenarios were presented of physical-based identification requirements to verify not only a person's name but also the person's age or residence to determine eligibility for the sale of certain goods or services, or to identify a person based on a photograph, and it was observed that some identity credentials based on IdM systems that did not collect or verify those attributes would not satisfy such physical-based identification requirements. It was explained that, without correlating the attributes of an identity required to satisfy a physical-based identification requirement with the attributes contained in the identity credentials used for electronic identification, article 9 would be inadequate as a functional equivalence rule. It was also explained

that, the relevant requirement was not to use a particular procedure to identify the person, which was addressed in article 2(3), but to verify a person's identity including a particular attribute of that identity according to the physical-based identification requirement.

112. It was suggested that the concern might be addressed by inserting "electronic" before the first instance of "person". This suggestion was not supported by the Working Group, with the observation being made that article 9 would no longer establish requirements for equivalence between offline and online identification.

113. Alternatively, it was suggested that the concern might be addressed as part of determining the reliability of the IdM system used, and therefore that article 9(1) could make reference to a reliable method "with respect to article 10". Specifically, it was explained that, if the IdM system did not provide for a certain attribute, which was needed for a particular purpose, to be collected and verified, that system could be considered not reliable in the circumstances. In this line, the Working Group was reminded of the importance of acknowledging in the instrument that reliability was relative (see para. 56). There were however doubts as to whether reliability of an identity credential was concerned with the range of attributes asserted by the identity credential, as opposed to the reliability of processes by which those asserted attributes were collected and verified. It was also felt that the reference to article 10 was not necessary given that article 10 itself referred back to article 9.

114. It was observed that some of the scenarios presented involved a verification of attributes and not the verification of identity. For example, a requirement to verify a person's age before selling the person a lottery ticket did not involve the identification of the person. It was stressed that the Working Group should avoid confusing those two processes.

115. In response, it was proposed that article 9(1) should be amended by (a) inserting the words "for a particular purpose" after the first instance of "person", and (b) inserting the words "for that purpose" after the second instance of "person" to address the scenarios described in paragraph 2.

116. The proposal received some support from the Working Group. However, some queried the need to refer to "purpose" given that the notion of "identity" was defined with reference to "context", which in turn determined the attributes required for identification.

117. After discussion, the Working Group decided to retain option A of paragraph 1 in the following terms:

> "Subject to article 2(3), where a rule of law requires or permits the identification of a person [for a particular purpose], that rule is satisfied with respect to IdM services if a reliable method is used for the electronic identification of the person [for that purpose]."

6. Article 10 – factors relevant to determining reliability

118. It was indicated that article 10 and article 23 had elements in common. It was suggested that article 10 should be recast in view of revised article 23 (see para. 57). Accordingly, the Working Group agreed to (a) replace the words "rules governing the operation of the IdM system" with the words "operational rules, policies and practices of the IdM service provider", and (b) amend paragraph 1(d) to specify that any relevant agreement between the parties included any limitation on the purpose or value of the transactions for which the IdM service might be used.

119. The view was reiterated that reference to "recognized international standards and procedures" was inappropriate as those standards could not be easily identified and might not exist.

120. It was suggested that the words "the purpose for which identification is being used" should be inserted as a new item in paragraph 1. It was explained that those words would not only address the concerns relating to the qualification of the method

used according to article 9 (see para. 111 above), but also the fact that reliability was relative to the function pursued. Support was expressed for the suggestion. The Working Group decided to insert the words "the purpose for which identification is being used" as a new item in paragraph 1.

121. It was also indicated that paragraph 1(a) should be deleted in view of revised article 6 (see para. 95). In response, it was said that paragraph 1(a) referred to compliance with all obligations listed in article 6, while the reference to compliance with operational rules, procedures and practices was only in amended article 6(a) and (b).

122. Yet another suggestion was that the factors listed in article 10 should be aligned with those listed in article 23 by replacing the list in article 10(1)(b) with that contained in article 23(1) and by adding to that list the item "The maintenance of integrity and authenticity of identity". It was explained that that additional factor was the only item specific to IdM. In response to a query, it was said that reference to identity would comprise both data managed by IdM service providers and identity credentials.

123. It was suggested to delete paragraph 1(d) out of similar concerns to those raised with respect to article 23(1)(h) (see para. 54).

124. It was further suggested that the title of article 10 should be changed to "Requirements for determining reliability" or aligned with the title of article 23.

7. Article 11 – designation of reliable IdM systems

125. It was proposed that articles 10 and 11 should be revised to clarify the references therein to "recognized international standards and procedures" in line with the amendments made to articles 23 and 24 (see para. 61). The Working Group agreed with that proposal.

126. A query was raised as to whether article 11 should refer to "IdM services" rather than "IdM systems" since the IdM service provider provided an "IdM service" to the subscriber and not an "IdM system", just as article 24 referred to "trust services" rather than the systems supporting the trust services. In response, it was indicated that the notion of IdM system encompassed IdM services, and that designation should involve the broader notion. After discussion, the Working Group agreed to insert a reference to "[service]" beside the word "system" throughout article 11 for further consideration.

127. It was indicated that users may be informed that an IdM system is designated by means other than a published list and therefore that the obligation to publish a list of designated providers contained in paragraph 2(b) was not necessary. It was added that that obligation could violate technology neutrality. Different drafting suggestions were heard.

128. In response, it was said that lists of designated IdM systems were very useful to ensure transparency, including in the cross-border context. It was added that, while subscribers could be informed by other means, there were no other reliable means to provide information to relying parties than by making lists publicly available, and that that was acknowledged in widely-used technical standards such as ISO 17065. Some delegations insisted that, while reference to other means to inform was possible, it was essential to retain an obligation to publish a list of designated IdM systems.

129. After discussion, the Working Group agreed to insert the words "[or otherwise inform the public]" at the end of paragraph 2(b) for further consideration.

8. Article 12 – liability of IdM service provider

130. It was recalled that the comments synthesized in A/CN.9/WG.IV/WP.164 expressed a variety of views on the different treatment of designated IdM service providers in relation to liability. It was suggested during the session that article 12 should be revised along the lines of the amendments suggested to article 25 taking

into account the specific requirements of IdM. The view was reiterated that the draft instrument should include a presumption of fault for designated IdM systems. Support was expressed for the comment (reproduced in A/CN.9/WG.IV/WP.164 at letter (a) of issue 2 for article 12) that an IdM service provider should not be liable to a relying party if the damage was caused by reliance of the relying party on a compromised credential.

131. Noting the parallelism between articles 12 and 25, the Working Group agreed to revise article 12 to reflect the amendments agreed with respect to article 25 (see para. 66).

F. Definitions and terminology (article 1)

132. The Working Group turned to the definitions and terms defined in article 1.

1. "Authentication" and "electronic identification"

133. It was recalled that the comments synthesized in A/CN.9/WG.IV/WP.164 expressed a variety of views on the use of "authentication" in context of IdM and trust services.

134. Support was expressed during the session to use the term "authentication" in the context of IdM instead of "electronic identification". It was suggested that the definition of "authentication" in article 1(b) could be used if "object" was replaced with "person". An alternative suggestion was to use the definition of "electronic identification" in article 1(d). However, the view was also expressed that that definition was more apt to describe identity proofing than authentication. The view was also expressed that the term could be misinterpreted as applying to the entire IdM process.

135. In the context of trust services, it was noted that, in light of the decision of the Working Group to delete article 22 (see para. 51), the term "authentication" was only used in the provision on website authentication (article 21). It was added that the term "website authentication" was a term of art which did not benefit from the definition in article 1(b), and that therefore the definition should not be applied in the context of those services. Accordingly, it was suggested that the words "in the context of trust services" should be deleted from the definition.

136. After discussion, the Working Group agreed to place the definitions of "authentication" and "electronic identification" in square brackets for further consideration.

2. "Identity credentials"

137. It was suggested that, in light of the discussion about the role of purpose in applying the functional equivalence rule in article 9 (see paras. 110-116), the definition of "identity credentials" should be amended to insert at the end of the definition ", considering the purpose for which that credential is issued or used".

3. "Subject"

138. It was suggested that, in light of the decision to delete article 22 (see para. 51), article 1(k) (definition of "subject") should be deleted, and that "subject" should be replaced with "person" throughout the instrument. It was recalled that the word "person" included both physical and legal persons. The Working Group agreed with that suggestion.