United Nations A/CN.9/1005

General Assembly

Distr.: General
9 December 2019

Original: English

United Nations Commission on International Trade Law
Fifty-third session
New York, 6–17 July 2020

Report of Working Group IV (Electronic Commerce) on the work of its fifty-ninth session (Vienna, 25–29 November 2019)

Contents

V.19-11600 (E) 111219 121219

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 document A/CN.9/WG.IV/WP.159, paragraphs 6–17. Following the Working Group's recommendation (A/CN.9/936, para. 95), the Commission requested, at its fifty-first session (2018), the Working Group to conduct work on legal issues related to IdM and trust services with a view to preparing a text aimed at facilitating cross-border recognition of IdM and trust services.[1] Subsequently, at its fifty-second session (2019), the Commission noted that, at this stage of the project, the Working Group should work towards an instrument that could apply to both domestic and cross-border use of IdM and trust services, and that the outcome of the work had implications for matters beyond commercial transactions.[2]

II. Organization of the session

2. The Working Group, composed of all States members of the Commission, held its fifty-ninth session in Vienna from 25 to 29 November 2019. The session was attended by representatives of the following States members of the Working Group: Algeria, Argentina, Austria, Belgium, Brazil, Canada, Chile, China, Czechia, Dominican Republic, Ecuador, France, Germany, Ghana, Hungary, India, Indonesia, Iran (Islamic Republic of), Italy, Japan, Malaysia, Mexico, Nigeria, Peru, Poland, Republic of Korea, Romania, Russian Federation, Singapore, Spain, Switzerland, Thailand, Uganda, Ukraine, United Kingdom of Great Britain and Northern Ireland, United States of America, Venezuela (Bolivarian Republic of) and Viet Nam.

3. The session was also attended by observers from the following States: Bolivia (Plurinational State of), Burkina Faso, Democratic Republic of the Congo, El Salvador, Greece, Guatemala, Iraq, Kuwait, Mauritania, Qatar, Saudi Arabia, Serbia and Uruguay.

4. The session was also attended by observers from the European Union.

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

(a) *United Nations system*: United Nations High Commissioner for Refugees (UNHCR), United Nations Industrial Development Organization (UNIDO) and World Bank;

(b) *Intergovernmental organizations*: Caribbean Court of Justice (CCJ), Commonwealth Secretariat and Gulf Cooperation Council (GCC);

(c) *International non-governmental organizations*: Alumni Association of the Willem C. Vis International Commercial Arbitration Moot (MAA), European Law Students' Association (ELSA), Institute of Law and Technology – Masaryk University (ILT), International and Comparative Law Research Center (ICLRC), International Association of Young Lawyers (AIJA), International Union of Notaries (UINL), Law Association for Asia and the Pacific (LAWASIA) and Organisation internationale de la Francophonie (OIF).

6. The Working Group elected the following officers:

Chairperson: Ms. Giusella Dolores FINOCCHIARO (Italy)

Rapporteur: Mr. Paul KURUK (Ghana)

[1] *Official Records of the General Assembly, Seventy-third Session, Supplement No. 17* (A/73/17), para. 159.

[2] *Official Records of the General Assembly, Seventy-fourth Session, Supplement No. 17* (A/74/17), para. 172.

7. The Working Group had before it the following documents: (a) annotated provisional agenda (A/CN.9/WG.IV/WP.159); and (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.160).

8. The Working Group adopted the following agenda:

1. Opening of the session and scheduling of meetings.
2. Election of officers.
3. Adoption of the agenda.
4. Legal issues related to identity management and trust services.
5. Technical assistance and coordination.
6. Other business.
7. Adoption of the report.

III. Deliberations and decisions

9. The Working Group continued its consideration of legal issues related to IdM and trust services on the basis of the documents listed in paragraph 7 above. The deliberations and decisions of the Working Group on that topic are found in chapter IV of this report.

IV. Legal issues related to identity management and trust services

10. The Working Group was invited to continue its deliberations on the basis of the draft provisions contained in document A/CN.9/WG.IV/WP.160. The Working Group agreed to start by discussing issues relating to trust services (arts. 13 to 25) as well as the definitions relevant to trust services in article 1. The Working Group expressed satisfaction at the revised draft provisions as they provided a significant contribution to expedite the completion of its work.

A. Trust services

1. General considerations

11. It was explained that the structure of the provisions on trust services had been revised as follows in light of the deliberations of the Working Group at its fifty-eighth session (A/CN.9/971, paras. 108–153): article 13 contained a general provision on legal recognition of trust services; article 23 offered a general reliability standard with a non-geographic discrimination clause to facilitate cross-border recognition (“ex post approach”); article 24 provided a mechanism for the ex ante designation of reliable trust services (“ex ante approach”); article 25 dealt with liability of the trust service provider; and articles 16–22 set out the requirements of specific trust services.

12. Broad support was expressed for: (1) the instrument accommodating both an ex ante and ex post approach for determining the reliability of trust services; (2) attaching greater legal effects to trust services designated as reliable ex ante; and (3) those greater legal effects taking the form of a rebuttable presumption of reliability.

13. By way of general comment, it was said that the form of the instrument was likely to influence how some of the provisions might be formulated. The Working Group agreed to postpone its discussion on the form of the instrument (for a preliminary discussion on form, see para. 123 below). It was also said that, while it was desirable to keep in full consideration existing UNCITRAL texts on electronic

commerce, it was equally desirable to verify whether concepts and provisions in those texts were relevant to the current work and whether they required adaptation in light of subsequent technological developments. It was added that additional guidance was desirable with respect to the relationship of the draft instrument with regulatory requirements as well as with contractual agreements. It was suggested that additional definitions, such as that of the notion of "authentication", could be inserted in the document (for further discussion on the notion of "authentication", see paras. 84 to 86 and 92 below).

2. Definition of "trust service"

14. The Working Group considered the definition of "trust service" contained in article 1(k) as set out in document A/CN.9/WG.IV/WP.160.

15. It was indicated that the definition did not provide adequate guidance and that therefore an approach similar to that taken in article 3(16) of the EU regulation on electronic identification and trust services ("eIDAS Regulation") [3] should be followed. In that line, it was suggested that a list of trust services should be included in the definition. It was added that the list should not be exhaustive.

16. The view was also expressed that a more precise definition of "trust service" was not desirable given the broad nature of the instrument. It was added that a more abstract definition could better accommodate future developments, and that specific examples of trust services were already identified in the instrument.

17. The view was expressed that the definition of "trust service" should not refer to "a certain level of reliability" as this could imply the exclusion of trust services offering a lower level of reliability. In response, it was indicated that the definition did not require a minimum level of reliability for a trust service. As an alternative, it was suggested that an abstract definition could refer instead to the "veracity and genuineness" of data.

18. After discussion, the Working Group agreed that a non-exhaustive list of trust services should be included in the current definition of "trust service" by making reference to articles 16–22.

3. Article 13. Legal recognition of trust services

19. The Working Group considered article 13 as set out in document A/CN.9/WG.IV/WP.160.

20. With respect to paragraph 1, it was indicated that the word "data" was more precise and capable of being legally defined. It was added that "data" and "data message" were terms already used in UNCITRAL texts on electronic commerce. It was therefore suggested that the word "data" should be retained. Conversely, the view was expressed that the word "information" was preferable as it was more generic and included data.

21. Support was expressed for the deletion of the phrase "that meets the requirements of [this chapter]" in paragraph 1.

22. It was suggested that the phrase "or admissibility as evidence" be retained to take into account fully the importance of giving evidentiary value to trust services. In that respect, it was noted that the evidentiary value of trust services provided by service providers that were designated when providing such service, but subsequently lost their designation, was unclear.

23. It was indicated that paragraph 2 was similar in content to article 3, paragraph 1 and should therefore be deleted to avoid repetition. In response, it was explained that paragraph 2 focused on technology neutrality while article 3,

[3] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

paragraph 1 dealt with the voluntary use of trust service, and therefore the two served different purposes.

24. With respect to paragraph 3, views were expressed in favour of maintaining the phrase “including any rule of law applicable to privacy and data protection” given the prominence of that subject matter. It was emphasized that the instrument should in general avoid matters dealing with substantive law and should not modify existing legal requirements under national law.

25. The question was asked whether a provision similar to that contained in article 5, paragraph 4 and dealing with legal requirements to use certain trust services should be inserted in article 13.

26. After discussion, the Working Group agreed that: (1) the word “data” should be retained without square brackets and the reference to “information” should be deleted; (2) the phrase “that meets the requirements of [this chapter]” should be deleted; (3) the phrase “or admissibility as evidence” should be retained without square brackets; and (4) the reference in paragraph 3 to privacy and data protection should be retained without square brackets.

4. Article 14. Obligations of trust service providers

27. It was suggested that a complete discussion on article 14 should take into account the link with article 25, which addressed liability for non-compliance with the obligations in article 14.

(a) Paragraph 1 – availability and correct operation of trust services

28. Several concerns were expressed with regards to article 14(1). First, it was suggested that the “availability” of trust services was primarily a matter for the contractual relationship between the trust service provider and the subscriber of the trust service. It was explained that, while the continuous availability of certain trust services was desirable, it was not appropriate to require this of all trust services. Second, it was queried what was meant by the term “correct” operation, and whether this invoked the policies of the trust service provider or some other standard of conduct.

29. It was suggested that, as an alternative, article 14(1) should require the trust service provider: (1) to have policies in place based on a risk analysis; (2) to make those policies available to subscribers; and (3) to provide trust services in accordance with those policies. It was added that this approach reflected the principle of transparency (see A/CN.9/936, para. 88). In response, it was suggested that it might not be helpful to refer to risk analyses.

30. It was also noted that article 9(1)(a) of the UNCITRAL Model Law on Electronic Signatures (MLES)[4] required a certification service provider to “act in accordance with representations made by it with respect to its policies and practices”. It was added that the reference to “representations” in that provision presupposed some degree of transparency on the part of the service provider. In response, it was queried whether article 9(1)(a) MLES was an appropriate formulation for a provision that applied to all trust services, not just those related to electronic signatures. It was also noted that, since the conclusion of the MLES, there had been a trend toward imposing greater obligations on trust service providers. In line with this trend, it was suggested that the instrument could include an obligation for the trust service provider to act diligently.

31. After discussion, the Working Group agreed to continue its consideration of article 14 on the basis of the following redraft:

> “The trust service provider shall act in accordance with representations made by it with respect to its policies and practices.”

(See also paragraph 73 below.)

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

(b) Paragraphs 2 and 3 – security breaches

32. There was general agreement that the instrument should deal with security breaches, while remaining mindful of possible intersections with existing legislation dealing with privacy and data protection. The Working Group also agreed that "significant impact" was an appropriate trigger for the obligations in paragraphs 2 and 3.

33. With regard to paragraph 2(a), it was suggested that it might not always be the most appropriate course of action for a trust service provider to "suspend" the affected services. It was noted that a partial suspension might be more appropriate in some circumstances. The Working Group agreed to reformulate the paragraph to oblige the trust service provider to "take all reasonable steps", which might include suspension or revocation.

34. With regard to paragraph 3, some queries were raised as to the meaning of "oversight authority". It was also noted that it might not be possible for the trust service provider to identify all relying parties affected by a security breach. It was therefore suggested that, instead of identifying the persons whom the trust service provider was to notify, the instrument should defer to applicable law.

35. It was suggested that the trust service provider could be obliged to publish information on the security breach. In response, it was noted that it might not be desirable to publicize this information as this might facilitate additional breaches. It was therefore suggested to defer to applicable law to determine what information, if any, needed to be published.

36. The Working Group agreed to reformulate paragraph 3 so as to defer to applicable law on matters such as (a) who needs to be notified, and (b) how notification is to be made.

5. Article 15. Obligations of trust service users in case of data breach

37. It was noted that, while the heading of article 15 referred to "data breaches", that term was not used in the text of the provision, which instead referred to the trust service being "compromised". It was suggested that the provision could instead refer to the reliability of the trust service being affected.

38. It was pointed out that, whereas article 8 (discussed in paras. 95 and 96 below) imposed an obligation on "subjects" and "relying parties" in the case of a data breach, article 15 imposed an obligation on "users". A question was raised as to whether the term "user" was intended to cover subscribers and relying parties. It was noted that the term "user" was defined in document A/CN.9/WG.IV/WP.150 (para. 61), and it was suggested that the instrument should define the term.

39. The view was expressed that, as it was in a contractual relationship with the trust service provider, the obligation in article 15 should be imposed on the subscriber and not on a relying party. It was added that an obligation imposed on a relying party might not be enforceable.

40. Alternatively, it was suggested that the obligation should apply to both subscribers and relying parties, and that the term "user" should encompass both. It was added that "employers" should also be included. It was explained that relying parties could be held liable on an extracontractual basis.

41. A concern was raised that paragraph (b) imposed an unreasonably high expectation on users. It was said that users might not have sufficient technical expertise to know whether data was compromised, and therefore that the obligation to notify the security breach to the trust service provider had been triggered. Accordingly, it was suggested that paragraph (b) should refer to circumstances known to the user that "give rise to a justified doubt as to whether the trust service works appropriately".

42. A question was raised as to the meaning of the term “trust service creation data”. It was indicated that, while this term might find application for electronic signatures, it might not find application for other trust services. As an alternative, it was suggested that article 15 might instead refer to “trust service”.

43. After discussion, the Working Group agreed: (1) to replace the words “trust service creation data” with “trust service”; and (2) to defer further consideration of article 15 until after it had discussed the interaction of that article with the trust services in articles 16 to 22. (For further decisions on article 15, taken in the context of discussions on art. 8, see para. 96 below.)

6. Article 16. Electronic signatures

44. It was suggested that article 16 needed to establish a clearer link to articles 23 and 24. In that line, a redraft of article 16, to be used as a template for other articles on trust services, was suggested as follows:

> “Where a rule of law requires or permits a signature of a person:
>
> (a) That rule is presumed satisfied in relation to a data message if a method designated as reliable according to article 24 is used to identify the person and to indicate the person’s intention in respect of the information contained in the data message; and
>
> (b) That rule may be satisfied in relation to a data message if a method considered reliable according to article 23 is used to identify the person and to indicate the person’s intention in respect of the information contained in the data message.”

45. Support was expressed for the suggested redraft, noting that it promoted legal clarity and predictability. It was added that the redraft also clarified the allocation of burden of proof.

46. In response, it was indicated that the current draft already provided sufficient clarity on that issue as articles 23 and 24 contained cross-references to articles 16–22. It was noted that footnote 53 in document A/CN.9/WG.IV/WP.160 further clarified the link between those articles. It was also noted that, as a matter of drafting, the provision should set out first the standard rule and then the presumption. It was also said that the reference to “may be satisfied” in paragraph (b) of the proposed draft needed to be clarified. As a result, it was suggested that article 16 should be retained without amendment. Yet another proposal was to insert the words “according to either article 23 or article 24” after the words “reliable method” in article 16. Each proposal received some support.

47. It was suggested that a second paragraph should be inserted in article 16 in the following terms: “A method is presumed to meet the requirements in paragraph 1 if it is designated according to article 24”. It was also suggested that, for the avoidance of doubt, a third paragraph should be inserted to ensure that the suggested second paragraph did not limit the ability of any person to establish in any other way the reliability of a method or to adduce evidence of the non-reliability of a designated method, along the lines of article 24, paragraph 5. Support was expressed for this suggestion.

48. It was noted that the current draft provided an option for the signatures of “subjects”, which was defined in article 1(j) to include objects. It was explained that, while objects could generate electronic signatures, they should not be considered signatories. Accordingly, it was suggested that the words “of a subject” should be deleted. It was also suggested that only natural persons could be signatories. However, it was pointed out that legal persons could also use electronic signatures and therefore should not be excluded from the scope of article 16.

49. It was indicated that the phrase “in relation to a data message” should be retained given that subparagraph (b) referred to information contained in a data message. However, it was also indicated that the use of a reliable method to identify the

person's intention was sufficient and that article 16 should contain no reference to data messages.

50. One concern was expressed that the signed information might be subsequently altered, and that therefore the intention indicated by a reliable method should only relate to the information existing at the time of signature. In this respect, it was noted that draft article 19 dealt with the notion of integrity.

51. After discussion, the Working Group agreed that: (1) two new paragraphs should be inserted in draft articles 16–22 to reflect the suggestions made in paragraph 47 above; (2) the words "of a person" should be retained in draft article 16 without square brackets and the reference to "of a subject" should be deleted; and (3) the phrase "in relation to a data message" should be retained in draft article 16 without square brackets.

7. Article 17. Electronic seals

52. The Working Group considered article 17 as set out in document A/CN.9/WG.IV/WP.160. Reference was made to the eIDAS Regulation, which defined electronic seals as a mechanism to ensure the "origin and integrity" of data, and defined the creator of a seal as a "legal person". It was suggested that article 17 should similarly focus on the "origin" of data, instead of the identity of the person affixing the seal, and that paragraph (a) should be recast accordingly. In response, it was observed that origin and identity essentially served the same purpose, i.e., to establish the provenance of the data. It was also suggested that article 17 should be limited to seals affixed by legal persons, on the understanding that article 16 applied to electronic signatures applied by both natural and legal persons.

53. A query was raised as to the notion of "affixing a seal", which might not necessarily relate to identifying the source of the data and to ensuring data integrity. Another query related to the possible impact on national law of limiting the use of electronic seals to legal persons.

54. After discussion, the Working Group agreed to insert to word "legal" before "person" in the chapeau of article 17, and to replace paragraph (a) with a reference to the origin of the data. It also agreed to retain the words "in relation to a data message" without square brackets. After further discussion, the Working Group agreed that assuring integrity was an essential component of electronic seals. It agreed to retain paragraph (b) but to revisit its drafting after consideration of article 19 (see paras. 56 to 58 below).

8. Article 18. Electronic timestamps

55. The Working Group considered article 18 as set out in document A/CN.9/WG.IV/WP.160. The Working Group agreed to retain the provision in its current form without square brackets.

9. Article 19. Assurance of integrity

56. The Working Group considered article 19 as set out in document A/CN.9/WG.IV/WP.160. It was observed that article 19 did not define a trust service but instead defined a component of some trust services, i.e., integrity. While there was agreement that article 19 expressed the notion of integrity in appropriate terms, there was broad support for omitting the provision and incorporating its content into provisions that defined trust services for which integrity was an essential component, or in a definition of "integrity". In this regard, it was noted that integrity was an essential component of electronic seals (art. 18) and electronic archiving (art. 20), while it was an optional component of other trust services.

57. It was stressed that the draft instrument should continue to make allowance for "the addition of any endorsement and any change that arises in the normal course of communication, storage and display". It was added that this text accommodated file migration and format changes that were part of ordinary data retention practices.

58. The Working Group agreed to omit article 19 and to reflect its content in articles 18 and 20.

10. Article 20. Electronic archiving

59. The Working Group's deliberations on article 20 focused predominantly on integrity as an essential component of electronic archiving. It was recalled that the text of article 20 was modelled on article 10 of the UNCITRAL Model Law on Electronic Commerce (MLEC),[5] which did not refer to the notion of integrity as formulated in article 19 of the present draft. Two options were put forward to revise article 20. The first option was for paragraph (b) to refer to the data message being retained in "original form" (see art. 8 MLEC) and to define "original" based on the elements contained in article 19. The second option was for paragraph (b) to be replaced with the language used in article 17(b), adapted so as to refer to the detection of any alteration after "archiving".

60. There was broad support for the second option, with a preference expressed for the instrument not to refer to originality, which could create confusion as it was a notion closely related to the use of paper. Accordingly, the Working Group agreed to recast paragraph (b) of article 20 so as to refer to the use of a reliable method to detect any alteration to the data message after its archiving, with allowance for the addition of any endorsement or change that arose in the normal course of communication, storage and display.

61. In response to a query, it was noted that article 20 was subject to article 13(3) and therefore did not pre-empt any rule applicable to privacy and data protection (for a discussion of this provision, see paras. 24 and 26 above).

11. Article 21. Electronic registered delivery services

62. The Working Group considered article 21 as set out in document A/CN.9/WG.IV/WP.160. Difficulties were identified with respect to the term "information system". It was noted that the term was imprecise, and a suggestion was made to replace it with "electronic address" as used in article 10 of the United Nations Convention of the Use of Electronic Communications in International Contracts (ECC).[6] It was explained that reference to electronic address would allow the instrument to deal with messages exchanged within the same information system.

63. In response, it was pointed out that the term "electronic address" was only used in the ECC to refer to the addressee of a data message – not the originator – while the term "information system" was used in other UNCITRAL texts on electronic commerce. It was also noted that, in practice, an electronic registered delivery service recorded the time at which the data message left or entered a particular delivery system, and an alternative suggestion was made to replace the term "information system" with "delivery system".

64. A suggestion was made that more appropriate language could be formulated by focusing on the functional equivalence between registered mail services and electronic registered delivery services. In this spirit, it was suggested that article 21 should refer to a reliable method for providing assurance "of the time at which the data message was received for delivery by the electronic registered delivery service and the time at which the data message was delivered by that system to the addressee". Broad support was expressed for this suggestion and the Working Group agreed to redraft article 21 accordingly.

12. Article 22. Website authentication

65. The Working Group engaged in a discussion about the function of website authentication. Reference was made to recital 67 of the eIDAS Regulation. With

[5] United Nations publication, Sales No. E.99.V.4.

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

respect to the reference to website "ownership", it was observed that website authentication services did not establish a link between the website and the website owner. Noting that Annex IV of the eIDAS Regulation referred to an indication of the domain name operator as a component of website authentication, it was suggested that the instrument should instead require a link between the website and the website operator. Alternatively, it was said that the instrument should require a link between the website and the person to whom the website certification was issued. The question was asked how article 22 would apply if the domain name was used to operate a web platform that allowed different persons to upload content and create their own web pages under the same top-level domain name.

66. After further discussion, it was suggested that it would be more accurate for the instrument to require a link between the website and the person to whom the domain name had been assigned or licensed as this better reflected the function of website authentication. The Working Group agreed to amend article 22 accordingly.

13. Article 23. Reliability standard for trust services

67. It was suggested that the chapeau of article 23 should be aligned with the chapeau of article 10. It was also suggested that a reference to articles 16–22 should be included in the chapeau to ensure a clearer link with these articles. After discussion, the Working Group agreed that the chapeau should be revised along the following lines: "In determining the reliability of the method for the purposes of articles 16–22, all relevant circumstances shall be taken into account, which may include:".

68. With respect to the non-exhaustive list of factors for determining reliability as set out in subparagraph 1(a), it was suggested: (1) to insert words such as "including any plan for the termination of activity in order to ensure continuity" at the end of item (i); and (2) to insert a new item referring to "any applicable recognized international standards and procedures". The Working Group agreed to amend article 23 accordingly.

14. Article 24. Designation of reliable trust services

69. It was explained that the focus of the designation should be trust services, rather than the methods used, on the understanding that the process for designating trust services necessarily involved an assessment of those methods. Accordingly, it was suggested that the term "methods" should be deleted in favour of the term "trust services". A query was raised as to whether the designation of reliable trust services might be inconsistent with the use of the term "reliable method" in articles 16–22. In response, it was said that a reliable method should be used when providing the trust service. It was also explained that the designation did not pertain to generic types of trust service or to all the trust services offered by a specific trust service provider, but rather to a specific trust service provided by an identified service provider.

70. It was suggested that paragraph 1 should include an obligation to publish a list of designated trust services to promote transparency and inform potential subscribers. Another suggestion related to transparency was to refer – either in article 23 or in article 24 – to the ease of accessing operational rules governing the trust service. While there was general support for promoting transparency, doubts were raised as to whether access to the operational rules was relevant to determining reliability. It was therefore said that the reference should be placed in article 14 on the obligations of trust service providers.

71. With respect to the relationship between articles 23 and 24, it was indicated that the factors listed in article 23(1)(a) were to be taken into account in designating a trust service. Accordingly, it was suggested that a reference to article 23(1)(a) should be included in article 24(1).

72. It was indicated that paragraphs 4 and 5 should be deleted in light of the decision of the Working Group to introduce similar provisions in articles 16–22 (see paras. 47 and 51 above), which made the paragraphs in article 24 redundant.

73. After discussion, the Working Group agreed that: (1) the words "trust services" should be retained without square brackets and the word "methods" should be deleted; (2) paragraph 1 should be redrafted to include reference to the factors listed in article 23(1)(a); (3) a new sentence should be inserted in paragraph 1 to establish an obligation to publish a list of designated trust services; and (4) paragraphs 4 and 5 should be deleted. The Working Group also agreed that a new sentence should be inserted at the end of article 14(1), along the following lines: "These policies and practices shall be made easily accessible to subscribers".

15. Article 25. Liability of trust service providers

74. The importance of dealing with liability issues was emphasized. It was noted that article 25 aimed at providing common rules that would facilitate the use of trust services, especially across borders. In that respect, the question was asked whether the draft instrument should establish stand-alone liability rules, and, if so, what the relationship was between those rules and the liability regime under existing laws on the one hand, and contractual agreements on the other, bearing in mind article 13(3) of the draft instrument. It was pointed out that the final form of the draft instrument was relevant for answering these questions. Reference was made to the deliberations of the Working Group at its fifty-eighth session on the liability of IdM services operators (A/CN.9/971, paras. 98–107).

75. There was general support for retaining a provision on liability in the draft instrument so as to provide legal certainty, but different proposals were put forward. One suggestion was to retain paragraph 1 and refer to the application of national rules on liability along the lines of article 11(4) of the eIDAS Regulation. Another suggestion was to replace article 25 with a provision along the lines of article 9(2) MLES, which provided for a service provider bearing the legal consequence of the failure to satisfy certain legal requirements. It was noted, however, that such an avenue would not provide a minimum standard of liability, and that the reference to bearing legal consequences might go beyond the issue of liability. Yet another suggestion was to replace article 25 with a provision along the following lines: "Liability of trust service providers will be determined according to applicable law". Each proposal received some support. After discussion, the Working Group requested the Secretariat to redraft article 25 to reflect the proposals described above for future consideration.

76. Concerns were expressed with respect to the reference in paragraph 2(b) to "reasonably accessible means" to ascertain the limitations of a trust service. It was explained that that provision was not intended to override more stringent notice requirements under other law. In response, it was indicated that ascertaining such requirements under foreign law might be challenging. It was suggested that explicit reference to an obligation under applicable law to notify should be included.

B. Identity management (IdM)

1. General considerations

77. It was explained that chapter II of the draft instrument on IdM followed the same structure as chapter III on trust services. The Working Group was invited to consider whether the amendments that it had agreed to make to the provisions of chapter III would apply – with necessary modifications – to the corresponding provisions of chapter II.

78. As a general comment, it was noted that several provisions of chapter II were modelled on the MLES. It was queried whether the MLES offered an appropriate model for an instrument dealing with IdM, based on an observation that there was

greater standardisation among electronic signatures than among IdM systems. In response, it was indicated that, while chapter III of the draft instrument was more directly influenced by the MLES, chapter II was based on the fundamental principles underlying UNCITRAL texts on electronic commerce. It was questioned whether and to what extent the specific features of IdM warranted a departure from these principles.

2. Article 5. Legal recognition of IdM

(a) Paragraph 1 – non-discrimination

79. It was recalled that article 5(1) enshrined the principle of non-discrimination against the use of electronic means, which was first formulated in article 5 MLEC. It was suggested that article 5(1) – as well as the other paragraphs of article 5 – should be recast in positive terms so as to state what the instrument did rather than what it did not do. In response, it was noted that article 5(1) adopted a well-settled formulation of the principle, and that compelling reasons would be needed to depart from that formulation.

80. The Working Group engaged in detailed discussions about: (1) the subject of the non-discrimination provision as identified in the chapeau of article 5(1); and (2) the prohibited grounds for discrimination as set out in paragraph 1(a).

81. With regards to (1), several proposals were put forward. It was suggested that the chapeau should refer to "the use of identity credentials produced by an IdM service". It was added that the reference to "produced by an IdM service" might be unnecessary if the connection between the credentials and the IdM system were established in the definition of "identity credentials" in article 1(e). Another suggestion was to refer to "the use of IdM services", which was understood to include the use of identity credentials. It was added that the term "IdM service" was preferable to "IdM system". Both proposals received some support.

82. With regards to (2), it was explained to the Working Group that the "results of the verification of identity" referred to in paragraph 1(a) referred to matching the person to the identity credential used by the person. It was noted that this matching could be regarded as "identification", while article 1(c) of the draft defined "identification" to cover a much broader range of processes including the collection of identity attributes to produce identity credentials (see also para. 84 below). Several proposals were put forward to amend paragraph 1(a). It was suggested that the paragraph should refer to the "results of the verification of identity produced by the IdM service". Another suggestion was to refer to "the IdM system". Both proposals received some support. Other suggestions were to refer to the "confirmation or otherwise of credentials" or to "identification carried out using identity credentials".

83. The Working Group was invited to consider these proposals for later discussion. In this regard, it was suggested that the equivalent provision on trust services in article 13 might provide guidance on the formulation of paragraph 1(a) insofar as the corresponding provision in article 13(a) was concerned with "data". It was also suggested that the Working Group should focus on identifying which legal effects needed to be protected, which in turn might provide guidance on the formulation of the chapeau of article 5(1). In this line, it was suggested that article 5(1) should be drafted along the following lines:

> "The results of the verification of identity shall not be denied legal effect, validity, enforceability or admissibility as evidence on the sole ground that the IdM system used is in electronic form or is not designated pursuant to article 11."

84. It was suggested that the same effect could be achieved by using the term "identification" in both instances, while also expanding the definition of "identification" to include "the results of the verification of identity". It was noted that article 1(c) defined "identification" in terms that included the enrolment stage of identity management but excluded the "authentication" or "verification" stage. It was

explained that this definition reflected a technical understanding of “identification”, and it was advocated that the instrument should encompass a broader understanding of the term that included “authentication” or “verification”.

85. It was acknowledged that the instrument should define the term “verification”. It was suggested to define “verification” as a process or instance of establishing authenticity (see A/CN.9/WG.IV/WP.150, para. 63). There was broad support for the view that, in the context of article 5, “verification” was synonymous with “authentication”. At the same time, it was noted that the notion of authentication was referred to in other provisions of the draft instrument, and that care should be exercised to ensure that the term was used consistently in all instances in the instrument.

86. After discussion, the Working Group agreed: (1) to amend article 5(1) along the following lines: “The verification of identity shall not be denied legal effect, validity, enforceability or admissibility as evidence on the sole ground that: (a) the identification and verification are in electronic form; or (b) the IdM system is not designated pursuant to article 11”; and (2) to ask the Secretariat to ensure that the notions of authentication, identification and verification were used consistently through the instrument, as well as consistently with terminology adopted by the International Telecommunication Union (ITU).

(b) Paragraph 3 – rules of law applicable to privacy and data protection

87. Referring to its earlier discussions on article 13(3) (see paras. 24 and 26 above), the Working Group agreed to retain the reference to privacy and data protection without square brackets.

(c) Paragraph 4 – legal requirements to identify according to a particular procedure

88. It was recalled that paragraph 4 had been inserted to address a concern raised at the fifty-eighth session (A/CN.9/971, para. 30). Support was expressed for retaining the provision, although a concern was raised that article 9 might be read to limit the effect of paragraph 4. The example was given of a legal requirement to use a particular IdM system that would not be reliable for the purposes of article 9. In response, it was noted that article 9 was not designed to displace that requirement. It was suggested that this could be clarified by refocussing article 9 on circumstances in which the law permitted the parties to use – or the parties had agreed to use – an IdM service to identify one another, rather than a legal requirement to identify.

3. Article 6. Obligations of IdM service providers

89. The Working Group was reminded that article 6 as set out in document A/CN.9/WG.IV/WP.160 had been developed in consultation with experts following a request by the Working Group at its last session (A/CN.9/971, para. 67). The Working Group was asked to consider whether the list of obligations in article 6 was complete and accurate. It was noted that the list should not prevent an IdM service provider from outsourcing some of the obligations.

90. A proposal was made to modify subparagraph (a)(i) so as to require only the IdM service provider to register and collect attributes “as appropriate for the service”. It was added that this proposal gave effect to the principle of data minimization. In response, it was noted that data minimization was a greater concern when using identity credentials in the context of the provision of services for which identification was required rather than for collecting identity attributes.

91. A question was raised as to whether paragraph (e), which required the IdM service provider to ensure the online availability and correct operation of the IdM system, needed to be revisited in light of the Working Group’s earlier discussions on article 14(1) (see paras. 28 to 31 above).

92. It was suggested that some of the terms used in article 6 should be defined, including “authenticate”, “authentication factors”, “authentication mechanisms” and

"rules governing the IdM system". In response, it was noted that definitions for some of these terms were already provided in document A/CN.9/WG.IV/WP.150. The Working Group was invited to consider whether some of those definitions could be used. It was also pointed out that the term "authentication" was not included in the definition of "identification", which was in turn used to define the scope of "IdM services" provided by an IdM service provider (see also para. 84 above).

93. After discussion, the Working Group agreed to amend subparagraph (a)(i) to give effect to the principle of data minimization.

4. Article 7. Obligations of IdM service providers in case of data breach

94. Referring to its earlier discussions on articles 14(2) and 14(3) (see paras. 32 to 36 above), and stressing the desirability of keeping a consistent approach to similar issues in the draft instrument, the Working Group agreed: (1) to keep the term "significant" without square brackets; and (2) to reformulate article 7 along the lines of revised articles 14(2) and 14(3).

5. Article 8. Obligations of subjects and relying parties

95. The question was asked as to whether it would be feasible to impose a notification requirement on a relying party. It was explained that the relying party did not enter into any contractual arrangement with the IdM service provider and might not even be aware of its existence. For these reasons, it was added, imposing obligations on relying parties, while in theory possible, was impractical. Reference was also made to the discussion of article 15 (see paras. 38 to 40 above). Views were expressed in favour of removing such an obligation. However, it was observed that article 11 MLES already imposed obligations on the relying party. In response, it was said that the obligation contained in article 11 MLES was to verify information to which the relying party had access rather than to notify a party possibly unknown to the relying party.

96. After discussion, the Working Group agreed to align article 8 with article 15. Accordingly, it also agreed that: (1) article 8(1) and 8(3) should be deleted; and (2) both article 8(2) and article 15 should refer to "subscribers" and exclude "relying party" from their scope.

6. Article 9. Identification using IdM systems

97. It was suggested that article 9 should be redrafted to cover circumstances in which the parties had agreed to use an IdM service to identify one another, rather than a legal requirement to identify. It was also suggested that the phrase "in accordance with a certain [method][policy]" should be deleted to avoid any potential conflict with national law requirements. Another suggestion was to refer to a requirement to use specific identity credentials so as to promote the use of IdM services offering the same level of security.

98. The Working Group considered a revised draft of article 9 as follows:

> "Where a rule of law requires or permits the identification of a subject, that rule is satisfied with respect to IdM if a reliable method is used to identify the subject."

99. In response to a query, it was explained that the term "permits" was used in UNCITRAL texts to cover those circumstances where the law provided a space in which the parties could agree to identify one another. It was suggested that article 9, as drafted in paragraph 98 above, should be recast along the lines of article 16, as revised (see para. 51 above). The Working Group agreed with that suggestion.

100. The concern that article 9 might be read to limit the effect of article 5(4) was recalled (see para. 88 above). It was indicated that, with the agreed amendments to article 9, article 5(4) could be deleted. However, it was also indicated that article 5(4) still served a useful purpose and should be retained. It was suggested that the content

of article 5(4) could be moved to article 9 to emphasize the close relationship between the two provisions. Alternatively, it was suggested that article 5(4) could be recast as a stand-alone provision, or that it could be moved to article 2 on scope of application. After discussion, the Working Group agreed to retain article 5(4) and asked the Secretariat to draft proposals for relocating the provision.

7. Article 10. Factors relevant to determining reliability

101. In keeping with its previous deliberations (see para. 67 above), the Working Group agreed to retain the word "method" without square brackets and to delete the words "IdM system".

8. Article 11. Designation of reliable IdM systems

102. The importance of referring to "level of assurance frameworks" in determining reliability of IdM systems was emphasized. It was noted that, in certain jurisdictions, there was no authority to designate IdM services. It was also noted that the provision should be compatible with the various presumptions under the rules of evidence. After discussion, the Working Group agreed to reformulate article 11 along the lines of article 24 (see para. 73 above).

9. Article 12. Liability of IdM service provider

103. It was recalled that paragraph 3 was intended to function as a safe harbour provision that excluded the liability of IdM service providers under certain conditions. A question was raised as to whether a safe harbour provision was justified, given that it did not exist for trust service providers. It was also said that the formulation of paragraph 3 relied on subjective determinations that did not promote legal predictability and could foster litigation.

104. A query was raised as to why paragraph 3 applied only to designated IdM service providers. In response, it was said that the challenges arising from the application of such a safe harbour provision, absent an ex ante determination of reliability, would affect legal predictability. After discussion, the Working Group agreed that paragraphs 3 and 4 should be deleted.

105. Another query was raised as to the liability of designating entities. It was explained that those entities were often accredited under standard ISO/IEC 17065:2012 entitled "Conformity assessment – Requirements for bodies certifying products, processes and services", which contained relevant provisions.

106. The Working Group agreed that paragraph 1 and paragraph 2 should be reconsidered at its next session in conjunction with article 25 on the liability of trust service providers.

C. Definitions

1. Definition of "identification"

107. The Working Group agreed that the reference to "specific context" should be replaced with "particular context", and that the term "particular" should be used to describe "context" in other definitions (cf. paragraphs (d), (e), (f) and (j)).

2. Definition of "identity"

108. With reference to the different options presented, some support was expressed for defining "identity" in terms of "distinguishing" the subject, while there was equally support for doing so in terms of "defining" the subject. There was general agreement that a requirement of "uniqueness" should be included in the definition. It was also suggested that the "sufficiency" of distinguishing the subject was more relevant to the reliability of the IdM system – addressed in article 10 – than to the

definition of “identity”. After discussion, the Working Group agreed to revise the definition in terms of attributes that “uniquely distinguish” the subject.

3. Definition of “identity credentials”

109. Broad support was expressed for defining “identity credentials” in terms of the second option (i.e., as “data, or the physical object upon which the data may reside, that a subject may present to verify or authenticate its identity in an online context”). It was suggested that the term “or” be replaced with “and/or” to reflect the fact that an identity credential could also take the form of data and a physical object. In response, it was noted that editorial practice was to avoid the term “and/or” and to use “or” in the English language, which was not deemed disjunctive. It was suggested that the words “verify or authenticate” should be revised in light of the views expressed earlier that the terms were synonymous (see para. 85 above).

110. It was suggested that the instrument should not define “identity credentials” by reference to their use “online”. It was noted that electronic credentials could be used offline. As an alternative, it was suggested that the definition should refer instead to identity credentials “in electronic form”. The Working Group agreed to amend the definition accordingly, as well as the definition of “IdM system” in paragraph 1(h).

4. Definition of “IdM service provider” and “IdM services”

111. The Working Group recalled the agreement at its fifty-eighth session to use the term “IdM service provider” in preference to “IdM system operator” (A/CN.9/971, para. 97). The Working Group agreed to define “IdM service provider” as the person “that provides IdM services”. It was noted that the option to define the term as the person “that provides services in relation to IdM systems” was too uncertain.

112. Reference was made to earlier discussions on the choice between “IdM service” and “IdM system” (see para. 81 above). A question was raised whether “IdM system” was needed, and whether “IdM services” could be defined by merging the definitions of each term in article 1. Recalling its subsequent decision to retain the reference to “IdM system” in article 5(1) (see para. 86 above), the Working Group agreed to retain both definitions.

5. Definition of “IdM system”

113. It was suggested that the notion of “IdM system” was broader than a set of processes, and should instead be defined as an “infrastructure” or “environment” to manage identification. It was noted that document A/CN.9/WG.IV/WP.150 provided a definition of identity management drawn from ITU sources, which referred to “a set of functions and capabilities”. Reference was also made to standard ISO 5127:2017, which defined “system” as a “combination of interacting elements organized to achieve one or more stated purposes”. A question was raised whether it was necessary to define “system” at all. After discussion, the Working Group agreed to define “IdM system” by reference to “functions and capabilities” for managing identification, consistently with ITU terminology.

6. Other definitions

114. It was noted that, in light of decisions taken by the Working Group during the session, the term “relying party” would no longer be used in the instrument. The Working Group also recalled its earlier deliberations with respect to the definition of “trust service” (see paras. 14 to 18).

D. Other general provisions

1. Article 2. Scope of application

115. The Working Group was invited to consider whether the reference in article 2 to “government” was necessary, or whether a generic refence to “trade-related services”

was sufficient to capture transactions with certain public authorities involved in trade, particularly single windows for customs operations. One view was that the instrument should apply solely in a commercial context. The Working Group agreed that the term "government" should be deleted.

2. Article 3. Voluntary use of IdM and trust services

116. The Working Group agreed to delete the reference to "identity credentials" and to use the term "IdM service" instead of "IdM system" in order to ensure consistency throughout the instrument. A similar agreement was reached with regard to article 26 (see also paras. 119 to 121 below). It also agreed to replace the term "subject" with "person" so as to include those relying parties whose consent was necessary.

3. Article 4. Interpretation

117. It was noted that article 4 was a provision used in several UNCITRAL texts and that it was desirable to follow past practice in its formulation in order to maintain uniformity and coherence of interpretation. It was added that reference to "international trade" was also relevant in case the instrument took the form of a model law. It was also explained that the reference to applicable law was useful in case the instrument took the form of a convention.

118. The Working Group agreed: (1) to retain the words "in international trade" without square brackets; and (2) to delete the terms "in particular non-discrimination against the use of electronic means, technology neutrality and functional equivalence".

E. International aspects

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

119. It was explained that article 26 was directed at facilitating the ex ante designation of services provided abroad. It was noted that other provisions already addressed cross-border recognition. The added function of article 26 was therefore questioned and there was some support for deleting it.

120. Different views were expressed on the level of equivalence required for cross-border legal effect. It was suggested that paragraph 1 should focus on the "result of the application" of the service. It was questioned whether all States had the necessary infrastructure to implement article 26, and whether relevant international standards existed. In response, it was said that standards existed but did not cover all the issues raised in the draft instrument.

121. Recognising a link with the form of the instrument, the Working Group decided to defer further consideration of article 26 to its next session, based on a revised text by the Secretariat.

2. Article 27. Cooperation

122. The Working Group agreed to replace "certification" with "designation" to align with articles 11 and 24.

F. Form of the instrument

123. Strong preference was expressed for the instrument taking the form of a model law as opposed to a convention. The need to carry out internal consultations on the issue was emphasized.

G. Next steps

124. The Working Group recalled that a number of issues remained open at the close of the session, including the liability of IdM and trust service providers, the form of the instrument, and the several provisions for which the Secretariat had been asked to provide drafting proposals. Delegations were encouraged to continue discussions and internal consultations between sessions with a view to advancing the Working Group's consideration of those issues at its next session and the possible finalization of the instrument at the Commission's fifty-third session, in 2020.

125. Finally, the Working Group was informed of ongoing work of the United Nations High Commissioner for Refugees on digital identities for refugees and asylum seekers. The Working Group was invited to bear that work in mind in its future deliberations on the topic.

V. Technical assistance and cooperation

126. The Secretariat made reference to recent technical assistance activities in the field of electronic commerce. In particular, reference was made to the "Digital Identity for Trade and Development" course conducted within the "Leapfrogging Skills Development in e-Commerce in South-East Asia in the Framework of the 2030 Development Agenda" project, which was run by UNCTAD as part of the TrainForTrade programme in cooperation with UNCITRAL, and which aimed at building capacity on IdM and trust services in the public and private sectors in South-East Asia.

127. With respect to the promotion of adoption of texts, the recent accession of Benin to the ECC was recalled. States were invited to consider adopting that Convention and other UNCITRAL texts on e-commerce. In that regard, reference was made to ongoing cooperation in drafting national laws enacting UNCITRAL texts.