United Nations A/CN.9/902

General Assembly

Distr.: General
5 May 2017

Original: English

United Nations Commission on International Trade Law
Fiftieth session
Vienna, 3-21 July 2017

Report of Working Group IV (Electronic Commerce) on the work of its fifty-fifth session (New York, 24-28 April 2017)

Contents

V.17-02928 (E) 050517 080517

I. Introduction

1. At its forty-ninth session, in 2016, the Commission confirmed its decision that the Working Group could take up work on the topics of identity management and trust services as well as of cloud computing upon completion of the work on the draft Model Law on Electronic Transferable Records. The Commission was of the view that it would be premature to prioritize between the two topics. It was mentioned that priority should be based on practical needs rather than on how interesting the topic was or the feasibility of work. The Secretariat, within its existing resources, and the Working Group were asked to continue to update and conduct preparatory work on the two topics including their feasibility in parallel and in a flexible manner and report back to the Commission so that it could make an informed decision at a future session, including the priority to be given to each topic.[1]

2. At its fifty-fourth session (Vienna, 31 October-4 November 2016), the Working Group held a preliminary exchange of views on a possible future work on cloud computing, without reaching any decision (A/CN.9/897, para. 126). On identity management and trust services, it was agreed that the Working Group should continue clarifying the goals of the project, specifying its scope, identifying applicable general principles and drafting necessary definitions (A/CN.9/897, paras. 118-120 and 122). (For further background information, see A/CN.9/WG.IV/WP.140, paras. 6-10.)

II. Organization of the session

3. The Working Group, composed of all States members of the Commission, held its fifty-fifth session in New York from 24 to 28 April 2017. The session was attended by representatives of the following States members of the Working Group: Argentina, Austria, Brazil, Canada, China, Colombia, Czech Republic, El Salvador, France, Germany, Honduras, Hungary, India, Indonesia, Israel, Italy, Japan, Kenya, Kuwait, Libya, Mexico, Namibia, Pakistan, Poland, Republic of Korea, Romania, Russian Federation, Singapore, Spain, Thailand, Turkey, United Kingdom of Great Britain and Northern Ireland and United States of America.

4. The session was also attended by observers from the following States: Belgium, Cambodia, Congo, Dominican Republic, Iraq, Paraguay, Saudi Arabia, Sweden, Syrian Arab Republic, Ukraine and Zimbabwe.

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

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

(a) *United Nations system*: World Bank;

(b) *Intergovernmental organizations*: International Institute for the Unification of Private Law (Unidroit);

(c) *International non-governmental organizations*: Alumni Association of the Willem C. Vis International Commercial Arbitration Moot (MAA), American Bar Association (ABA), Center for International Legal Education (CILE), China Society of Private International Law (CSPIL), CISG Advisory Council, European Law Students' Association (ELSA), European Multi-Channel and Online Trade Association (EMOTA), Grupo Latinoamericano de Abogados para el Derecho del Comercio Internacional (GRULACI), GSM Association (GSMA), International Bar Association (IBA), International Federation of Freight Forwarders Associations (FIATA), Jerusalem Arbitration Center (JAC), Law Association for Asia and the

[1] *Official Records of the General Assembly, Seventy-first Session, Supplement No. 17* (A/71/17), paras. 235 and 353.

Pacific (LAWASIA) and World Association of Former United Nations Interns and Fellows (WAFUNIF).

7. The Working Group elected the following officers:

Chairperson: Ms. Giusella Dolores FINOCCHIARO (Italy)

Rapporteur: Mr. Kyoungjin CHOI (Republic of Korea)

8. The Working Group had before it the following documents: (a) annotated provisional agenda (A/CN.9/WG.IV/WP.140 and Add.1); (b) a proposal by the Russian Federation on improving the identity management system through the use of a transboundary trust environment and a common trust infrastructure for cross-border electronic transactions (A/CN.9/WG.IV/WP.141); (c) a note by the Secretariat on contractual aspects of cloud computing (A/CN.9/WG.IV/WP.142); (d) a note by the Secretariat containing terms and concepts relevant to identity management and trust services (A/CN.9/WG.IV/WP.143); (e) a proposal by Austria, Belgium, France, Italy, the United Kingdom, and the European Union on legal issues relating to electronic identity management and trust services (A/CN.9/WG.IV/WP.144); (f) a paper by the United States on legal issues relating to identity management and trust services (A/CN.9/WG.IV/WP.145); and (g) a proposal by the United Kingdom on outcome based standards and international interoperability (A/CN.9/WG.IV/WP.146).

9. The Working Group adopted the following agenda:

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

III. Deliberations and decisions

10. The Working Group engaged in the discussion of contractual aspects of cloud computing on the basis of a note by the Secretariat (A/CN.9/WG.IV/WP.142) and legal issues related to identity management and trust services on the basis of a note by the Secretariat (A/CN.9/WG.IV/WP.143) and proposals by States (A/CN.9/WG.IV/WP.141, A/CN.9/WG.IV/WP.144, A/CN.9/WG.IV/WP.145 and A/CN.9/WG.IV/WP.146). The deliberations and decisions of the Working Group on contractual aspects of cloud computing are reflected in chapter IV of this report, and the deliberations and decisions of the Working Group on legal issues related to identity management and trust services are reflected in chapter V of this report.

IV. Contractual aspects of cloud computing

11. The Working Group discussed contractual aspects of cloud computing on the basis of document A/CN.9/WG.IV/WP.142. The value of an UNCITRAL guidance text on cloud computing, especially for micro, small and medium-sized enterprises, was recognized. In light of the evolving range of cloud computing services, of the variety in types of cloud services contracts and of rapid developments in technology and business practices, it was suggested that general and flexible guidance should be offered.

12. With respect to the drafting approach, there was agreement that the guidance document should aim at explaining the main features of cloud services contracts without attempting to address exhaustively all potential issues arising from all types of such contracts. The desirability of focusing on unique cloud-specific aspects was noted. It was added that existing work by other international organizations, including on technical standards, should be taken into account.

13. As regards the form of the guidance text, there was agreement that at this stage the preparation of a legislative guide or other legislative text or of a detailed legal guide was not desirable. The prevailing view was that a work product should take a form of a checklist of issues to be taken into account when drafting a cloud services contract (the "checklist"). The checklist should describe contractual issues without favouring any particular party and should uphold the principle of party autonomy.

14. The other view was that model contractual clauses or a guide should be prepared on particularly relevant aspects such as data portability and data security. Another view was that the Working Group should start with defining terms relevant to cloud services and prepare a legal guide once definition of those terms had been clarified.

15. After discussion, the Working Group decided to recommend to the Commission the preparation of a checklist of major issues that contracting parties might wish to address in cloud services contracts. In light of its nature, the checklist should not offer best practice guidance or recommendations. The need for preparation of guidance materials or model contractual clauses could be considered at a later stage.

16. As regards the scope of the work, the Working Group was of the view that only issues arising from business-to-business cloud services contracts should be addressed, while government-to-business and business-to-consumer contexts should be excluded. Issues arising from business-to-government relations would be addressed only incidentally. It was added that the guidance document should not address the use of cloud computing in specific sectors, such as education, health-care and financial services, since those sectors posed peculiar challenges addressed by dedicated regulation.

17. It was understood that all clusters of issues listed in paragraph 24 of document A/CN.9/WG.IV/WP.142 should be retained. However, it was added, a detailed discussion should be offered only for those issues specific to cloud computing. Highlighted issues included data portability, data security, subcontracting and risk allocation. Certain matters, such as regulatory ones, including privacy and data protection, and intellectual property rights, should be only mentioned in order to alert contracting parties.

18. It was indicated that providing guidance on choice of law and forum in cloud services contracts would be useful, particularly in developing countries. It was recalled that the various jurisdictions provided different levels of recognition of party autonomy in choice of law and forum, which could have particularly relevant impact on the enforceability of cloud services contracts.

19. It was further indicated that general contract law could address a number of issues arising from cloud services contracts. It was added that providing a reference to general contract law could have a significant impact on familiarizing less sophisticated concerned parties, including in developing countries, with cloud services contracts. Moreover, it could be useful to distinguish between matters addressed in general contract law and matters addressed in service contracts law. After discussion, it was agreed that the checklist should list relevant issues, including those that could be addressed in general contract law or in other law.

20. It was explained that, since the content of cloud services contracts could vary significantly, it was for applicable law to qualify those contracts in light of their actual content. That qualification would then allow the parties to deal appropriately with issues such as: formation and form of the contract; price and payment; duration, renewal and termination; amendments of contractual terms; and dispute

resolution. Hence, it was suggested, it would be particularly useful to provide a detailed description of possible services offered.

21. It was agreed that pre-contractual aspects within contract law could be discussed but that the existence of pre-contractual obligations should not be implied. It was suggested that it could be useful to address separately issues arising from standard contracts for the provisions of off-the-shelf cloud services, which were usually concluded by adhesion, and custom-tailored contracts. In response, it was stated that, as with other types of contracts, cloud computing contracts might involve parties with different levels of sophistication.

22. It was indicated that risk allocation and liability were particularly relevant when considering entering into cloud services contracts and therefore should be included in the checklist. It was added that for the time being that discussion should be limited to liability of contractual parties and should not extend to third-party liability.

23. After discussion, the Working Group suggested that the Commission could ask the Secretariat to prepare, with the help of experts, a draft checklist reflecting the above preliminary considerations, and to submit it to the consideration of the Working Group.

24. As regards the timing of work, one view was that the work could be undertaken in parallel with work on another topic assigned by the Commission to the Working Group. In response, concern was expressed that parallel work on more than one topic could affect the quality of the outcome of that work. Priority should be allocated to work on contractual aspects of cloud computing in light of timeliness and importance of that work. The Working Group deferred a recommendation to the Commission on that aspect until after consideration of other topics on its agenda. (For further discussion, see chapter VI below).

25. The Working Group considered whether the checklist should define the concept of cloud computing, for example with reference to its main features, benefits and risks listed in paragraphs 1 and 2 and 17 to 23 of the annex in document A/CN.9/WG.IV/WP.142. It was observed that, while the annex might assist in the drafting of the checklist, the draft would not necessarily utilize the text or approach contained in the annex. The understanding was that the checklist should describe but not define cloud computing and related concepts. Paragraph 2 of the annex would need to be amended to reflect that point and to explain that cloud services contracts could be qualified as variants of contracts for provision of services and of other types of contracts depending on the actual content of the contract. It was agreed that an explanation of the contracts covered by the checklist would need to be provided from the outset.

26. With reference to paragraph 8 of the annex, it was recalled that the Working Group had decided not to discuss in the checklist the involvement of cloud service partners, such as cloud auditors and cloud service brokers. The checklist could alert contracting parties about issues related to third parties, other than cloud auditors and cloud service brokers, only to the extent that those issues might need to be addressed in a cloud services contract.

27. With reference to paragraph 10, it was explained that the provision of cloud services might raise cross-border issues even in domestic cloud services contracts. Accordingly, it was confirmed that cross-border issues should be duly reflected in the checklist in addition to private international law matters. With reference to paragraph 13 of the annex, it was understood that it would need to be redrafted to reflect the deliberations of the Working Group not to include specific clauses in the checklist. It was agreed that, although the checklist should be as broad and complete as possible, it should not convey to a reader that it dealt exhaustively with all possible pre-contractual and contractual issues related to cloud computing. With reference to paragraph 15 of the annex, the understanding was that, in light of the nature of the checklist, the text would use such expressions as “the parties may wish to consider” or “the parties might wish to provide”.

28. With those preliminary suggestions for a redraft of the annex in document A/CN.9/WG.IV/WP.142, the Working Group completed its consideration of agenda item 4 (for the recommendation of the Working Group to the Commission on the timing of work on cloud computing, see chapter VI below).

V. Legal issues related to identity management and trust services

A. General comments

29. A question was asked on whether the work on identity management ("IdM") and trust services should consider also their use in relation to government services. In response, it was explained that, while non-commercial matters were outside the mandate of UNCITRAL, commercial applications often relied on identity schemes or credentials originating in the public sector. It was recalled that the Working Group had agreed that its future work on IdM and trust services should be limited to the use of IdM systems for commercial purposes and that it should not take into account the private or public nature of the IdM services provider (A/CN.9/897, para. 118). The Working Group reaffirmed that decision.

30. It was recalled that the mandate received from the Commission referred to both IdM and trust services (A/71/17, para. 235).

31. The value of UNCITRAL's work in identifying and addressing legal obstacles to the commercial use of IdM and trust services, including in the broader framework of the work conducted by the United Nations and other international organizations on legal identity, was emphasized. Such work would signal to the international community that legally enabling electronic identification at the global level was possible.

B. Objectives of the project

32. It was suggested that the main goal of work on IdM and trust services should be to enable their cross-border recognition. It was noted that the achievement of that goal would require defining elements of mutual legal recognition such as the recognizing entity, the object of the recognition, the purpose of the recognition and under which circumstances recognition might occur.

33. In order to achieve cross-border recognition, it was suggested that the Working Group could prepare a legal toolbox that would: identify the various solutions relating to IdM and trust services; define their levels of reliability; and specify the legal consequences attached to each reliability level, including liability for failure to provide the specified level of reliability. The benefits of that toolbox would include providing parties with different options for managing risks on an informed basis and ensuring interoperability.

34. Another view was that the main goal of the proposed work was to address fundamental issues related to the legal recognition of identity in electronic form. It was suggested that work could commence with identifying cases when identification was required by law. Subsequently, the conditions under which identity information in electronic form could satisfy identification requirements would be defined. Similarly, the circumstances under which a commercial operator could rely on identity information in electronic form would be specified.

35. Support was expressed for the formulation of a functional equivalence rule for identification. It was indicated that when doing so the distinction between foundational identity and transactional identity would need to be taken into account.

36. Another proposal was to compile existing models for IdM, ranging from self-assertion schemes to dedicated legislation, identify those models that were more appropriate for commercial purposes and prepare related sets of rules.

37. It was suggested that any work should take into consideration ongoing efforts to promote technical and legal interoperability and not override, but enable existing schemes. Efforts to create new identities and IdM systems instead of using existing ones were questioned.

38. A question was asked on the relationship between IdM and trust services. Support was expressed for the view that the two notions were closely interlinked, and that work on IdM entailed work on trust services since IdM was a means to an end, and not an end in itself. Hence, it was suggested that work on IdM alone would not suffice. It was added that IdM was a precondition of trust services and that therefore work should begin on IdM aspects.

39. The view that work should start on trust services was also expressed. In particular, a suggestion was to identify specific trust services intended to be covered by an UNCITRAL instrument and describe the features of those trust services. In response, it was indicated that trust services should be addressed only in the context of IdM and not in a broader context or discretely.

40. Support was also expressed for the view that, while IdM was necessary for certain trust services as well as for other purposes, it was a fundamental notion with autonomous relevance and should therefore be dealt with separately and on a priority basis. It was added that, on the basis of the work carried out on IdM it could be possible to identify at a later stage which trust services were relevant for IdM and conduct further work limited to those trust services.

41. It was suggested to consider identifying common fundamental issues relevant to both IdM and trust services in light of general guiding principles. The Working Group was invited to consider to that end paragraphs 15 and 16 of document A/CN.9/WG.IV/WP.144.

42. In response to a query on the relationship between IdM and trust services, several jurisdictions reported that the two were separate and distinct notions although closely interrelated. It was explained that IdM was an enabler of trust services. Examples of the interaction between IdM and trust services in various contexts and at various levels, including with respect to anti-money laundering and know-your-customer regulations, were provided. Different views were expressed on the desirability of carrying out work on IdM and trust services simultaneously or sequentially.

43. A query was raised on whether attribution of identity information would pertain to the domain of trust services, in particular electronic signatures as addressed in UNCITRAL instruments, rather than to that of IdM. Reference was made to the distinction between identification required by law and identification in a business environment for enforcement purposes.

44. To make a more informed decision on the objectives of UNCITRAL work in the area of IdM, a proposal was made to identify gaps and practical needs that UNCITRAL could address through its work in the area of IdM.

45. In light of the general mandate of UNCITRAL to reduce or remove legal barriers to international trade, the Working Group agreed that it would be appropriate to identify the legal recognition and mutual recognition of IdM and trust services as the goals of the work of UNCITRAL in that area.

46. It was indicated that reference to the notion of mutual recognition could be more appropriate in a legal context than reference to interoperability, which might have technical implications falling outside the mandate of UNCITRAL.

47. It was suggested that the notion of mutual recognition in a commercial context should not necessarily refer to cross-border recognition. Rather, it should refer to

recognition of identity credentials created for commercial purposes across IdM systems regardless of their national or international nature. It was added that mutual recognition should be voluntary rather than mandatory. It was also indicated that legal recognition and mutual recognition could have similar or different meaning depending on the context but would always refer to the concept of identification.

C. Introduction of proposals submitted by States with respect to the scope of work and general principles

48. The delegation of the Russian Federation introduced a paper contained in document A/CN.9/WG.IV/WP.141. It was highlighted that, despite the importance and breadth of IdM, an appropriate legal framework was still missing, and that therefore UNCITRAL should focus on defining the legal regime for IdM, addressing in particular the legal significance of identification. It was added that the scope of the suggested work should focus on clarifying issues specific to electronic IdM and should not touch upon IdM regimes well-established in a paper-based environment. The importance of not excluding any particular system model, especially decentralized ones, was stressed. It was suggested that, in light of the relevance and diversity of the issues to be addressed, work should initially focus on IdM, and that trust services should be addressed thereafter. That work should be based on existing UNCITRAL e-commerce texts and their well-recognized underlying general principles. The desirability of developing adequate terminology, taking into account International Telecommunications Union standards, was mentioned.

49. The delegation of the United Kingdom introduced a paper contained in document A/CN.9/WG.IV/WP.146. It was indicated that the use of cross-border IdM was an enabler of the digital economy and that that use required interoperability among national schemes, which could be established by defining outcome-based standards. Bearing in mind that IdM schemes could vary significantly both nationally and internationally, the goal of the suggested work would be to establish a common understanding of levels of assurance. Reference was made to the relevance of the principle of technological neutrality and of other general principles applicable in the area of e-commerce.

50. The observer delegation of Belgium introduced a paper contained in document A/CN.9/WG.IV/WP.144. The objective of the suggested work was to increase legal certainty of electronic transactions through IdM and trust services, tools enabling international trade actors to conduct risk management. Goals to pursue included: achieving clarification and harmonization of legal terms; establishing legal interoperability as a precursor of technical interoperability; increasing awareness of relevant legal issues; and operationalizing and concretising existing UNCITRAL texts. That work would be based on existing UNCITRAL texts, including general principles, in the area of e-commerce. Additional principles specific to IdM and trust services and listed in paragraph 16 of the paper would be applicable, such as: different levels of assurance and security defined on the basis of objective criteria; distinct legal effects, including burden of proof, according to the level of assurance; and liability according to the level of assurance.

51. The delegation of the United States introduced a paper contained in document A/CN.9/WG.IV/WP.145, outlining governing principles and substantive topics for discussion by the Working Group. It was clarified that the paper was not a proposal and did not express United States' position on issues listed in the paper. It was indicated that the paper focused on IdM-related issues on the understanding that work on trust services would take place after work on IdM. In addition to referring to the already established e-commerce general principles that inspire UNCITRAL's work, the paper identified issues specific to IdM such as: system model neutrality; the relationship between IdM law and privacy law and between IdM law and data security law; and contract-based system rules. It was indicated that the obligation to identify would be found in other law or in contractual agreement. Therefore, IdM law should not aim at imposing any new identification obligation.

D. General principles applicable to the work on IdM and trust services

52. The Working Group agreed that the following four fundamental principles would guide its work in the area of IdM: party autonomy, technological neutrality, functional equivalence and non-discrimination. The understanding was that those principles would be equally applicable to both IdM and trust services but the way in which they apply might differ.

53. It was explained that the principle of proportionality considered by the Working Group at its fifty-fourth session (A/CN.9/897, para. 115) referred to freedom of the parties in the choice of the IdM solution, in particular with respect to the desirable level of assurance. It was indicated that proportionality should not be treated as a separate guiding principle but rather as an aspect of the application of the principle of party autonomy.

54. With respect to technological neutrality, it was indicated that that notion should include reference to economic model neutrality (referred to in document A/CN.9/WG.IV/WP.144) and system model neutrality (as described in document A/CN.9/WG.IV/WP.145), so as not to preclude the use of or discriminate against any existing or future system model.

55. In response to a question on whether the centralized, decentralized or distributed architecture of a mutual recognition mechanism would be relevant for future discussions, it was explained that issues related to model architecture should be addressed according to the principle of technological neutrality and, in particular, its application to neutrality of system models.

56. With reference to the concept of functional equivalence, the Working Group considered it premature to identify functions that IdM would purport to fulfil. The terms related to identification defined in document A/CN.9/WG.I/WP.143 were found unhelpful for such purpose.

57. It was noted that IdM services could go beyond services available in a paper-based environment. The concern was raised that adopting a functional equivalence approach might have the unintended consequence of limiting IdM services to only those existing in a paper-based environment.

58. It was recalled that the goal of the work on IdM was to identify legal obstacles to the use of electronic identity credentials and to formulate provisions to overcome them. In that respect, it was also recalled that identification was a process involving interaction of at least two persons and the presentation of an identity document. Moreover, it was stated that the identification process required the following steps: (a) verification of the validity and accuracy of the identity document; (b) verification of whether the person presenting the document was the person identified in that document; and (c) correctness of the steps undertaken and judgment used in identifying the person. It was added that the use of IdM would not alone satisfy identification requirements. In particular, it was observed that IdM would not purport and be able to verify questions of fact such as forgery, hacking and good faith of a relying party.

59. Those concerns were shared by other delegations. Reference in that context was made to the notion of attribution of identity information described in document A/CN.9/WG.IV/WP.145.

60. It was noted that under a functional equivalence approach the legal effects of identification would arise from substantive law. However, it was also noted that the law could set forth identification requirements without making reference to a paper-based document, and that in that case a functional equivalence approach would not be applicable.

61. Another point was that a wide variety of identification methods existed and that therefore it would be impossible to achieve functional equivalence for all of

them. On the other hand, it was observed that harmonizing substantive rules could interfere with existing law.

62. Other delegations questioned the prudence of focusing on functional equivalence requirements for identification as opposed to IdM as a process. It was noted that IdM may or may not involve the use of paper-based identification documents. It was also explained that, while identification could be a function of certain trust services such as electronic signatures and seals, it would be difficult to identify a function of identification.

63. After discussion, the Working Group agreed that the principle of functional equivalence would be relevant for the work of UNCITRAL on IdM but cases could arise where it would not be applicable. The Working Group deferred consideration of possible approaches to those cases, in particular whether any substantive rules would need to be formulated for such situations.

64. As regards the principle of non-discrimination, the Working Group's attention was drawn to various formulations of that principle found in documents A/CN.9/WG.IV/WP.144 and A/CN.9/WG.IV/WP.145. Support was expressed for the formulation found in document A/CN.9/WG.IV/WP.145 since it closely followed the formulation found in UNCITRAL texts in the area of e-commerce. The alternative view was that that formulation did not refer to trust services, and that therefore the formulation found in paragraph 15 of document A/CN.9/WG.IV/WP.144 was preferable.

65. The Working Group agreed that certain fundamental issues identified for discussion in document A/CN.9/WG.IV/WP.145, in particular the relationship between IdM law and privacy law, between IdM law and data security law, and between contract-based system rules and other law, should also be considered by the Working Group. It was indicated that those issues could be either considered in substance or by deferral to other applicable law.

E. Subjects to be addressed in the work on IdM and trust services

66. The Working Group continued consideration of topics and issues that need to be addressed in discussing IdM and trust services based on paragraph 16 of document A/CN.9/WG.IV/WP.144 and the chapter entitled "Substantive topics" of document A/CN.9/WG.IV/WP.145. The convergence between the two documents, in particular on issues of legal recognition, levels of assurance and risk allocation, was highlighted. However, it was reiterated that the considerations found in document A/CN.9/WG.IV/WP.145 were applicable only to IdM.

67. The Working Group was invited to identify principles, issues and topics equally applicable to IdM and trust services.

1. Legal recognition

68. It was indicated that legal recognition might be understood as referring to the use of IdM to satisfy legal requirements for identification. It was specified that those requirements might be set forth in the law or agreed upon. Moreover, that notion could refer to a presumption of identity attributed to the use of credentials in certain circumstances. Other meanings were also possible. A number of issues, such as who provides recognition and for which purpose, would need to be clarified.

69. It was explained that the notion would also be relevant when parties used IdM and trust services for risk management in the absence of a formal legal obligation but for purely contractual reasons. It was indicated that instances when the law provided for consequences in the absence of proper identification should also be captured.

70. The view was reiterated that work should aim at enabling legal recognition instead of creating binding requirements. It was clarified that that would mean that

no additional standard should be established; instead, interoperability between existing standards should be assured.

2. Mutual recognition

71. The Working Group was invited to consider the notion of mutual recognition addressing such questions as who would perform recognition, what would be recognized, how, and the legal effects. It was explained that the notion referred to the acceptance of identity credentials created in one IdM system by another IdM system regardless of the use of different technology, rules or business model.

72. It was indicated that eIDAS was an example of federated IdM system based on standards of the International Organization for Standardization (ISO) that should be considered by UNCITRAL given that it had already been accepted by 28 States with different IdM systems in place and it was referred to in negotiations with more States. In response, the view was expressed that solutions designed for enabling access to online public services would not necessarily be appropriate in a commercial context. The alternative view was that commercial parties were already able to use those solutions on a voluntary basis as long as they met their identification needs. It was said that examples existed of commercial entities such as banks and other financial institutions using public trust frameworks for their commercial needs.

73. Reference was made to the Intra-ASEAN Secure Transactions Framework, applicable to both public and private sectors and also based on the ISO 29115 standard. It was explained that the goal of that non-regulatory scheme was to promote legal recognition of identification and authentication across ASEAN countries. There were however many challenges encountered in that respect, and UNCITRAL was well placed to address them by developing a global mechanism.

74. The view was reiterated that the scope of the work of UNCITRAL on IdM and trust services was not to impose particular solutions on commercial parties but rather to provide a set of options to satisfy their risk management needs. It was added that commercial parties should be free to attribute various effects to different levels of assurance. However, it was noted that the value of ensuring a common understanding of the assertion of identity by an IdM scheme against a set of uniform assurance levels should not be questioned. It was observed that the availability of a shared reference framework to which IdM systems could be mapped was considered essential for international trade.

3. Attribution of identity information to a subject

75. It was explained that the notion of attribution referred to two aspects: the determination that the person using the identity credential was the person purported to be; and how a relying party could carry out that determination.

76. It was indicated that attribution could be addressed with the use of credentials bound to identity and with reference to levels of assurance. It was added that attribution was also related to risk management. It was explained that a discussion of the mechanics of attribution processes would require in-depth reference to technical details.

77. In response, it was noted that the ability to attribute identity was not necessarily related to the level of assurance. It was also noted that a discussion on the legal effects of attribution, such as presumptions associated with levels of assurance and the possibility to rebut them, did not necessarily imply reference to technical details. The use of pseudonyms and anonymization were considered relevant issues for future consideration.

4. Reliance/attribution of action, data message or signature to a subject

78. It was explained that reliance was a notion related to, but distinct from attribution, since reliance on identity credentials might be inappropriate even in case

of successful attribution of those credentials. It was added that reliance had relevance also for the allocation of liability and for broader issues such as fraud and good faith.

5. Liability/Risk allocation

79. It was indicated that liability and risk allocation had a fundamental role in the work on IdM and trust services. It was stressed that commercial operators would greatly benefit from clarity on liability and risk allocation as currently applicable laws had often been drafted without taking into account IdM and trust services. Examples were provided of how liability for IdM and trust services had been addressed in legislative texts. It was added that liability matters could also be addressed contractually.

80. A question was put on whether addressing liability and risk allocation would imply work on a legislative text. The prevailing view was that, irrespective of the form of the work on IdM and trust services, liability and risk allocation would need to be addressed.

6. Transparency

81. It was explained that the notion of transparency had two distinct aspects. The first aspect was to what extent users should be informed about methods and processes used to deliver IdM and trust services. The second aspect related to duties to inform concerned parties in case of security breaches. The relevance of that information in the choice of IdM and trust services was highlighted.

82. Examples of transparency mechanisms, including through certification and peer review, were provided. Sanctions, disclosure obligations under applicable law and respect for confidentiality, commercially sensitive information and secrecy were mentioned among the issues to be considered in the context of transparency.

7. Other issues

83. While deferring its consideration of the nature of the text to be prepared, the Working Group recognized that that aspect might dictate certain approaches. A view was expressed that, for the Working Group to be productive in its work on IdM, the Commission would need to clarify the nature of the text to be prepared. If a non-legislative text was envisaged, certain issues would not need to be discussed in such depth as for a legislative text. The application of the four fundamental principles identified by the Working Group (see para. 52 above) might also vary.

84. On a preliminary basis, some delegations expressed their reservations on the formulation of substantive rules on IdM. On the other hand, other delegations indicated that the intended goal of the project required a higher level of legal harmonization, which could only be achieved with the preparation of a legislative text.

8. Conclusions

85. The Working Group agreed that the notions of legal recognition, mutual recognition, attribution, reliance, liability and risk allocation, and transparency were relevant for its work on IdM and trust services and suggested that those notions should be further considered, taking into account the above considerations, at a future session.

F. Possible definitions of main terms and concepts

86. It was suggested that the Working Group could further clarify the scope of the suggested work on the basis of the non-exhaustive list of concepts and definitions provided in paragraph 20 of document A/CN.9/WG.IV/WP.144. It was indicated that such additional clarification could greatly assist the Commission in its consideration of the matter.

87. In response, it was said that a discussion of concepts and definitions could be premature, since they would need to be considered in a specific context and they were likely to be modified in light of the progress of work. It was therefore suggested that that list should be retained for future reference. It was added that reference to the information contained in the documents submitted to the current session of the Working Group would suffice to inform the Commission.

88. The prevailing view was that the list of concepts should be considered, if not in detail, at least in general terms.

89. In introducing concepts and definitions contained in paragraph 20 of A/CN.9/WG.IV/WP.144, it was explained that those concepts and definitions were a reduced set of the definitions contained in the eIDAS Regulation[2] selected on the basis of their relevance to UNCITRAL work on IdM and trust services. It was explained that those concepts and definitions could be applied to a large number of different schemes.

90. The suggestion was made that those definitions and concepts listed in paragraph 20 of document A/CN.9/WG.IV/WP.144 and not yet appearing in document A/CN.9/WG.IV/WP.143 should be added to a revised set of defined terms. Subject to confirmation of the mandate, such revised tentative and non-binding list would provide a basis for future deliberations by the Working Group without any implication on the future direction of those deliberations. It was added that at the current stage of deliberations, in the absence of the specific context, any agreement on definitions would not be possible.

91. In response, a concern was reiterated that the current list of defined terms in document A/CN.9/WG.IV/WP.143 was unnecessarily technical and therefore difficult to understand. In that line, it was suggested that the list of defined terms should contain legal definitions found in national, regional and international legal texts and should be as broad as possible to offer an adequate basis to future deliberations. The view was also expressed that the definitions contained in paragraph 20 of document A/CN.9/WG.IV/WP.144 should actually provide a basis to determine the future direction of work.

92. Subject to the deliberations of the Commission with respect to future mandate, the Working Group asked the Secretariat to revise document A/CN.9/WG.IV/WP.143 by including definitions and concepts listed in paragraph 20 of document A/CN.9/WG.IV/WP.144, without prejudice to the future direction of possible work by UNCITRAL on IdM and trust services.

VI. Recommendations on priority of work

93. It was recalled that the Commission had asked the Working Group to continue to update and conduct preparatory work on the topics of cloud computing and IdM and trust services so that it could make an informed decision at a future session, including on the priority to be given to each topic.

94. There was general agreement on the view that the suggested work on the two topics was different in scope and content. It was suggested that work on the two topics could continue in parallel, taking into account that differences between the two projects could lead to different paces in their development. However, the view was reiterated (see para. 24 above) that parallel work on both topics could pose excessive demands on the Working Group, in particular at a more advanced stage, to the detriment of the quality of the final products.

95. It was indicated that work on cloud computing had made more progress towards a specific direction and that therefore it could be finalised sooner than work

[2] 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.

on IdM and trust services. Therefore, the preference was expressed for commencing work on cloud computing on a priority basis. It was added that the outcome of that work could provide useful guidance, in particular, to users in developing countries and to small and medium-sized enterprises.

96. On the other hand, it was indicated that significant progress had been made in better defining the scope and general principles underlying future work on IdM and trust services. The foundational importance of that work for enabling electronic commerce was stressed. It was indicated that, in light of that importance, including vis-à-vis the more limited scope of work on cloud computing, priority should be given to work on IdM and trust services, in particular, in case the resources of the Secretariat would not allow to conduct work in parallel on the two topics.

97. The Working Group submitted the above considerations to the Commission for its determination.

VII. Technical assistance and coordination

98. The Working Group heard an oral report on technical assistance and coordination activities undertaken by the Secretariat related to the promotion of UNCITRAL texts in the area of electronic commerce.

99. Reference was made to the work being carried out inter-sessionally on legal issues relating to electronic single window facilities and paperless trade facilitation. It was recalled that UNCITRAL had provided input in the preparation of the Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific (Bangkok, 19 May 2016).[3] It was indicated that that work had highlighted the importance of fully appreciating the interaction between UNCITRAL texts and e-commerce chapters of global and regional trade agreements. Reference was made to the fact that those chapters often contained provisions on mutual recognition of authentication methods on a technologically neutral basis.

100. Reference was also made to work on enactment of UNCITRAL texts on electronic commerce. It was mentioned that new enactments of those texts were taking place in Southern Africa, thanks to their transposition in a regional model law. It was added that some States had concluded the domestic procedures for the adoption of the United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005),[4] and that therefore additional treaty actions relating to that Convention could be expected in the near future.

101. It was indicated that, pending adoption of the Model Law on Electronic Transferable Records by the Commission, some States had already started considering actively the adoption of that text, in particular, in light of its possible impact on enabling technological innovation, including through the use of distributed ledgers, in the banking and financial sector.

VIII. Other business

102. The Working Group took note that its fifty-sixth session is tentatively scheduled to be held in Vienna from 20 to 24 November 2017, those dates being subject to confirmation by the Commission at its fiftieth session, scheduled to be held in Vienna from 3 to 21 July 2017.

---

[3] Available at https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=X-20&chapter=10&clang=_en.

[4] General Assembly resolution 60/21, annex.