United Nations A/CN.9/WG.IV/WP.158

General Assembly

Distr.: Limited
1 February 2019

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Fifty-eighth session
New York, 8–12 April 2019

Explanatory Remarks on the Draft Provisions on the Cross-border Recognition of Identity Management and Trust Services

Note by the Secretariat

Contents

V.19-00602 (E)

I. Introduction

1. This note provides remarks on the draft provisions on cross-border recognition of identity management (IdM) and trust services that are contained in document A/CN.9/WG.IV/WP.157. Background information on the work of the Working Group on legal issues related to IdM and trust services may be found in document A/CN.9/WG.IV/WP.156, paras. 6–15.

II. Main policy objectives pursued by the draft provisions

2. The last twenty years have seen an exponential growth in online activity. The increase in online commercial activity, i.e. electronic transactions between businesses, businesses and consumers and businesses and governments, is particularly significant in terms of the value that it represents. Global e-commerce grew from $64 billion in 1999 to over $25 trillion in 2015.[1] This growth coincides with increased access to the Internet among individuals and businesses. For instance, the percentage of households with Internet access grew from 35 per cent in 2002 to 83.6 per cent in 2017.[2] The availability of e-government (including trade-related services), e-banking and e-payments has increased accordingly.

3. This growth needs to be supported by a sense of trust in the online environment. One important component of online trust is the ability to identify each party in a reliable manner, especially in the absence of any prior in-person interaction. Over the years, various solutions have been suggested to address the need for online identification. This has led to a proliferation of methods, technologies and devices used to manage identity. Addressing the legal aspects of IdM at a global level has the potential not only to bridge these different solutions but also to encourage interoperability between IdM systems regardless of private or government operation.

4. Several obstacles to the broader use of IdM and trust services exist. Some obstacles are of a legal nature, and include: (1) a lack of legislation giving legal effect to IdM and trust services; (2) divergent laws and approaches to IdM, including laws that are based on technology-specific requirements; (3) legislation requiring paper-based identification documents for entering into online commercial transactions; and (4) the absence of mechanisms for cross-border legal recognition of IdM and trust services (A/CN.9/965, para. 52).

5. The main objective of the work of the Working Group is to address these obstacles through the development of uniform legal rules. These rules serve several purposes: to increase efficiency; to lower transactions costs; to increase the security and legal certainty of electronic transactions thus establishing trust; and to bridge the digital divide.

6. By doing so, the work of the Working Group contributes to the implementation of the Sustainable Development Goals. Specifically, the importance of identity is acknowledged in Sustainable Development Goal 16, target 9 of which calls for the provision of legal identity for all human beings. In the digital economy, this becomes the right to a digital identity. A legal framework for IdM and trust services will promote the secure operationalization of digital identity. By promoting trust in the online environment, this framework will also contribute to sustainable development and social inclusion consistently with Sustainable Development Goal 9, which deals with fostering innovation (among other things).

[1] Source: UNCTAD, E-Commerce and Development Report 2001, UN Doc UNCTAD/SDTE/ECB/1, p. 44; UNCTAD, Information Economy Report 2017, UN Doc UNCTAD/IER/2017, p. 28.

[2] Source: ITU, ICT Statistics, Global ICT Developments, 2001–2018, available at https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

III. Explanatory remarks on draft provisions

A. Chapter I – Sphere of application (draft articles 1 to 3)

1. Purpose of the use of IdM (draft article 1(1))

7. Identification may be required for different purposes, namely for regulatory compliance, to establish the validity of a commercial document and to comply with contractual obligations (A/CN.9/965, paras. 82–83; see also A/CN.9/WG.IV/WP.153, paras. 32–34). **The Working Group may wish to consider how the draft provisions apply for the purposes of regulatory compliance.**

2. Cross-border and domestic legal recognition (draft article 1(1))

8. The recognition of foreign IdM and trust services benefits from the existence of a domestic legal framework. This is because such a framework establishes legal notions that are relevant to the recognition mechanism. Cross-border recognition is further facilitated where domestic legislation contains harmonized rules sharing general principles, if not identical provisions. Moreover, recognition of IdM across borders and recognition across IdM systems regardless of any cross-border or foreign element share a degree of commonality. For these reasons, the draft provisions have been drafted with a view to offering a basis for both an international agreement and model legislation to be enacted domestically.

3. Relevant entities (draft article 1(2) and (3))

(a) Public entities

9. While the primary focus of the work of the Working Group is business-to-business transactions, IdM systems established in other contexts relevant for commercial operations – notably in the context of trade-related government services such as single windows for customs operations – should also be taken into account (A/CN.9/965, para. 83). For these reasons, the inclusion of public entities as entities to which the draft provision may apply is justified.

10. **The Working Group may wish to consider whether the involvement of public entities in IdM transactions or in trust services raises specific issues**, bearing in mind the application of the principles of technology neutrality (see below, para. 23) and party autonomy (see below, para. 24).

(b) Identification of objects

11. It has been suggested that the work of the Working Group should facilitate reliable identification of both subjects (i.e., physical and legal persons) and objects (i.e., physical and digital objects) of transactions and that identification of an object may be useful for identifying the subjects of a transaction. In any case, a clear distinction between subjects and objects should be maintained given that objects do not have legal personality and cannot bear liability (A/CN.9/965, para. 11).

12. The reference in paragraph (3) to the "verification of identity" reflects the decision of the Working Group that its work should focus on transactional identity and, in that context, on issues of recognition, i.e. verification of identity rather than its attribution (A/CN.9/965, para. 10). Transactional (or secondary) identity and foundational (or primary) identity are described in more detail in A/CN.9/WG.IV/WP.153, paras. 7–10.

4. No new obligation to identify (draft article 2(1))

13. A general principle common to UNCITRAL texts on electronic commerce relates to the fact that substantive law, e.g. law applicable to commercial transactions in general, is not affected.

14. In the context of IdM and trust services, this principle requires that legislation on IdM should not introduce any new duty to identify, that legislation on trust services should not introduce any new duty to use any particular type of trust services, and that existing duties should remain unaffected.

15. It has been said that a close link exists between the principle of no new obligation to identify and the principle of party autonomy (A/CN.9/965, para. 110). It has also been noted that new obligations to identify may arise because of the use of a particular trust service but, in any case, the use of that trust service would take place on a voluntary basis (ibidem).

5. Reference to privacy and data protection laws (draft article 2(2))

16. The Working Group has emphasized the importance of data protection regimes for IdM and trust services. Draft article 2(2) contains a specific reference to privacy and data protection laws to reflect the importance that the Working Group has placed on these laws.

B. Chapter II – General provisions (draft articles 4 to 7)

1. Definitions (draft article 4)

17. The draft definitions in draft article 4 have been prepared on the basis of terminology used in existing UNCITRAL texts on electronic commerce.

18. At its fifty-seventh session, the Working Group requested the Secretariat to include in the list of essential definitions for future reference several definitions drawn from article 3 of the eIDAS Regulation.[3] These definitions are as follows:

(a) "Electronic identification" means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;

(b) "Electronic identification means" means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;

(c) "Person identification data" means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;

(d) "Electronic identification scheme" means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;

(e) "Authentication" means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;

(f) "Authoritative source" means any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity;

(g) "Relying party" means a natural or legal person that relies upon an electronic identification or a trust service.

19. **The Working Group may wish to consider whether these definitions, which do not correspond with UNCITRAL defined terms, should replace or supplement the definitions in draft article 4**.

[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.

2. General principles and uniform interpretation (draft articles 5 to 7)

20. UNCITRAL texts commonly contain a provision referring to their uniform origin and a duty of uniform interpretation. Paragraph 2 of article 5 aims to ensure that uniformity is maintained at the time of the interpretation and application of the legislative text.

21. The Working Group has identified the following general principles as relevant for its work on legal aspects of IdM and trust services: (1) non-discrimination against the use of electronic means; (2) functional equivalence; (3) technology neutrality; and (4) party autonomy (A/CN.9/936, para. 67).

22. While these general principles have been elaborated in existing UNCITRAL texts on electronic commerce for application at a domestic level (see, e.g., articles 3, 5 and 6 of the MLES[4]), they equally apply at a cross-border level by laying a domestic legal foundation that allows the receiving jurisdiction to grant and sustain legal status to foreign IdM and trust services.

23. The importance of the principle of technology neutrality for IdM has been fully acknowledged. With regard to developing countries, it has been said that its implementation may prevent the adoption of technical requirements that traders find too costly or sophisticated (A/CN.9/965, para. 38). The implementation of the principle of technology neutrality in the context of IdM may require minimum system requirements for IdM systems that refer to system properties rather than to specific technologies (A/CN.9/936, para. 69).

24. Party autonomy is a fundamental principle of commercial law. However, its application is subject to limitations set out in mandatory law (A/CN.9/936, para. 72). Those limitations are particularly important as the legislative requirements fulfilled by the use of IdM and trust services are often mandatory. As its work progresses, **the Working Group may wish to identify which core rules the party may not vary or derogate from to increase certainty and predictability of cross-border recognition of IdM and trust services** (A/CN.9/965, para. 109). For this reason, a draft provision on party autonomy (e.g., based on article 5 MLES) has not been drafted. Elements of the principle of party autonomy are, however, reflected in draft article 3.

25. The principle of party autonomy aims also at supporting enforceability of contractual agreements, such as IdM system rules and trust services system rules and frameworks. System rules may be particularly relevant in the context of IdM system federations (see A/CN.9/WG.IV/WP.154, para. 39).

C. Chapter III – IdM (draft articles 8 to 13)

1. Legal recognition of IdM on the basis of functional equivalence (draft article 8)

26. The principle of functional equivalence demands identifying the requirements that an electronic record, method or process must meet to fulfil the same functions as a paper-based notion. It has been noted that a provision on functional equivalence would apply only to the extent that paper-based identification is relevant (A/CN.9/965, para. 69) and that a link with the offline IdM processes may need to be expressed in the provision (A/CN.9/965, para. 66).

27. At its fifty-seventh session, the Working Group highlighted some elements for a provision on functional equivalence giving legal effect to IdM: reference to a physical identification element used offline (be it a document, a registry or other authoritative source); reference to all phases of the IdM process (i.e., identification and authentication); and reference to levels of assurance or other standard to assess the confidence in correct identification (A/CN.9/965, paras. 70–78).

[4] *UNCITRAL Model Law on Electronic Signatures* (United Nations publication, Sales No. E.02.V.8).

28. Different views have been expressed within the Working Group as to the object of legal recognition (A/CN.9/965, para. 25), which in turn determines the focus of a functional equivalence provision. In the context of IdM, the object of legal recognition may be: (a) the IdM system; (b) the identity credentials issued by an IdM system; or (c) the outcome of the identification process using an IdM system (i.e., the identity transaction) (A/CN.9/965, para. 24).

29. The prevailing view is that the Working Group should focus on the recognition of processes (i.e. systems) as well as the recognition of outcomes with respect to both IdM and trust services (A/CN.9/965, paras. 94–99). In that respect, it was also explained that legal recognition of IdM systems, of credentials and of the outcome of the identification process are complementary (A/CN.9/965, para. 26). Hence, if IdM systems are recognized, consequently the credentials used for identification are also recognized, as is the outcome of the identification process. Both options for draft article 8, which were discussed at the fifty-seventh session of the Working Group, reflect this approach.

30. There could be instances where identification is carried out exclusively online and functional equivalence may not find application (A/CN.9/965, para. 62). In order to address all instances, it was suggested that the Working Group should discuss the features of an acceptable method of identification instead of trying to elaborate functional equivalence provisions (A/CN.9/965, para. 69).

2. Reliability standards (draft article 9)

31. Elements relevant to determine the reliability of the method in a functional equivalence provision include: (a) contractual agreements, if permitted under applicable law; (b) certification and supervision; and (c) levels of assurance.

(a) Certification

32. Certification of IdM and trust service providers may significantly assist in establishing trust in those providers and their services. Certification options include: self-certification; certification by an independent third party; certification by an accredited independent third party; and certification by a State body. The choice of the most appropriate form of certification is influenced by the type of service involved, the cost and the level of trust sought. In a business-to-business context, it is appropriate to offer all certification options, including absence of certification, since business partners should be able to choose the option most appropriate for their needs, recognizing that each option would produce different legal effects (A/CN.9/965, para. 112).

33. However, it was suggested that any solution presupposing a central certification, accreditation or supervision body may not be appropriate where distributed ledger technology is used because of challenges in identifying the body able to request the certification and the body to assess and in taking corrective and enforcement actions, among others (A/CN.9/965, paras. 114 and 129).

34. In existing legal recognition mechanisms (see A/CN.9/WG.IV/WP.153, paras. 61–73 and 76–79) that are based on an ex ante approach (see below, paras. 47–49), certification (including self-certification) is a necessary element to assess IdM systems using outcome-based standards.

35. Certification can also be relevant for ex post legal recognition (see below, paras. 44–45). For example, paragraphs (e) and (f) of article 10 MLES refer to, but do not mandate, the existence of accreditation, audits and self-certification as factors in assessing the trustworthiness of the systems used by a certification service provider.

36. Different views have been expressed on the desirability of involving public authorities in the certification process. On the one hand, it has been said that voluntary certification does not necessarily involve public entities but may rely on independent certification (A/CN.9/965, para. 112).

37. On the other hand, it has been indicated that State oversight of activities of private sector certifying bodies is essential to prevent risks to competition and abuse, in particular with respect to small market players (A/CN.9/965, paras. 115 and 128). Moreover, it has been observed that accreditation of certifying bodies by State authorities aims at ensuring independence, impartiality and fairness in the activities of those bodies. In response, it was suggested that independent authorities might be in a better position to achieve those goals (A/CN.9/965, para. 115).

38. The approach taken in article 10 MLES is a product of model neutrality. The insertion of mandatory provisions on supervision may be seen to prevent the adoption of a market model based on self-regulation of trust services.

(b) Supervision

39. Supervision of IdM systems is common, since its existence is considered useful or even necessary to create trust in service providers and in the services that they provide. However, establishing such a body entails administrative and financial consequences. Alternative or complementary mechanisms, such as third-party certification, may assist in achieving the goals pursued by supervision while reducing associated costs.

40. It has been noted that public authorities are becoming increasingly involved not only in supervision but also in the development and deployment of IdM systems and the provision of IdM and trust services, and that this necessitates separating supervisory functions from other functions carried out by public authorities (A/CN.9/965, para. 128).

(c) Levels of assurance and mapping

41. The level of assurance is a measure of the degree of confidence in the identification and authentication processes and is therefore key to establishing the reliability of the IdM system (A/CN.9/965, para. 61). Different views have been expressed on the desirability of referring to levels of assurance (see A/CN.9/965, paras. 63–68).

42. Levels of assurance could be referred to in a functional equivalence provision (i.e., draft article 8), or in a provision that establishes standards for the reliability of the IdM system (i.e., draft article 9). **The Working Group may wish to consider whether, if levels of assurance are referred to, a generic reference suffices, or whether reference to different levels of assurance is needed** and, in the latter case, whether each level of assurance should be associated with a different legal effect (see A/CN.9/965, paras. 59–60).

43. At its fifty-seventh session, the Working Group discussed “mapping” as a method to verify whether an IdM system meets the generic description of a level of assurance (see A/CN.9/965, paras. 43–48 and 54). A practical example of how the mapping exercise might work is set out in document A/CN.9/WG.IV/WP.153, paragraph 80.

3. Ex post determination of reliability (draft article 9)

44. Draft article 9 aims to implement an ex post approach for the determination of reliability of IdM systems. The ex post approach assesses an IdM system only in the event of an actual dispute, albeit on the basis of predefined conditions. UNCITRAL texts have followed this approach with respect to trust services (see, e.g., article 9(3) ECC).

45. Additional information on the ex post approach may be found in documents A/CN.9/965 (paras. 40–45) and A/CN.9/WG.IV/WP.153 (paras. 74–75).

4. Presumption of reliability (draft article 10)

46. Draft article 10 is based on article 6(3) MLES, which gives a presumption of reliability to electronic signatures meeting certain requirements. Draft article 10 may apply both ex post and ex ante. Ex post, it supports the implementation of draft article 9 by expressing objective technical criteria that allow an easier determination of reliability. However, the same criteria may be assessed ex ante by a specified body. In that latter case, draft article 10 operates in conjunction with draft article 11.

5. Ex ante determination of reliability (draft article 11)

47. Draft article 11 aims to implement an ex ante approach for the determination of reliability of IdM systems.

48. This approach presupposes the prior definition of conditions that an IdM system must satisfy in order to be included on a whitelist of recognized IdM systems. The view has been expressed that the ex ante approach is preferred where higher levels of assurance are used (A/CN.9/965, para. 47).

49. The discussion of this approach in the Working Group has raised two issues: (1) the need for a centralized institutional mechanism to assess IdM systems; and (2) the involvement of public authorities. Additional information on institutional mechanisms to implement the ex ante approach may be found in documents A/CN.9/965 (paras. 40–45) and A/CN.9/WG.IV/WP.153 (paras. 61–73). Additional information on the involvement of public authorities may be found in document A/CN.9/965 (paras. 49–50).

6. Obligations of IdM system operators (draft article 12)

50. Draft article 12(1) provides initial elements to identify the fundamental obligations of IdM system operators. It is inspired by the corresponding provisions of the eIDAS Regulation.

(a) Duty to notify security breaches

51. Draft article 12(2) establishes a duty to notify security breaches. This duty is an aspect of the principle of transparency (A/CN.9/936, para. 88).

52. Security breaches may affect both systems and transactions. A proper security breach notification mechanism has been identified as important for improving performance and increasing the level of confidence in IdM and trust services (A/CN.9/965, para. 123).

53. Security breach notifications have elements in common with data breach notifications, but also significant differences. Examples of existing legislation providing a regime for the disclosure of security breaches are set out in document A/CN.9/WG.IV/WP.154 (paras. 43–44).

(b) Duty to disclose service offering

54. The Working Group has considered the duty to disclose service offering in its discussions on the principle of transparency (A/CN.9/965, para. 121). Transparency of the service offering is important not only for users (to allow them to make an informed choice) but also for competitors and other concerned entities (e.g., to monitor competition in the market) (A/CN.9/965, para. 121). In its current form, draft article 12(1) does not establish a free-standing duty to disclose service offering.

55. A significant amount of information would be disclosed by IdM system operators participating in federations or otherwise obtaining a certification of their services. Minimum duties of disclosure may be established for other providers. For instance, article 9(1) MLES contains a list of information that the certification service provider must disclose to the relying party.

7. Liability of IdM system operators (draft article 13)

56. It has been stated that, so far as the work of the Working Group contains rules applicable at the national level, it is necessary to address the allocation of liability (A/CN.9/965, para. 116) since the applicable liability regime may have a significant impact on promoting the use of IdM and trust services both for commercial and non-commercial uses.

57. In this regard, the Working Group has identified the following issues to be addressed: identification of the entities bearing liability, taking into account special liability regimes for public entities; the possibility to limit liability of parties complying with predetermined requirements; statutory mechanisms to limit liability (e.g., by exemption or reversal of burden of proof); and contractual limitations of liability (A/CN.9/936, para. 85). Document A/CN.9/WG.IV/WP.154 contains a short description of legislation dealing with the liability of IdM system operators (paras. 23–30).

58. Draft article 13(1) implements the general principle that an IdM system operator should be held liable for the consequences of failing to provide the services as agreed or as otherwise required by law (A/CN.9/965, para. 117). However, in certain cases, it may not be easy to identify the IdM system operator (e.g., when using distributed ledger technology).

59. Under that provision as currently drafted, a public entity may be held liable when acting as a service provider. Different liability profiles may arise when the public entity performs supervisory functions and issues foundational identity credentials.

60. Draft article 13 currently allocates liability only to IdM system operators. **The Working Group may wish to consider whether liability rules should apply also to other concerned entities** (e.g. users and relying third parties), or if, alternatively, general liability rules should apply to those entities. The Working Group may also wish to consider whether the applicable liability regime should be mandatorily disclosed to users and other concerned entities in the interests of transparency.

61. Draft article 13 refers to intention and negligence as basis for liability. A discussion of standards of care, including ordinary and presumed negligence and strict liability, with respect to liability of public-key infrastructure operators is available in the document “Promoting confidence in electronic commerce”.[5]

62. **The Working Group may wish to consider whether additional rules should be established with respect to burden of proof and to the definition of damages** or, alternatively, whether those rules should be found in applicable national law.

63. Draft article 13(2) limits the liability of IdM system operators for damages arising from use exceeding limits disclosed by the IdM system operator. This provision complements the duty to disclose service offering, which is an aspect of the principle of transparency. The document “Promoting confidence in electronic commerce” discusses the ability of public-key infrastructure operators to contractually limit or disclaim liability.[6]

64. Draft article 13(3) sets forth a mechanism that encourages IdM operators to adopt certain standards by requiring the use of those standards as a condition for exempting liability. Alternatively, the provision could refer to the use of higher levels of assurance.

65. Draft article 13(3) is subject to draft article 13(4). The standard of “gross negligence or wilful misconduct” finds expression in the Virginia Electronic IdM Act (see A/CN.9/WG.IV/WP.154, para. 29).

---

[5] *Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods* (United Nations publication, Sales No. E.09.V.4), paras. 179–201.

[6] Ibid., paras. 202–210.

66. Alternative ways for dealing with liability issues include the establishment of an insurance-based mechanism, under which the insurer compensates for damages arising from the use of an IdM system. Another available mechanism foresees the automated release of pre-liquidated compensation or fixed penalties when certain conditions are met.

D. Chapter IV – Trust services (draft articles 14 to 18)

67. As a preliminary matter, **the Working Group may wish to consider whether it should proceed with an open-ended list based on a common definition of "trust service" or rather provide common rules applicable to all trust services and specific rules applicable to each of them**. An open-ended list of trust services may include: electronic signatures; electronic seals; electronic timestamps; electronic registered delivery; website authentication; electronic archiving; electronic escrow; and electronic proof of presence.

1. Legal recognition of trust services on the basis of functional equivalence (draft article 14)

68. In order to draft an adequate functional equivalence provision for a trust service, it is necessary to determine the specific functions pursued by that trust service. Draft article 14 contains basic functional equivalence provisions tailored to each identified trust service. **The Working Group may wish to consider whether a provision on the functional equivalence of trust services should address: (a) generic or specific reliability standards; (b) presumption of reliability; (c) ex ante assessment of reliability; and (d) non-repudiation safety clause**.

(a) Electronic signatures

69. Draft article 14(1) deals with electronic signatures, which are a common form of trust service. All UNCITRAL texts on e-commerce contain provisions on the use of electronic signatures.

70. Certain types of electronic signatures and of other trust services, e.g. electronic archiving, may offer assurance of integrity of the data message. In UNCITRAL texts, maintaining integrity of a data message is a requirement for functional equivalence with the paper-based notion of "original". **The Working Group may wish to consider whether the assurance of integrity should be addressed as a discrete trust service**.

(b) Electronic seals

71. Electronic seals are used in the eIDAS Regulation to provide evidence of the origin and integrity of an electronic document issued by a legal person (eIDAS Regulation, recital 59). Moreover, "electronic seals can be used to authenticate any digital asset of the legal person, such as software code or servers" (eIDAS Regulation, recital 65).

72. UNCITRAL texts on trust services are applicable to both physical and legal persons. Moreover, it has been suggested that the current work of the Working Group should apply also to physical and digital objects, thus covering also software code or servers.

73. Article 8 MLEC[7] requires integrity to achieve functional equivalence of the paper-based notion of "origin". Article 6, paragraph 3 MLES refers to the notion of "integrity" where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates.

[7] *UNCITRAL Model Law on Electronic Commerce* (United Nations publication, Sales No. E.99.V.4).

74. In light of the above, **the Working Group may wish to consider whether electronic seals should be treated as a discrete trust service** or whether they may be considered a subset of electronic signatures.

(c) Electronic archiving

75. Draft article 14(3) deals with electronic archiving services, which in turn relate to the preservation of electronic records. The electronic records to be preserved may have been generated for the first time electronically or may represent information originally issued on paper. Electronic archiving services may also provide a guarantee as to the integrity of the archived electronic records as well as of the time of the archiving.

76. Electronic archiving pursues the function of providing legal certainty on the validity of archived electronic records in case of dispute and for other needs. It has been suggested that the legal recognition mechanism for electronic archiving could be limited to ensuring compliance with the legal requirements of the jurisdiction where the archived records need to be used (A/CN.9/965, para. 126). Should the Working Group wish to consider a provision on electronic archiving, it is suggested to use article 10 MLEC, dealing with retention of data messages, as a basis for that discussion.

77. Moreover, the law may require that archived electronic records should also be capable of being migrated so that access is possible regardless of technological evolution. That result may be obtained by applying the principle of technology neutrality and the requirements for functional equivalence with the notion of "integrity", namely that, when it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented (article 8(1)(b) MLEC).

(d) Other trust services

78. Electronic timestamps, which are dealt with in draft article 14(2), aim at providing evidence of the date and the time when the stamp has been bound with data. They may also provide evidence of the integrity of the data to which the date and time are bound.

79. Electronic registered delivery services, which are dealt with in draft article 14(4), aim at providing evidence of the despatch of an electronic communication by the identified sender and of its receipt by the identified addressee. They may also provide evidence of the integrity of the data exchanged and of the time of despatch and receipt of the data.

80. Draft article 14(5) deals with website authentication. According to the eIDAS Regulation, "website authentication services provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website" (eIDAS Regulation, recital 67). **The Working Group may wish to consider whether website authentication should be treated as a discrete trust service** or may be considered a subset of electronic signatures.

81. Draft article 14(6) deals with escrow services, which consist of taking custody of an asset and releasing it to the entitled person once the conditions set forth in the escrow agreement are met. Escrow services are used with respect to the payment of sums of money and the release of source code of software. For instance, the payment of the price of goods may be delayed until the goods are received by the buyers; at the same time, the seller receives confirmation that the money to pay the price is available and will be released upon goods' delivery and acceptance.

82. Electronic proof of presence services aim to prove that a subject was at a given location at specific times. The trust service has been discussed with respect to electronic wills. It may also be relevant for online enrolment, e.g. for banking services. **The Working Group may wish to consider whether a dedicated provision for electronic proof of presence services should be drafted**.

2. Presumption of reliability of trust services (draft article 15)

83. The MLES and several national laws on electronic signatures distinguish between trust services on the basis of the level of reliability that they offer. Specifically, these laws attach legal consequences to electronic signatures that satisfy certain requirements and therefore are deemed to offer a higher level of reliability. To avoid confusion, it is recommended that the work of the Working Group refer to levels of reliability when discussing trust services, and that the term "levels of assurance" be used only when referring to IdM systems.

84. **The Working Group may wish to consider whether the notion of level of assurance should be applied to the recognition of trust services**, or whether some other notion should be applied to establish the reliability of a particular trust service. It has been noted that identity credentials offering a high level of assurance could be used for trust services with different levels of reliability (A/CN.9/965, para. 106). Therefore, there is no correlation between levels of assurance of electronic identification and levels of reliability of a trust service.

3. Liability of trust service providers (draft article 18)

85. As a general principle, trust service providers should be held liable for the consequences of failing to provide the services as agreed or as otherwise required by law (A/CN.9/965, para. 117). The type of trust service provided will determine the extent of that liability.

86. The MLES contains provisions dealing with liability arising from the conduct of the signatory (art. 8), of the certification service provider (art. 9) and of the relying party (art. 11). Those provisions stipulate the obligations for each entity involved in the electronic signature life cycle. Moreover, the MLES acknowledges the possibility for certification service providers to limit the scope or extent of their liability.

87. Document A/CN.9/WG.IV/WP.154 contains a short description of legislation dealing with the liability of trust service providers (paras. 33–35).

E. Chapter V – International aspects (draft articles 19 to 20)

1. Cross-border legal recognition (draft article 19)

88. Cross-border legal recognition may be understood in different ways (see A/CN.9/WG.IV/WP.153, para. 55). At the fifth-seventh session of the Working Group, it was said that granting national treatment should be the preferable approach for cross-border legal recognition (A/CN.9/965, para. 30). Draft article 19 has been drafted accordingly.

89. The applicable liability regime may be relevant in assessing the equivalence of a foreign IdM system. Accordingly, it has been suggested that, in order to facilitate the cross-border recognition of IdM, it is necessary to determine the law applicable to the liability regime (A/CN.9/965, para. 116). This may require the preparation of a dedicated private international law rule or reference to existing ones. **The Working Group may wish to consider whether cross-border legal recognition would entail the application of the domestic liability regime to foreign IdM and trust services**.

90. Draft article 19 does not deal explicitly with limitation of liability. Additional rules may be applicable, including under mandatory law, that may limit the validity of such contractual clauses.

91. Draft article 19(2) prescribes the level of reliability as the standard for assessing the equivalence of a foreign IdM system or identity credentials. It presents two alternatives: that the foreign IdM system provides the same level of reliability; or that it provides a substantially equivalent level of reliability. The notion of "substantially equivalent level of reliability" is drawn from article 12 MLES. **The Working Group may wish to consider whether, with respect to the recognition of IdM, additional**

guidance should be given with respect to reference to the notion of levels of assurance and the use of mapping.

2. Institutional cooperation mechanisms (draft article 20)

92. Institutional cooperation mechanisms may assist in achieving mutual legal recognition and interoperability of IdM systems and trust services.

93. Draft article 20 refers to institutional cooperation in the form of cooperation among States. Cooperation may consist of exchanges of information, experience and good practice, in particular with respect to technical requirements and levels of assurance, peer review of IdM systems and examination of relevant developments. An eIDAS implementing act[8] provides additional details on exchange of information and peer review, including by indicating that the member State may not provide the required information if disclosure could violate matters of public security or national security, or business, professional or company secrets.

94. Another form of cooperation may be achieved through IdM systems federation. Federations are usually based on contractual agreements, although statutory provisions may contribute to promoting federation. For more information on IdM systems federation, see document A/CN.9/WG.IV/WP.154, paragraph 39.

95. IdM systems federations operate based on technical interoperability and a common legal framework defined by a set of system rules. Harmonization of contractual and legislative rules may contribute to the establishment of that common legal framework (A/CN.9/965, para. 120).

96. It has been mentioned that the adoption of an ex ante mechanism for legal recognition may also result in a form of institutional cooperation.

[8] Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification.