United Nations A/CN.9/WG.IV/WP.153

General Assembly

Distr.: Limited
6 September 2018

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Fifty-seventh session
Vienna, 19–23 November 2018

Legal Issues Related to Identity Management and Trust Services

Note by the Secretariat

Contents

V.18-05868 (E)

I. Introduction

1. This note illustrates certain aspects of some of the topics identified by the Working Group as relevant to its consideration of legal issues related to identity management ("IdM") and trust services (A/CN.9/936, para. 58) in order to facilitate further discussion. In particular, it aims at highlighting key issues and suggesting possible solutions and does not intend to limit the possibility of considering additional topics or of considering some topics together, as appropriate. Working paper A/CN.9/WG.IV/WP.154 illustrates certain aspects of other topics identified by the Working Group as relevant to its consideration of legal issues related to IdM and trust services.

2. Background information on the work of the Working Group on legal issues related to IdM and trust services may be found in working paper A/CN.9/WG.IV/WP.152, paras. 6–17. A list of additional relevant documentation may be found in working paper A/CN.9/WG.IV/WP.152, paragraph 18.

II. Relevant Issues for Future Work on Legal Aspects of Identity Management and Trust Services

A. Scope of work

3. Following the Working Group's recommendation, the Commission requested the Working Group to conduct work on legal issues relating to IdM and trust services with a view to preparing a text aimed at facilitating cross-border recognition of IdM and trust services. The Commission's request is framed in terms sufficiently broad to include aspects of the legal treatment of IdM and trust services additional to those already identified (see above, para. 1).

4. Legal mechanisms for cross-border recognition of IdM and trust services are a fundamental component of the enabling legal framework of the digital economy and their absence may contribute to further increasing the digital divide. The Working Group may therefore wish to consider the broader implications of its work for addressing the digital divide.

5. In that respect, the Working Group may wish to consider whether the absence of a domestic legal framework enabling the use of IdM and trust services may pose a challenge to cross-border legal recognition of IdM and trust services. In that case, the Working Group may wish to identify the legal provisions that should be enacted in domestic legislation in order to fully enable cross-border legal recognition of IdM and trust services, and to discuss the type of legal text (e.g., treaty, model law or both) that would be most appropriate for achieving that goal.

6. Moreover, cross-border legal recognition of identity has elements in common with legal recognition of identity across IdM systems regardless of foreign elements. The Working Group may therefore wish to consider whether it should discuss a mechanism enabling legal recognition across identity management systems, taking into account, when relevant, foreign elements. In that case, the outcome of the work of the Working Group could provide guidance on IdM both at the national and at the international level.

1. Foundational vs. transactional identity

7. The Working Group may wish to recall that a distinction has been suggested between primary and secondary determination of identity (A/CN.9/WG.IV/WP.149, para. 29).

8. Primary determination of identity, or foundational identity, relates to attribution of identity in the context in which the entity originates and at the time of its origin. As such, foundational identity is typically unique and irreplaceable. Examples of

primary determination of identity include: inscription of a physical person by a government in a civil registration and vital statistics record; inscription of a legal person in a dedicated registry by the relevant authority, e.g. a registry of incorporated commercial companies; and attribution of a digital object identifier to a digital object.

9. Secondary determination of identity, or transactional identity, refers to the use of identity to fulfil a specific function (e.g., the conclusion of a contract; the distribution of cash from an automated teller machine; the release of a certificate from a public authority).

10. While foundational identity may not be commonly used in commercial transactions as such, it may be used by identity providers to establish transactional identity. For instance, UNCITRAL provisions on electronic signatures require the identification of the signatory. In some cases, reliable identification of the signatory may be based on the use of an identity credential and authentication process that establishes identity on the basis of foundational identity credentials. Hence, legal recognition of foundational identity across borders and across identity management systems may be useful or even necessary.

2. Relevant entities

11. The Working Group held a preliminary discussion on the types of entity relevant for its work (A/CN.9/936, paras. 63–65), i.e., the entities to which the outcome of its work would apply. The relevance of physical and legal persons involved in trade, including across borders, was generally acknowledged. Entities without distinct legal personality, but relevant for commercial activities, may also be taken into consideration. For instance, traders operating in the informal sector in least developed countries may use mobile identity as their primary means of identification.

12. The involvement of public entities may be justified in light of the relevance for international trade of certain business-to-government and government-to-government transactions, such as cross-border single windows for customs operations. 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, in particular, the application of the principles of technology neutrality (see below, paras. 38–40), party autonomy (see below, paras. 41–47) and proportionality of electronic identification means to the function pursued (see below, para. 46).

13. Different views have been expressed on whether identification of physical and digital objects fell within the scope of this work. According to one view, physical and digital objects should be excluded because they did not have legal personality and could not be held autonomously liable. However, the view was also expressed that identification did not require autonomous legal personality or the imposition of liability on the identified object (A/CN.9/936, para. 64).

14. Another view was that consideration of identification of objects could take place after the Working Group had dealt with that of persons (A/CN.9/936, para. 65). In that respect, it should be noted that objects are a major source of big data according to the “Internet of things” model, and that reliable attribution of data may be particularly relevant under that model. For instance, medical devices are increasingly used to remotely monitor a patient’s condition during daily activities. It is critical to ensure that the information generated by those devices is attributed to the correct patient. Similarly, medications need to be traced not only at the time of their use, but throughout the production cycle to ensure appropriate identification of the medication, as well as to guarantee its origin and content. It is likewise critical that the medication and its components are reliably identified.

B. Definitions

15. The Working Group may wish to refer to document A/CN.9/WG.IV/WP.150 for a list of terms and concepts relevant to identity management and trust services that

could be useful for its deliberations. That list does not pre-empt the Working Group's deliberations on definitions of relevant terms as work progresses.

16. With respect to IdM, the following definitions contained in document A/CN.9/WG.IV/WP.150 may be particularly useful in the Working Group's deliberations of the issues raised in this note.

17. "Identity" means (a) information about a specific subject in the form of one or more attributes that allow the subject to be sufficiently distinguished within a particular context; (b) a set of the attributes about a person that uniquely describes the person within a given context (A/CN.9/WG.IV/WP.150, para. 31).

18. The Working Group may wish to consider the relationship between those definitions and the notions of foundational identity and transactional identity (see above, paras. 7–10) as well as the relevance of those notions for its future work. In that respect, the Working Group may wish to clarify whether uniqueness is an attribute of foundational identity.

19. "Identity management" means a set of processes to manage the identification, authentication, and authorization of individuals, legal entities, devices, or other subjects in an online context (A/CN.9/WG.IV/WP.150, para. 35).

20. "Identity system" means an online environment for identity management transactions governed by a set of system rules (also referred to as a trust framework) where individuals, organizations, services, and devices can trust each other because authoritative sources establish and authenticate their identities (A/CN.9/WG.IV/WP.150, para. 38).

21. "Identity transaction" means any transaction involving two or more participants which involves establishing, verifying, issuing, asserting, revoking, communicating, or relying on identity information (A/CN.9/WG.IV/WP.150, para. 39).

22. The Working Group may wish to refer to the notions of "identity management", "identity system" and "identity transactions" to clarify whether its work on legal recognition of IdM should refer to identity systems, identity transactions or both (see below, paras. 57–59).

23. "Level of assurance" means a designation of the degree of confidence in the identification and authentication processes — i.e., (a) the degree of confidence in the vetting process used to establish the identity of an entity to whom a credential was issued, and (b) the degree of confidence that the entity using the credential is the entity to whom the credential was issued. The assurance reflects the reliability of methods, processes and technologies used (A/CN.9/WG.IV/WP.150, para. 42).

24. The Working Group may wish to refer to the definition of "level of assurance" when discussing that topic (see A/CN.9/WG.IV/WP.154, paras. 10–19). In doing so, the Working Group may also wish to take into account the following definition of "assurance level": "a level of confidence in the binding between an entity and the presented identity information" (A/CN.9/WG.IV/WP.150, para. 12), as well as the note to that definition explaining that the notions of "identity assurance" and "authentication assurance" may be viewed as separate components of the overall concept of "level of assurance".

C. General principles

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

1. Non-discrimination against the use of electronic means

26. The principle of non-discrimination against the use of electronic means is well-settled in UNCITRAL texts. One possible formulation of that principle in the context of IdM and trust services could read:[1]

> The verification of identity through the use of identity [credentials] [management systems] and trust services shall not be denied legal effect, validity or enforceability on the sole ground that those identity [credentials] [management systems] and trust services are in electronic form.

27. The draft provision contains a choice between "identity credentials" and "identity management systems" depending on whether reference should be made to the use of the credentials for identification or rather to the use of the whole IdM system (see below, paras. 57–59).

2. Functional equivalence

28. In the field of electronic commerce, the principle of functional equivalence establishes the requirements that an electronic record, method or process must meet in order to fulfil the same functions as a paper-based notion.

(a) IdM

29. A possible functional equivalence rule on IdM could read as follows:

> Where the law requires or permits the identification of an entity, that requirement is met with respect to [electronic] [digital] identity management if a reliable method is used to [verify the [relevant] attributes of the entity].

30. The intended effect of a functional equivalence provision on identification would be to transpose the identification requirements applicable to paper-based identification into an electronic environment. The Working Group may wish to consider the insertion of the word "[relevant]" to indicate that only those attributes that are requested for offline identification would be necessary to successfully achieve online identification. The Working Group may also wish to clarify whether reference should be made to "electronic identity" or "digital identity".

31. Further guidance could be provided on the elements relevant to determine the reliability of the method, including: (a) contractual agreements, if permitted under applicable law; (b) third-party and self-certification; and (c) reference to levels of assurance. In particular, reference to the use of a "reliable method" in a functional equivalence provision may require the use of a method that provides an equivalent level of reliability in online and offline identification.

32. The discussion of a functional equivalence rule on IdM could benefit from reference to cases where IdM is used. In that respect, it should be noted that identification may be required for different purposes or functions. One purpose is regulatory compliance. Examples of such requirement are the application of "Know Your Customer" ("KYC") rules in the finance, telecom and other business sectors and in the field of electronic procurement, where the correct identification of potential vendors and clients is necessary to prevent fraud and collusion and to enforce debarment.

33. Another purpose of identification is to establish the validity of a commercial document. For instance, the law applicable to a bill of lading may require the identification of certain parties. This is the case under article 15 of the United Nations Convention on the Carriage of Goods by Sea (Hamburg, 1978) (the "Hamburg Rules")[2] and article 36 of the United Nations Convention on Contracts for the

[1] Draft provisions are inserted for illustrative purposes only, without any prejudice to the recommendations of the Working Group to the Commission on the possible form of its work, and to the decisions of the Commission on that form.

[2] United Nations, *Treaty Series*, vol. 1695, No. 29215, p. 3.

International Carriage of Goods Wholly or Partly by Sea (New York, 2008) (the "Rotterdam Rules").[3]

34. Moreover, parties to an online transaction may agree on the use of certain procedures and methods to identify each other accurately for risk management purposes and in absence of any statutory requirement to do so. The source of that obligation to identify is contractual.

35. A policy decision to adopt higher identification standards could be made to better enforce identification duties in situations where offline identification, although in use, is not fully satisfactory. The Working Group may wish to consider the interaction between the adoption of a functional equivalence provision on identification and the possible introduction of requirements for online identification that are more stringent than those applicable offline.

(b) Trust services

36. UNCITRAL texts contain functional equivalence rules for certain trust services, namely for electronic signatures, in article 7 of the UNCITRAL Model Law on Electronic Commerce ("MLEC"),[4] article 6 of the UNCITRAL Model Law on Electronic Signatures ("MLES"),[5] article 9(3) of the United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005) ("ECC")[6] and article 9 of the UNCITRAL Model Law on Electronic Transferable Records,[7] and for retention and archiving in article 10 MLEC. The Working Group may wish to consider whether specific provisions should be prepared for the output of each type of trust service, or, alternatively, if a general rule on functional equivalence can or should be drafted (see A/CN.9/WG.IV/WP.154, para. 58).

37. The Working Group may also wish to consider whether a provision on attribution of identity information would be desirable, or whether the functional equivalence rule would suffice as the identity information would be attributed to the same entity as in an offline environment and, in any case, would not be attributed to the identity service provider. Article 13 MLEC provides an example of a provision dealing with attribution.

3. Technology neutrality

38. The principle of technology neutrality is a cornerstone of UNCITRAL texts and of many other legislative texts dealing with the use of electronic communications. In the context of IdM and trust services, it may be necessary to provide guidance on minimum system requirements by referring to system properties rather than specific technologies (A/CN.9/936, para. 69). Alternatively, if a transactional approach is chosen (see below, paras. 57–59), guidance may be required on minimum identity transactions requirements by referring to transactions properties. In the context of trust services, the implementation of the principle of technology neutrality may require identifying the specific objectives to be achieved by each trust service, without mandating the use of any particular technology to achieve those objectives.

39. A provision on the equal treatment of IdM and trust services technologies, methods and systems may read as follows:

> Nothing in this [draft instrument] shall be applied so as to exclude, restrict or deprive of legal effect any [technology, method or system] used for identity management and trust services that satisfies the requirements referred to in this [draft instrument][, or otherwise meets the requirements of applicable law].

---

[3] General Assembly resolution 63/122, annex.
[4] United Nations publication, Sales No. E.99.V.4.
[5] United Nations publication, Sales No. E.02.V.8.
[6] United Nations, *Treaty Series*, vol. 2898.
[7] United Nations publication, Sales No. E.17.V.5.

40. The words “or otherwise meets the requirements of applicable law”, which may be found in article 3 MLES, refer to the possibility that law other than the draft instrument could prescribe, in certain identified cases, the use of requirements different from those set forth in the draft instrument.[8]

4. Party autonomy

41. One consequence of the principle of party autonomy is that the use of identity and trust services is optional. While that principle may be fully applied with respect to commercial services, its application, for policy reasons, may be limited with respect to access to services provided by public entities or for interaction with those entities.

42. A possible provision on the optional use of identity and trust services may read as follows:

> 1. Nothing in this [draft instrument] requires an entity to use or accept identity [credentials] [management systems] and trust services without that entity’s consent.
>
> 2. The consent of an entity to use identity [credentials] [management systems] and trust services may be inferred from the entity’s conduct [and other circumstances].
>
> [Paragraph 1 does not apply to …]

43. The draft provision contains a choice between “identity credentials” and “identity management systems” depending on whether reference should be made to the use of the credentials for identification or rather to the use of the whole identity management system (see also below, paras. 57–59).

44. In the second paragraph of the draft provision, the words “[and other circumstances]” are inserted to refer to instances where the entity is not capable of autonomous conduct (e.g. a physical or digital object). In those cases, the consent will not be attributable to the entity, but to the physical or legal person controlling that entity.

45. The application of the principle of party autonomy 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. In that light, a formulation of that principle based on article 5 MLES is suggested:

> The provisions of this [draft instrument] may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law.

46. Another application of the principle of party autonomy relates to the freedom to choose the identity and trust services more appropriate for the function pursued by the parties (so-called “principle of proportionality”). The freedom of choice of the type of service is also closely related to the principle of technology neutrality.

47. 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 therefore be particularly relevant in the context of IdM systems federation (see A/CN.9/WG.IV/WP.154, para. 39). The working definition of IdM federation refers to “a group of identity providers, relying parties, subjects and others that agree to operate under compatible policies, standards, and technologies specified in system rules (or a trust framework) in order that subject identity information provided by identity providers can be understood and trusted by relying parties” (A/CN.9/WG.IV/WP.150, para. 28).

[8] *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment* (United Nations publication, Sales No. E.02.V.8), para. 107.

5. Obligation to identify

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

49. 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.

50. A possible provision could read as follows:

> Nothing in this [draft instrument] imposes a requirement on a party [to verify the identity of] [identify] another entity or to use a trust service.

6. Uniform interpretation

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

52. A possible draft provision could read as follows:

> 1. In the interpretation of this [draft instrument], regard is to be had to its international character and to the need to promote uniformity in its application and the observance of good faith in international trade.
>
> 2. Questions concerning matters governed by this [draft instrument] which are not expressly settled in it are to be settled in conformity with the general principles on which it is based or, in the absence of such principles, in conformity with the law applicable by virtue of the rules of private international law.

53. In the second paragraph of the draft provision, reference to “the law applicable by virtue of the rules of private international law” may be particularly useful in a cross-border context.

D. Legal recognition requirements and mechanisms

54. At a general level, legal recognition may be understood as defining the requirements that must be satisfied to obtain legal status in a jurisdiction. Granting legal recognition at the domestic level may require the formulation of substantive rules.

55. Cross-border legal recognition may be understood as: (a) granting the same legal status in the receiving jurisdiction as in the originating jurisdiction; (b) granting the same legal status as in the receiving jurisdiction, regardless of any foreign element; or (c) defining the effects of legal recognition in a dedicated instrument. Moreover, cross-border legal recognition may be mutual, i.e. reciprocal, or unilateral. In both cases, it may be subject to conditions.

56. Legal recognition of IdM schemes and trust services is the central issue in the work of the Working Group and should legally enable technical features such as interoperability of identity credentials and trust services and portability of identity and trust across IdM schemes. As noted above (para. 6), cross-border legal recognition of identity has elements in common with legal recognition of identity across identity management systems, regardless of foreign elements.

57. The object of legal recognition may be IdM and trust services systems and schemes. In that case, legal guidance may be needed on the features that those systems and schemes must comply with in order to achieve legal recognition. As a consequence, the output of those systems and schemes to be used in transactions,

i.e. electronic identification means and specific trust services, may also benefit from legal recognition.

58. The object of legal recognition may also be the transactions facilitated by the use of IdM and trust services. In that case, legal guidance may be needed on the conditions to be fulfilled to provide legal recognition to identity credentials and verifications and to the output of trust services. Existing UNCITRAL texts on electronic commerce mainly deal with transactional matters. For instance, the MLES deals mostly with the transactional use of electronic signatures and only partially with the features of electronic signatures systems.

59. The Working Group may wish to consider whether its work on legal recognition should apply to IdM and trust services systems and schemes, to transactions facilitated by the use of IdM and trust services or to both.

60. The Working Group may further wish to consider whether its work should envisage only a cross-border legal recognition mechanism or should deal also with domestic cross-system legal recognition.

1. IdM

(a) Ex ante legal recognition

61. One available mechanism for legal recognition of IdM schemes envisages the prior establishment of a list of recognized IdM schemes and of the conditions to be met in order to be included in that list. Such an approach typically requires setting up a centrally-managed evaluation and licensing institutional mechanism to assess IdM schemes.

62. This approach, which may be used also for trust services, may provide clarity and predictability on which schemes and services may be used across systems and borders. However, it may deny legal recognition to those schemes and services that, although used, are not on the list. Depending on its governance, it may not react to developments as rapidly as technological evolution may require, thus possibly hindering innovation, and may result in the imposition of technology-specific requirements.

63. The institutional mechanism needed to implement this approach requires identification of the requisites for membership of the evaluating entity and definition of the criteria to evaluate IdM schemes as well as of the mechanisms to update them, of the decision-making evaluation process and of the funding sources. Depending on a number of factors including pre-existing institutional arrangements, governance of that licensing system may be more or less complex and costly.

64. Moreover, a centrally-managed licensing system may be more effective when operating on a comparatively limited scale and in the framework of broader economic integration initiatives but may pose challenges if implemented at the global level since it may require a significant level of cooperation by members.

65. The adoption of a centrally-managed licensing system at the global level may require the adoption of a treaty or similarly binding international law instrument. The advantages of a treaty-based mechanism include predictability and, possibly, easier application to public bodies; the disadvantages include costs related to setting up and maintaining the institutional mechanism, costs charged to participating schemes and the need to gather support from a sufficient number of States, schemes and users. A treaty-based mechanism may be particularly appropriate to ensure funding of long-term financial obligations, although cost recovery from users may be possible.

66. Recently-adopted dedicated IdM laws rely on central oversight to recognize legal effects of IdM schemes.

67. The eIDAS Regulation [9] is the only piece of legislation that specifically addresses IdM cross-border issues. In particular, article 6 eIDAS enables the use of the electronic identification means of one EU member State to access a service provided online by a public-sector body in another Member State, subject to the fulfilment of certain conditions. One of those conditions requires the electronic identification means to be issued under an electronic identification scheme that is notified to the European Commission and complies with the interoperability requirements set out by the European Commission. A peer review is part of the notification process.

68. Other IdM laws aim to address IdM matters without specific reference to cross-border issues. In that respect, it should be noted that, while the eIDAS Regulation does not affect existing IdM schemes but aims to achieve mutual legal recognition among those schemes across borders, national laws on IdM establish the conditions for the operation of IdM schemes.

69. The Law 2017-20 of Benin contains a section on IdM, dealing with assurance levels of electronic identification schemes, eligibility for notification of electronic identification schemes, security breaches, liability and interoperability. The provisions are generally inspired by the corresponding ones of the eIDAS Regulation.

70. The Virginia Electronic IdM Act[10] relies on a mechanism whereby identity trust framework operators may avoid liability if they comply with a number of regulatory and statutory requirements (see A/CN.9/WG.IV/WP.154, paras. 28–29). With respect to legal effects, the use of an identity credential or identity attribute that is compliant with the standards set by the Commonwealth of Virginia, contractual representations and federation rules satisfies any requirement for a commercially-reasonable security or attribution procedure under the Uniform Electronic Transactions Act and the Uniform Computer Information Transactions Act.[11]

71. Act No. 205-2018 of the State of Vermont created a new type of dedicated business entity, called a Personal Information Protection Company, to manage personal information, namely, to provide elements of personal information concerning individual consumers to third parties for transactional purposes and certification or validation services concerning personal information.

72. A stated goal of the Act is that the personal information protection company shall operate “in the best interests and for the protection and benefit of the consumer” (section 2451(3)(B)). Section 2452 of Act No. 205-2018 establishes that a personal information protection company has a fiduciary relationship towards the consumer when providing personal information protection services.

73. The Department of Financial Regulation of the State of Vermont, which has oversight authority on personal information protection companies, may adopt rules on timing and content of reports to be submitted by those companies. It may also adopt rules on protection and safeguarding of personal information and on exchange of that information with third parties.

(b) Ex post legal recognition

74. Alternatively, legal recognition may be achieved through a mechanism that generally allows exchanges and assesses suitability for use of IdM schemes and trust services only in the event of dispute and on the basis of predetermined criteria.

[9] 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.

[10] Virginia Electronic Identity Management Act, VA Code §§ 2.2-436–2.2-437 and VA Code §§ 59.1-550–59.1-555.

[11] The Uniform Electronic Transactions Act, 1999, and the Uniform Computer Information Transactions Act, 1999, amended in 2000 and 2002, are model laws prepared by the United States National Conference of Commissioners on Uniform State Laws.

UNCITRAL texts have followed this approach, for instance by implementing the so called “ex post facto” reliability test (see, e.g., article 9(3) ECC).

75. This approach has the benefit of providing maximum flexibility in the choice of technologies and methods to the parties to the transaction. Moreover, it does not require the establishment of an institutional mechanism, thus avoiding associated costs, and may be administered in a decentralized manner. On the other hand, it has the disadvantage of requiring the intervention of a third-party adjudication process to evaluate the suitability of the IdM scheme or trust service for cross-border use, which may also be costly and time-consuming, and exposes the parties to uncertainty.

(c) Mapping-based legal recognition

76. One suggestion makes reference to the possibility of mapping IdM systems according to a common template. The legal requirements for, and the effects of, the mapping exercise would be defined by the receiving jurisdiction and IdM system.

77. In carrying out the mapping exercise, reference could be made to generic descriptions of levels of assurance in order to ensure that the exercise would be outcome-based, which, in turn, would preserve the application of the principle of technology neutrality.

78. The mapping exercise would not rely on approval by a central authority but could be carried out by any concerned party, including private and commercial entities. The result of the mapping exercise would be published in a trusted list for public dissemination.

79. Some elements to be taken into consideration when carrying out the mapping exercise may be those identified in the Commission Implementing Regulation (EU) 2015/1502, operating in the framework of the eIDAS Regulation. Those elements are: enrolment, electronic identification means management, authentication, and management and organization. Each element includes several sub-elements. The Working Group may wish to consider to what extent guidance should be provided on specifications and procedures to be followed in a mapping exercise.

80. A practical example may illustrate how the mapping exercise might work. As noted above, KYC requirements are common in various business sectors. Depending on the transaction to be carried out, KYC requirements are typically satisfied by the use of credentials complying with level of assurance “two” or “high”, or with level of assurance “three” or “substantial” (see A/CN.9/WG.IV/WP.154, paras. 13–14, for a description of different levels of assurance).

81. Those requirements typically may not be satisfied by using identity credentials issued in a different jurisdiction without a mechanism for legal recognition of IdM schemes. By mapping the credentials against generic descriptions of levels of assurance, it would be possible to verify whether the identity credentials could satisfy the requirements for the level of assurance needed for KYC purposes in that specific transactions.

82. For instance, identity system operator A could submit a certification that its electronic identification scheme X complies with level of assurance 2 or high and that its electronic identification scheme Y complies with level 3 or substantial, thus inserting electronic identification schemes X and Y in the trusted list. Legal person B wishing to conduct business electronically with financial institution C may use credentials issued under electronic identification scheme X or electronic identification scheme Y, depending on the requirements of the transaction. Financial institution C may verify that electronic identification schemes X and Y are inserted in the trusted list, and the associated levels of assurance, and accept the credentials issued under those electronic identification schemes accordingly.

83. The above example may apply also in a national context if domestic law does not specify the requirements for the legal recognition and equivalence of electronic identification schemes.

84. The envisaged mechanism could be based on two provisions dealing, respectively, with the conditions for the insertion in the trusted list and the effects of that insertion.

85. A possible provision on the conditions for the insertion in the trusted list could read as follows:

> 1. Where IdM and trust service providers intend to start providing their services, they shall submit to […] [the supervisory body] a notification of their intention together with a certification.
>
> 2. The certification shall indicate at a minimum the following:
>
> (a) Type of assessment report;
>
> (b) Qualification of the assessing entity;
>
> (c) Technical specifications and formats used for the delivery of the services, including with reference to levels of assurance and to messaging standards.
>
> 3. [The supervisory body] […] shall establish, maintain and publish trusted lists including information related to the IdM and trust service providers and the services provided by them.

86. The Working Group may wish to consider whether the word "certification" in the draft provision may refer also to self-certification, which may be appropriate for services associated with a lower level of assurance (see A/CN.9/WG.IV/WP.154, paras. 3–9).

87. The draft provision requires the designation of the entity maintaining the trusted list. This could be a national entity if a mechanism for the notification of responsible national entities is established.

88. With regard to the legal effects of the insertion in the trusted list, some useful elements could be gathered from article 12 MLES. Moreover, a provision on effects of legal recognition could also incorporate the principle that foreign identity and trust services should be recognized only if they provide a level of assurance equal to or higher than that required in the country where recognition is sought (so-called "principle of reciprocity"). A possible provision could read as follows:

> An identity or trust service provided outside [receiving State] and listed in the trusted list established according to article … shall have the same legal effect in [receiving State] as an identity or trust service provided in [receiving State] [of equivalent [level of assurance][…]].

89. The Working Group may wish to consider whether additional guidance should be given with respect to the use of the mapping process and reference to the notion of levels of assurance to determine the legal effect of the foreign identity and trust service. In that context, the Working Group may wish to consider whether reference to the notion of "substantially equivalent level of reliability", contained in article 12 MLES, would be appropriate.

90. In its deliberations, the Working Group may wish to consider various examples of use of IdM schemes. As this issue may arise both in domestic and in cross-border transactions, the Working Group may wish to consider both scenarios. In particular, it may wish to consider the frequent challenges that seem to arise from the need to comply with mandatory requirements established by public authorities that may not be addressed easily in contractual agreements. For instance, as illustrated above (paras. 80–83), a bank may wish to know which IdM schemes may be used to satisfy KYC requirements.

91. To sum up, elements possibly relevant for a legal recognition mechanism include: notification and insertion in a trusted list; requirements to be met, including with reference to levels of assurance; use of certification to provide evidence that requirements are met; central oversight and licensing authority; mapping exercise.

92. The Working Group may wish to consider on which approach a legal recognition mechanism should be based. In doing so, it may also wish to further discuss whether that legal recognition mechanism should apply only across borders or also across systems in a domestic context (see above, para. 60).

2. Trust services

93. With respect to trust services, several legal mechanisms have been devised to achieve legal recognition of electronic signatures. In that respect, it should be noted that, according to one view, not all electronic signatures are the output of trust services, but only those requiring the involvement of a third party trust service provider may be considered so. According to another view, all electronic signatures are the output of trust services. The Working Group may wish to clarify the matter.

94. With respect to UNCITRAL texts, functional equivalence rules on electronic signatures (see above, para. 36) provide legal recognition at the domestic level.

95. Regarding cross-border legal recognition, article 12 MLES, based on a "substantive equivalence" approach,[12] requires that no discrimination should arise from the foreign elements of the electronic signature. Article 9(3) ECC specifies the requirements to establish functional equivalence between handwritten and electronic signatures, but does not, per se, determine the legal status of the signature in the jurisdiction where recognition is sought.[13]

96. Another mechanism for cross-border recognition of electronic signatures relies on the conclusion of a dedicated international agreement or, under delegated authority, of a memorandum of understanding. For instance, article 14 eIDAS requires that trust services provided by providers established outside the European Union may be recognized as legally equivalent to those provided by qualified providers established in the European Union, only if recognized under an international agreement. Section 19 of the Information Technology Act, 2008, of India allows for recognition of foreign certifying authorities as follows:

> "(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognize any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.
>
> (2) Where any Certifying Authority is recognized under sub-section (1), the Electronic Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.
>
> (3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) he may [sic], for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition."

97. Other methods to ensure cross-system or cross-border recognition of electronic signatures based on public key infrastructure ("PKI") are cross-recognition and cross-certification.[14] Cross recognition is an interoperability arrangement in which the relying party in the area of a PKI can use authority information in the area of another PKI to authenticate a subject in the area of the first PKI.[15] Cross-certification refers to the practice of recognizing another certification services provider's public

---

[12] More information on substantive equivalence is available in the UNCITRAL publication *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. 158–161.

[13] *Explanatory Note to the United Nations Convention on the Use of Electronic Communications in International Contracts* (United Nations publication, Sales No. E.07.V.2), para. 156.

[14] More information on cross-recognition and cross-certification is available in the publication *Promoting confidence in electronic commerce*, cit., paras. 165–172.

[15] *Promoting confidence in electronic commerce*, cit., para. 165.

key to an agreed level of confidence, normally by virtue of a contract.[16] Those contract-based methods may be supported by a dedicated statutory provision. For instance, article 43 of the Law 527 of 1999 of Colombia indicates that:

> Digital signatures certificates issued by foreign certification authorities may be recognized under the same terms and conditions required by the law for the issuance of certificates by national certification authorities, provided that such certificates are recognized by an authorized national certification authority that guarantees the correctness of the details of the foreign certificate as well as the foreign certificate's validity and effectiveness in the same way as its own certificates.

98. The above mechanisms have been available for some time but have not yet managed to fully enable cross-border recognition of electronic signatures. The MLES has been enacted by a limited number of States and often without adopting article 12. Participation of States in the ECC, although steadily increasing, is still limited. Statutory-based mutual recognition mechanisms are time and resource-intensive and have been used sparingly. PKI-based cross-recognition and cross-certification apply only to those certification authorities negotiating them, and, if not supported by statutory provisions in all concerned jurisdictions, may not satisfy mandatory legislative requirements.

[16] *Promoting confidence in electronic commerce*, cit., para. 169.