United Nations A/CN.9/WG.IV/WP.171

General Assembly

Distr.: Limited
10 September 2021

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Sixty-second session
Vienna, 22–26 November 2021

Explanatory Note to the Draft Provisions on the Use and Cross-border Recognition of Identity Management and Trust Services

Note by the Secretariat

Contents

V.21-06688 (E)

I. Introduction

1. At its sixty-first session, the Working Group requested the secretariat to present draft explanatory materials together with revised draft provisions for consideration by the Working Group at its sixty-second session. Those materials are set out in the explanatory note contained in the annex.

2. The explanatory note has been prepared by the secretariat for comment and eventual adoption by the Working Group. It contains a record of the deliberations of the Working Group, as reported to the Commission, as well as additional contextual information related to the mandate of the Working Group. It refers to the draft provisions that are contained in document A/CN.9/WG.IV/WP.170 and will be revised to reflect any amendments to those provisions – and any comments – that are agreed by the Working Group at its sixty-second session. The explanatory note may also assist the Working Group in finalizing the draft provisions.

Annex

Explanatory Note to the Draft Provisions on the Use and Cross-border Recognition of Identity Management and Trust Services

I. Introduction

A. Purpose of this Explanatory Note

1. [To be completed.]

B. Objectives

2. The last twenty years have seen an exponential growth in the value of online commercial activity (i.e., electronic transactions between businesses, businesses and consumers and businesses and governments). Global e-commerce grew from $64 billion in 1999 to $29 trillion in 2017.[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 builds on trust – and 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 the development of various systems, methods, technologies and devices that are used to create and manage digital identities of natural and legal persons. Addressing the legal aspects of identity management (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. There are obstacles to the broader use of IdM and trust services. Obstacles of a legal nature include: (1) a lack of legislation giving legal effect to IdM and trust services; (2) divergent legal 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.[3]

5. The main objective of the [draft instrument] 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 contribute to bridging the digital divide through harmonized solutions.

6. By doing so, the [draft instrument] 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

[1] UNCTAD, E-Commerce and Development Report 2001, UN Doc UNCTAD/SDTE/ECB/1, p. 44; UNCTAD, Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries, UN Doc UNCTAD/DER/2019, p. 15.

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

[3] A/CN.9/965, para. 52

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 in accordance with Sustainable Development Goal 9, which deals with fostering innovation, among other things.

C. Scope

7. [To be completed.]

D. Structure

8. The [draft instrument] consists of four chapters, dealing respectively with general provisions, IdM, trust services and international aspects. Chapters I and IV apply both to IdM and to trust services. Moreover, the structure and content of chapters II and III have significant similarities. Hence, the explanation of a provision of chapter II may also apply to the corresponding provision of chapter III, to the extent that the provisions coincide. This may apply, in particular, to articles 13, 14, 15, 22, 23 and 24, with respect to articles 5, 6 and 7, 8, 10, 11 and 12, respectively.

9. Chapter I contains the definition of certain terms used in the [draft instrument]; the delimitation of the scope of application; provisions on the voluntary use of IdM and trust services, including of particular services; provisions on the relationship between the [draft instrument] and other laws, including requirements to identify or to use specified trust services; and provisions on the autonomous interpretation, including for gap-filling purposes, of the [draft instrument] in light of its uniform nature and international origin.

10. Chapter II establishes the basic elements of the legal regime applicable to IdM, lists certain core obligations of IdM service providers and of subscribers, and sets rules on liability of IdM service providers. Article 5 establishes the principle of legal recognition of electronic identification and non-discrimination against IdM. Article 6 lists the core obligations of IdM service providers; in doing so, it identifies the main steps in the IdM life cycle. Article 7 deals with the obligations of the IdM provider in case of data breach and is complemented by article 8, on the obligations of subscribers in case identity credentials are compromised. Article 9 contains a rule for functional equivalence between offline and electronic identification that requires the use of a reliable method. The reliability of the method is assessed with an ex post determination based on the circumstances listed in article 10 or with an ex ante designation according to article 11. Moreover, if the method has in fact fulfilled its function, a determination of its reliability is not required. Finally, article 12 deals with the liability of IdM service providers.

11. Chapter III establishes the basic elements of the legal regime applicable to the use of trust services. Article 13 contains a general rule on non-discrimination against the legal effects of trust services. Article 14 sets the obligations of trust service providers and article 15 deals with the obligations of trust service subscribers in case the trust service has been compromised. Articles 16 to 21 describe the functions pursued with certain named trust services (electronic signatures; electronic seals; electronic timestamps; electronic archiving; electronic registered delivery services; website authentication) and associated requirements, including the use of a reliable method. The provisions on named trust services are mostly drafted as functional equivalence rules. However, since a trust service may not have a paper-based equivalent, it does not necessarily require a functional equivalence rule. Article 22 provides guidance on ex post determination of reliability of the method used for the trust service and article 23 on its designation ex ante. Finally, article 24 contains rules on liability of trust service providers.

12. Chapter IV deals with enabling cross-border recognition of IdM and trust services, which is one of the main goals of the [draft instrument]. The [draft instrument] does not contemplate the establishment of a dedicated body for legal

recognition of IdM and trust services, but foresees several mechanisms based on a decentralized approach. Besides articles 25 and 26, the dedicated provisions in articles 10(3), 11(4), 22(3) and 23(4), relating to non-geographic discrimination in determining reliability of IdM and trust services and in designating reliable IdM and trust services, are directly relevant. Contractual agreements may also be relevant in enabling cross-border use of IdM and trust services.

E. Background

1. Drafting History

13. [See paras. 4–20 of A/CN.9/WG.IV/WP.169].

14. [To be completed.]

2. Relationship with earlier UNCITRAL texts

15. Earlier UNCITRAL texts do not contain provisions on trust services. However, they do contain functional equivalence rules that may be relevant for certain trust services. In particular, article 7 MLEC, article 6 MLES, article 9(3) ECC and article 9 MLETR set out the requirements that electronic signatures must comply with in order to be functionally equivalent to paper-based ones. Article 16 of the [draft instrument] is based on article 9 MLETR. Similarly, article 10 MLEC sets out the requirements for functional equivalence of retention of information. Article 19 of the [draft instrument] is based on article 10(1) MLEC.

16. Articles 16 to 21 of the [draft instrument] refer to trust services that aim to provide assurance of certain qualities of a data message. However, not all trust services covered in those provisions have equivalent paper-based notions. Moreover, it may not be necessary to use a trust service named in the [draft instrument] to satisfy the functional equivalence rules contained in those earlier UNCITRAL texts.

F. Key concepts and principles

17. This section explains several key concepts and principles that underpin the [draft instrument]. Further explanation of defined terms used in the [draft instrument] is set out in the commentary on article 1 below, while a more expansive list of terms and concepts relevant to IdM and trust services compiled on the basis of definitions contained in internationally agreed legal and technical texts is available in document A/CN.9/WG.IV/WP.150. As indicated in that document, those texts may employ different defined terms for the same concept or define the same term differently.

1. Fundamental principles

18. Like earlier UNCITRAL texts, the [draft instrument] is based on the principles of party autonomy, technology neutrality, functional equivalence and non-discrimination against the use of electronic means, subject to adjustments. [4] While the [draft instrument] does not explicitly identify those general principles, they frame key provisions of the text. For instance, the principle of non-discrimination, as it applies to IdM and trust services, is embodied in articles 5 and 13, respectively, while the principle of functional equivalence has informed articles 9 and 16-21.

19. The functional equivalence approach presupposes the existence of legal requirements that directly or indirectly prescribe some physical or paper-based activity, such as the use of a paper-based credential to identify a person or a paper-based communication to authenticate a fact or thing. It then analyses the purposes and functions of those requirements with a view to determining how those purposes or functions could be fulfilled by electronic means. However, just as digital technology has facilitated a range of activities that do not have paper-based

[4] A/CN.9/902, paras. 52 and 63.

equivalents, some of the IdM and trust services covered in the [draft instrument] may not have a paper-based equivalent.

2. Identity management (IdM)

20. Identification is the process of distinguishing a person by reference to information relating to that person (i.e. attributes). That information may be collected or observed. Identification is particularly important to build trust in online transactions. At its core, identification involves verifying that collected or observed attributes match an "identity" previously established for the person being identified. Identification in this sense is often carried out in response to claiming a particular identity and presenting attributes for verification.

21. Accordingly, under the [draft instrument] IdM involves two distinct stages (or phases) – first, the issuance of identity credentials, i.e. data that may be presented for electronic identification; second, the presentation and verification of those credentials by electronic means:

(a) The first stage of IdM involves the collection of attributes that may comprise the person's "foundational identity" (i.e., attributes that are recorded by government agencies in civil registration and vital statistics systems for natural persons and company and business registries for legal persons). These attributes may be presented in the form of government-issued credentials (e.g., a certificate of registration) verified with the issuing agency. This process, which may be carried out "offline" based on physical credentials presented in-person, results in the issuance of credentials to the person;

(b) The second stage of IdM involves the presentation of those credentials by electronic means and the verification by electronic means that the person presenting the credentials is the person to whom the credentials were issued in the first stage.

22. IdM systems are used to manage the identification processes associated with each of those stages, as well as to manage the attributes collected, credentials issued, and the means used for verification. IdM systems may involve a single entity performing all processes involved in each stage of IdM, or multiple entities performing these processes. Moreover, some IdM systems may offer different IdM "services" according to the needs of the parties (i.e., the party seeking to identify and the party seeking to be identified).

23. IdM systems are used to provide IdM services. IdM systems may be operated by public or private entities and may offer multiple IdM services. In practice, public IdM systems generally correspond to a single IdM service, while private IdM systems may correspond to multiple IdM services with different levels of reliability. Another classification of IdM systems pertains to their centralized or distributed nature. The [draft instrument] is technology and model neutral and may therefore be applied to all types of IdM systems and services.

24. IdM service providers, subscribers, relying parties and other concerned entities may agree to operate under compatible policies, standards and technologies, which are specified in system rules, so that credentials provided by each participating IdM service provider can be understood and trusted by all participating relying parties. This arrangement may be referred to as "identity federation" and the system rules, which are of a contractual nature, as "trust framework". Identity federation may contribute to increasing the number of users and of applications sharing the same IdM services, which, in turn, may assist in containing costs and in ensuring long-term sustainability.

3. Trust services

25. Trust services are likewise of critical importance in building trust in the use of electronic transactions. At their core, trust services are concerned with providing assurance as to certain qualities of data messages, such as source, integrity, and time of processing a certain action with respect to data. While the [draft instrument]

identifies certain trust services commonly used, it acknowledges that other trust services may exist or may be developed in future.

26. The notion of trust service in the [draft instrument] is concerned with the delivery of a service and not merely with that service. For instance, it is concerned with services that support the methods for creating and managing an electronic signature, and not merely with the electronic signature.

4. Determination of reliability

27. Consistent with earlier UNCITRAL texts, several provisions of the [draft instrument] make reference to the use of a reliable method. The [draft instrument] foresees two mechanisms to assess the reliability of the method: articles 10 and 22 provide an indicative list of factors relevant for determination of reliability; articles 11 and 23 provide for a mechanism for designation of reliable methods. This approach builds upon articles 6 and 7 MLES.

28. In combining determination and designation, the [draft instrument] does not favour one mechanism over the other but aims to combine the advantages of both mechanisms while minimizing their disadvantages and to ultimately enable the parties' choice of the preferred solution.

29. Not all UNCITRAL texts dealing with trust services contain provisions enacting both the ex ante and the ex post approaches. However, ex ante and ex post approaches are generally considered compatible and complementary.

(a) Ex post determination of reliability

30. The determination of reliability operates only in case of dispute, hence after the method has been used (ex post). In this manner, the [draft instrument] generally enables IdM transactions and limits the need for a determination of the reliability of the method used to cases of dispute on the validity of a transaction due to absence of or insufficient identification of one or more parties.

31. The ex post approach has the benefit of providing maximum flexibility in the choice of technologies and methods to parties. Moreover, it may be administered in a decentralized manner and does not require the establishment of an institutional mechanism, thus avoiding associated costs.

32. On the other hand, the ex post approach has the disadvantage of not promoting legal certainty in advance and therefore does not provide parties with predictability on the validity of the method used, thus potentially exposing them to additional risks in case the method used is considered unreliable. Moreover, it leaves the determination of the reliability of the method to a third-party adjudication process, which may be time-consuming and may lead to inconsistent decisions.

(b) Ex ante designation of reliable services

33. The designation of reliable services takes place before the method is used (ex ante), against a list of predetermined conditions, and in general terms rather than with reference to a specific transaction. The further determination of the conditions set in the [draft instrument] should not result in the imposition of technology-specific requirements.

34. Designation does not pertain to generic types of IdM and trust services or to all IdM and trust services offered by an IdM service provider or a trust service provider, but rather to a particular service provided by a specific service provider.

35. The ex ante approach may provide a higher level of clarity and predictability on the legal effect of IdM and trust services, including when used across borders, than the ex post approach. However, its governance should allow rapid adjustment to technological evolution to avoid hindering innovation. Otherwise, it may discriminate those IdM and trust services that, although available and based on reliable methods, are not designated.

36. The enacting jurisdiction must identify the entity in charge of designation, which may be a private or public body. Designating entities may be accredited according to technical standards applicable to bodies certifying products, processes and services. Certification (including self-certification) is also useful to assess services using outcome-based standards and may therefore be relevant for their designation.

37. The institutional mechanism needed to implement the ex ante approach requires a dedicated mechanism for designation that is often centrally managed. Such mechanism shall include various elements such as criteria to evaluate services, details of the decision-making evaluation process and funding sources. Depending on several factors including institutional arrangements, governance of that licensing system may be complex and costly. For that reason, designation may be preferably applied to services that provide a higher level of assurance and reliability and are therefore used for higher value transactions. For enacting jurisdictions wishing to implement the ex ante approach, the [draft instrument] presupposes the existence of the necessary institutional mechanism and does not make provision for its establishment or administration.

5. International aspects

38. Legally enabling cross-border use of IdM and trust services is one of the main goals pursued by the [draft instrument]. This is done through the application of the principles of technology neutrality and non-discrimination against geographic origin. These principles inform articles 10(3), 11(4), 22(3) and 23(4) of the [draft instrument]. Moreover, chapter IV (articles 25 and 26) deals specifically with cross-border recognition.

39. The [draft instrument] does not require the establishment of a formal institutional arrangement for cross-border legal recognition. However, examples of such arrangements exist at a regional and bilateral level. Enacting jurisdictions may wish to use the [draft instrument] as a template for establishing an institutional arrangement with international partners, including under a dedicated agreement.

40. The [draft instrument] may also assist in implementing mutual legal recognition provisions contained in free trade agreements or in dedicated digital economy agreements.

II. Article-by-article commentary

A. Chapter I – General provisions (articles 1 to 4)

1. Article 1. Definitions

41. Article 1 contains definitions of terms used in the [draft instrument].[5]

“Attribute”

42. “Attribute” means an item of information or data relating to a person. Examples of attributes of a natural person include name, address, age, and electronic address, as well as data such as network presence and device used. Examples of attributes of a legal person include corporate name, principal office address, registration name, jurisdiction of registration. The notion of attribute is used in the definition of identity.

[5] A list of terms and concepts relevant to IdM and trust services compiled on the basis of definitions contained in internationally agreed legal and technical texts has been prepared in support of the preparation of the [draft instrument] and is available in document A/CN.9/WG.IV/WP.150.

43. Attributes may contain personal data whose treatment is the object of data privacy and protection law. The [draft instrument] does not deal with data privacy and protection and expressly preserves the application of that law.

References

A/CN.9/WG.IV/WP.150, para. 13.

"Data message"

44. The definition of "data message" may be found in all existing UNCITRAL texts on electronic commerce. The term is the main reference point to define the requirements of trust services since the result of the application of a trust service is the assurance of the qualities of a data message.

References

A/CN.9/1045, para. 40.

"Electronic identification" ["Authentication"]

45. The term "electronic identification" refers to the verification of the binding between the purported identity and the credentials presented, which is the second stage of IdM. The term "electronic identification" is used instead of the term "authentication" to address the concerns on the multiple meanings attributed to the term "authentication". In technical usage, the term "authentication" refers to presenting evidence of the identity.

46. The term "identification" without qualifier is used in a non-technical sense in article 9.

References

A/CN.9/1005, paras. 13, 84–86, 92; A/CN.9/1045, paras. 134 and 136; A/CN.9/1051, para. 67.

"Identity"

47. The definition of "identity" is at the core of the notion of IdM and refers to the ability to uniquely distinguish a natural or legal person in a particular context. It is therefore a notion relative to the context. This definition is drawn from that contained in Recommendation ITU-T X.1252, clause 6.40.

References

A/CN.9/WG.IV/WP.150, para. 31; A/CN.9/1005, para. 108.

"Identity credentials"

48. "Identity credentials" are the data or the physical object containing the data presented for identity proofing. Examples of digital credentials include usernames, smart cards, mobile identity and digital certificates, biometric passports, and electronic identity cards. Identity credentials in electronic form may be used online or offline depending on the features of the IdM system. The term "identity credentials" is broadly synonymous with the term "electronic identification means" used in regional and national legislation (e.g., in article 3(2) eIDAS Regulation).

References

A/CN.9/1005, para. 110; A/CN.9/1045, para. 137.

"IdM services"

49. The definition of "IdM services" reflects the understanding that IdM comprises two stages (or phases): "identity proofing" and "electronic identification". The definition of IdM services refers to services that relate to either or both stages as the use of the term "or" in that definition is not disjunctive. Article 6(a), on the core obligations of the IdM service provider, describes the various phases and steps that are comprised in the provision of IdM services.

References

A/CN.9/1005, paras. 84 and 109.

"IdM service provider"

50. The IdM service provider is the natural or legal person providing IdM services by carrying out, directly or through subcontractors, the functions listed in article 6. However, not all the functions listed in that article may be relevant to all IdM systems and therefore an IdM service provider does not need to perform each listed function.

References

A/CN.9/971, para. 97; A/CN.9/1005, para. 111; A/CN.9/1045, para. 88.

"IdM system"

51. The definition of "IdM system" describes the system used for managing IdM by carrying out identity proofing and electronic identification. It refers to "functions and capabilities" consistent with ITU terminology, namely, Recommendation ITU-T X.1252, clause 6.43. Unlike the definition of "IdM services", the definition of "IdM system comprises necessarily both stages, even if different service providers are involved at each stage.

References

A/CN.9/1005, para. 112.

"Identity proofing"

52. The term "identity proofing" refers to the first stage of IdM and includes enrolment, which is the process used by IdM service providers to verify the identity claims of a subject before issuing a credential to such subject. It is used instead of the term "identification" to address the concerns on the multiple meanings of "identification".

References

A/CN.9/1005, para. 84.

"Subscriber"

53. The term "subscriber" refers to the person to whom services are provided and does not include relying parties. It presupposes the existence of a contract between the service provider and the subscriber. For instance, the signatory of an electronic signature falls within the definition of "subscriber".

References

A/CN.9/1005, paras. 43 and 96; A/CN.9/1045, paras. 18 and 22.

"Trust service"

54. The definition of "trust service" combines an abstract description of the function pursued with the use of trust services, which focuses on a service providing the

assurance of quality of data such as veracity and genuineness, with a non-exhaustive list of the trust services that are named in the [draft instrument]. The adoption of a non-exhaustive lists allows for the application of the general rules on trust services to future types of trust services.

55. The reference to "methods for creating and managing" clarifies that the notion of "trust service" refers to the services provided and not to the result deriving from the use of those services. The trust service is not, for example, the electronic signature itself (i.e. the data identifying the signatory and indicating their intention in respect of the information contained in the underlying data message), but rather the service that supports the electronic signature (i.e. the service providing the methods for the signatory to create the electronic signature and to provide assurance as to the fulfilment of the functions required of the electronic signature).

References

A/CN.9/965, paras. 101–106; A/CN.9/971, paras. 110–111; A/CN.9/1005, paras. 14–18; A/CN.9/1051, paras. 35–40.

"Trust service provider"

56. The trust service provider is a natural or a legal person that provides trust services. A certification service provider within the meaning of the MLES provides an example of a trust service provider with respect to electronic signatures. Unlike for IdM service providers (article 6), the [draft instrument] does not identify the functions to be carried out by trust service providers.

57. The [draft instrument] does not require the use of a third-party trust service provider as a condition for legal recognition. If a third-party trust service provider is not used, the same entity may have the roles of trust service provider and of subscriber.

References

[To be completed.]

2. Article 2. Scope of application

58. Article 2 delimits the scope of application of the [draft instrument] by referring to the use and cross-border recognition of IdM systems and trust services in the context of commercial activities and trade-related services. The term "trade-related services" aims to capture transactions that are closely related to trade but that are not commercial in nature. Those transactions may involve public entities such as customs authorities operating a single window for import and export formalities.

59. As the use of IdM and trust services has implications beyond commercial transactions, enacting jurisdictions may expand the scope of the [draft instrument] to all types of transactions.

60. In line with the general principle underlying UNCITRAL texts on electronic commerce that favours avoiding or minimizing modifications to existing substantive law, paragraph 2(a) clarifies that the [draft instrument] does not introduce any new obligations to identify.

61. Paragraph 2(b) and (c), indicating that the [draft instrument] does not require the use of any particular IdM or trust service, implements the principles of technology neutrality, including with respect to neutrality of models and systems.

62. Paragraph 3 preserves those legal requirements that demand the use of a certain procedure for identification or the use of a specified trust service. Such typically regulatory requirements include, for instance, the request of a specific identity document (e.g., a passport) or of an identity document with certain features corresponding to relevant attributes (e.g. an identity card with photo and date of birth of the holder). Identification requirements may also demand that identification is

carried out by a certain person with specific functions. When electronic identification is admitted, the relevant regulators often require the use of a specified IdM procedure or trust service such as identity credentials issued by a public authority.

63. Given its enabling nature, the [draft instrument], like existing UNCITRAL model laws, does not affect the application to IdM and trust services of other law that may govern those activities or some substantive aspects of transactions carried out using identity and trust services. Paragraph 4 specifies that principle with respect to data privacy and protection law, which is specifically mentioned because of its relevance. The provision does not refer to privacy in other contexts.

References

A/74/17, para. 172; A/CN.9/936, para. 52; A/CN.9/965, para. 125; A/CN.9/971, para. 23; A/CN.9/1005, para. 115; A/CN.9/1045, paras. 76–78.

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

64. Article 3 indicates that the [draft instrument] does not impose the use IdM or trust services to a person who has not agreed to using IdM or trust services. However, such an agreement may be inferred from a party's conduct, for instance when opting for the use of a specific electronic commerce software or electronic communications system supported by IdM and trust services.

65. The principle of voluntary use of IdM and trust services is related to the principle of party autonomy as both principles are based on will. Consent to the use of IdM and trust services may not coincide with consent to treatment of personal information under data privacy and protection law.

66. Article 3, which is based on article 8(2) ECC, prevents the imposition of any new obligation to use IdM and trust services on the subscriber, on the service provider and on the relying party. This is in line with the general rule that no amendment to substantive law is intended.

67. An obligation to use IdM and trust services may exist in other law. Such obligation may be imposed in transactions with public entities or in transactions involving compliance with regulatory obligations.

References

A/CN.9/965, paras. 22 and 110; A/CN.9/1005, para. 116; A/CN.9/1045, para. 79.

4. Article 4. Interpretation

68. Article 4 is based on provisions found in several earlier UNCITRAL treaties and model laws, including those on electronic commerce (art. 3 MLEC; art. 4 MLES; art. 5 ECC; art. 3 MLETR).

69. Paragraph 1 aims to promote uniform interpretation across enacting jurisdictions. It does so by drawing the attention of judges and other adjudicating bodies to the fact that domestic enactments of the [draft instrument] should be interpreted in light of their international origin and the need for uniformity of application. Adjudicators are therefore encouraged to take into account decisions originating from foreign jurisdictions when deciding cases with a view to contributing to the consolidation of transnational uniform interpretive trends.

70. Paragraph 2 aims to preserve uniformity in the interpretation and application of the enactments of the [draft instrument] by requiring that questions not expressly settled in it should be settled in conformity with the general principles on which the [draft instrument] is based, rather than principles found in domestic law.

71. Similar to other UNCITRAL legislative texts on electronic commerce, the [draft instrument] does not explicitly identify the general principles on which it is based. The principles of non-discrimination against the use of electronic means, technology

neutrality, functional equivalence and party autonomy generally underpin UNCITRAL legislative texts on electronic commerce and have been identified as relevant also for the [draft instrument], subject to adjustments. For instance, while party autonomy is a fundamental principle of commercial law, its application is subject to limitations set out in mandatory law, including those provisions of the [draft instrument] that the parties may not derogate to. Moreover, as noted above (para. 20), the principle of functional equivalence may not find application when an offline requirement does not exist.

References

A/CN.9/936, paras. 67 and 72; A/CN.9/1005, paras. 117–118; A/CN.9/1051, paras. 53–56.

B. Chapter II – Identity management (articles 5 to 12)

1. Article 5. Legal recognition of IdM

72. Article 5 gives legal recognition to IdM by indicating that the electronic form of identity proofing and electronic identification shall not, by itself, prevent their legal effect, validity, enforceability or admissibility as evidence. Thus, paragraph 1 implements the general principle of non-discrimination against the use of electronic means with respect to IdM. The principle applies regardless of the existence of an offline equivalent.

73. Article 5 prohibits discrimination against electronic identification as the outcome of the IdM process. Its title refers to “legal recognition”, rather than to “non-discrimination”, to maintain uniformity with the title of corresponding provisions in existing UNCITRAL texts.

74. Subparagraph (b) specifies that the fact that the IdM service is not a designated service does not prevent its legal recognition. In other words, subparagraph (b) gives equal legal recognition to IdM services that are designated and to those that are not designated, thus ensuring neutrality with respect to the approach chosen to assess reliability. However, subparagraph (b) does not imply that any IdM service uses reliable methods and therefore provides a sufficient level of assurance for electronic identification: in order to achieve that outcome, the reliability of the method used needs to be assessed according to articles 10 and 11, as the case may be.

75. The reference to article 2, paragraph 3 in the chapeau of article 5 emphasizes that article 5 does not affect any legal requirement that a person be identified in accordance with a procedure defined or prescribed by law. Article 2, paragraph 3 qualifies not only article 5 but also all other provisions of the [draft instrument].

References

A/CN.9/965, paras. 107–108; A/CN.9/1005, paras. 79–86; A/CN.9/1045, paras. 17 and 82–84.

2. Article 6. Obligations of IdM service providers

76. Article 6 lists the obligations of IdM service providers. Those listed are the fundamental obligations of the IdM service provider, which may be supplemented by additional statutory or contractual obligations. Non-performance of these obligations may engage liability according to article 12 and affect the reliability of the IdM service, including a designated one.

77. Moreover, article 6 aims to ensure that the IdM service provider remains responsible for the full suite of IdM services provided to the subscriber, although certain functions could be carried out by other entities such as contractors or discrete IdM service providers in multi-party private sector IdM systems. Article 6 does not

prevent the IdM service provider from outsourcing any function or from allocating risk among its contractors or other business partners.

78. IdM systems may vary significantly in purpose and design, and in services offered. In turn, the design of the IdM system may depend also on the model chosen. Accordingly, not all obligations listed in article 6 may apply to all IdM service providers: rather, the design of the IdM system and the type of IdM services provided will determine which obligations apply to a specific IdM service provider. This flexibility in the design of IdM systems approach is reflected in the words "as appropriate to the purpose and design".

79. The obligations are described in a technology-neutral manner as the implementation of the principle of technology neutrality in the context of IdM calls for minimum IdM system requirements that refer to system properties rather than to specific technologies.

80. In business practice, the functions listed in article 6 would ordinarily be governed by contract-based operating rules, especially when private sector IdM service providers are involved. Those rules, which provide guidance on how operations should be carried out, are based on policies, implemented through practices, and reflected in contractual agreements. The obligation to "have in place operational rules, policies and practices" acknowledges that business practice. Because of their legal and practical importance, letter (d) requires that operational rules, policies and practices should be easily accessible to subscribers and third parties.

81. The principle that the service provider should be bound by its representations and commitments has been enshrined in article 9(a) MLES, which establishes an obligation of the certification service provider to "act in accordance with representations made by it with respect to its policies and practices".

References

A/CN.9/936, para. 69; A/CN.9/1045, paras. 85–95.

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

82. Article 7 establishes fundamental obligations for IdM service providers in case of data breach that has a significant impact on the IdM system. The obligations under article 7 apply regardless of purpose and design of the IdM system and cannot be varied by contract, including in the operational rules. Security breaches may affect both IdM systems and IdM services and may also impact the attributes managed in the IdM system.

83. The notion of "data breach" refers to a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, data transmitted, stored, or otherwise processed. It may be defined in data privacy and protection law.

84. The notion of "significant impact" is used in regional[6] and national laws. Several factors may contribute to the assessment of the impact. Breach notification forms assist in assessing the impact by clarifying its duration, the type of data and the percentage of subscribers affected, and other relevant information. Technical guidelines for incident reporting, as well as annual reports on security incidents, are also available.

85. Acknowledging that measures other than full suspension might be appropriate, article 7 requires the IdM service provider to "take all reasonable steps" to respond to and contain a security breach.

[6] Article 19(2) of the 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 ("eIDAS Regulation).

86. Paragraph 1(c) establishes a duty to notify security breaches, which is an aspect of the principle of transparency. A proper security breach notification mechanism is important for improving performance and increasing the level of confidence in IdM and trust services.

87. Certain aspects of the obligations contained in article 7, such as identification of the parties to be notified of the breach, timing and content of the notification, and disclosure of the breach and of its technical details, may be specified in national law, in contractual agreements and in the operational rules, policies and practices of the IdM service provider.

88. The obligations established in article 7 may coincide with obligations under data privacy and protection law. In that case, all actions listed, not just notification, should be performed in accordance with applicable data privacy and protection law.

89. Article 7 applies concurrently with data privacy and protection law as well as any other law applicable to the given event. For instance, data breach notifications have elements in common with security breach notifications, but also significant differences.

References

A/CN.9/971, paras. 84–87; A/CN.9/1005, paras. 32–36 and 94; A/CN.9/1045, paras. 96–101.

4. Article 8. Obligations of subscribers

90. Article 8 sets the obligations of the subscribers with respect to notification of the compromise, or of the risk of compromise, of the identity credentials. These obligations complement those of the IdM service provider to provide a means for notification of security breaches (article 6 (e)) and to react to security breaches or loss of integrity (article 7).

91. The obligation of the subscriber in case of data breach arises in case the identity credentials have been compromised, or there is a qualified possibility that they may have been compromised. This event is therefore different from the event that establishes the obligations of the IdM service provider in case of data breach, which is the occurrence of a breach of security or loss of integrity that has a significant impact on the IdM service.

92. Reference to a probability that the identity credentials may have been compromised aims at ensuring that no unreasonably high expectation of technical expertise is imposed on subscribers. The obligation to notify should arise only in circumstances known to the user that give rise to a justified doubt as to whether the identity credentials operate appropriately.

93. The contract between the subscriber and the IdM service provider may contain additional obligations of the subscriber. That contract may also contain additional information on how the obligation to notify contained in article 8 may be complied.

94. The reference to “otherwise using reasonable means” indicates that the subscriber is not limited to using the communication channels provided by the IdM service provider.

95. The notion of “compromised identity credentials” refers to instances of unauthorized access to the identity credentials.

96. Paragraph (b) aims to address those cases where the subscriber does not have actual knowledge of the compromise but has reasons to believe this may have happened. It is inspired by article 8(1)(b)(ii) MLES, which contains similar obligations for the signatory.

References

A/CN.9/936, para. 68; A/CN.9/971, paras. 88–96; A/CN.9/1005, paras. 37–43 and 95–96; A/CN.9/1045, paras. 102–105.

5. Article 9. Identification of a person using IdM

97. In UNCITRAL texts on electronic commerce, functional equivalence rules establish the conditions that an electronic record, method or process must meet to fulfil a paper-based legal requirement. Article 9 provides a functional equivalence rule for those cases where the law requires identification, or the parties agree to identify one another. Since the goal of this provision is to establish conditions for equivalence between offline and online identification, article 9 applies only if an offline identification equivalent exists. Article 9 is nevertheless a core provision for establishing a legal regime for IdM.

98. In line with established principles in UNCITRAL texts, this functional equivalence rule complements the rule on legal recognition set out in article 5. However, while article 5 applies to all forms of electronic identification, regardless of the existence of an offline identification equivalent, the object of article 9 is electronic identification as a functional equivalent of offline identification and therefore article 9 may operate only with reference to a paper-based equivalent.

99. Article refers to the use of IdM services to indicate that the equivalence requirements are satisfied with the use of identity credentials, as opposed to the use of IdM systems or of identity itself.

100. Article 9 does not affect requirements to identify according to a specific method or procedure, as set out in article 2(3). Those requirements may relate to regulatory compliance, such as those set by banking and anti-money-laundering regulations (see para. 62 above).

101. Electronic identification may be used to satisfy a requirement to verify particular attributes of one person's identity, such as age or residence, as required by physical-based identification. In that regard, since the notion of "identity" is defined with reference to "context", which in turn determines the attributes required for identification, the successful identification of a person based on article 9 includes verification of the required attributes. The need to verify the relevant attributes is reflected also in the words "for that purpose". Verification of particular attributes is not addressed by the provisions on reliability contained in article 10 as those provisions are concerned with the processes in managing identity credentials rather than with the attributes contained in identity credentials.

102. Articles 9 and 16 to 21 of the [draft instrument] refer to instances where the law requires or provides consequences for the absence of an action. This formulation, which is used in article 9 ECC, has been drafted to accommodate functional equivalence rules in cases where the law does not require, but attaches legal consequences to certain actions, and covers also instances where the law permits certain actions (see article 9 MLETR).

References

A/CN.9/965, paras. 62–85; A/CN.9/971, paras. 24–49; A/CN.9/1005, paras. 97–100; A/CN.9/1045, paras. 106–117; A/CN.9/1051, paras. 42–44.

6. Article 10. Reliability requirements for IdM services

103. Article 10 provides guidance on the determination of the reliability of the method used for identification in article 9 after the method has been used (ex post approach).

104. Paragraph 1(a) implements the ex post approach by referring to the use of a method that is "as reliable as appropriate for the purpose for which the IdM service is being used". This provision reflects the understanding that reliability is a relative

notion. However, unlike certain trust services that may pursue multiple functions, electronic identification pursues only one function, which is reliable identification with electronic means. That function may be pursued for different purposes, each associated with a different level of reliability.

105. Paragraph 1(b) contains a clause aimed at preventing repudiation of the IdM service when it has in fact fulfilled its function. Repudiation occurs when a subject declares not having performed an action. For the mechanism contained in paragraph 1(b) to operate, the method, whether reliable or not, must have in fact fulfilled the identification function, i.e., associate the person seeking identification with the identity credentials. This provision is based on article 9(3)(b)(ii) ECC.

106. Paragraph 2 contains a list of circumstances, described in technology neutral terms, that may be relevant for the determination of reliability by the adjudicator. Since the list is illustrative and not exhaustive, additional circumstances may be relevant. Moreover, not all listed circumstances may be relevant in all cases where reliability is to be determined. In particular, the relevance of the agreement of the parties may vary significantly depending on the level of recognition that the relevant jurisdiction gives to party autonomy in the field of identification. In addition, contractual agreements may not affect third parties and that circumstance would therefore not be relevant when third parties are involved.

107. Paragraph 3 specifies that the location where the IdM service is provided and the place of business of the IdM service provider are not relevant per se for the determination of the reliability. This provision aims at facilitating the cross-border recognition of IdM services and is inspired by article 12(1) MLES, which establishes a general rule of non-discrimination in determining the legal effectiveness of a certificate or electronic signature. For a discussion of the interaction between articles 12(1) and 12(2) MLES, see A/CN.9/483, paras. 28–36.

108. According to paragraph 4, the designation of a reliable IdM service according to article 11 gives a presumption of reliability to the methods used by the designated IdM service. This is the only distinction between designated and non-designated IdM services. Moreover, according to paragraph 5(b) the presumption of reliability attached to designation may be rebutted.

109. Paragraph 5 clarifies the relationship between articles 10 and 11 by specifying that the existence of a designation mechanism does not exclude the operation of an ex post determination of reliability of the method. The provision is inspired by article 6(4) MLES.

(a) Level of assurance framework

110. Article 10 and article 11 refer to the notion of “level of assurance” or similar frameworks otherwise named. The level of assurance provides guidance to relying parties on the degree of confidence that they may place in the identity proofing and electronic identification processes and whether they are adequate for specific purposes. The [draft instrument] neither defines levels of assurance nor requires them to be defined or used.

111. Levels of assurance frameworks foresee different levels of assurance that are associated with different requirements. In other words, levels of assurance frameworks describe the requirements that IdM systems and services must meet to provide a certain level of assurance in their reliability. Levels of assurance should be described in generic terms to preserve technology neutrality.

112. In turn, the requirement of a certain level of assurance of the reliability of the identities used may be expressed by reference to the levels described in a level of assurance framework. Specific IdM systems and services may then be mapped against the requirements of the required level of assurance. The successful match between the IdM service and the requirements associated with that level of assurance results in the possibility of using that IdM service for that particular type of transaction.

(b) Certification and supervision

113. Article 10 lists among the possibly relevant circumstances the existence of "supervision or certification provided with regard to the IdM service", if any. Certification and supervision may significantly assist in establishing confidence in IdM service providers and their services, including for the purpose of determining the reliability of the method used, as they are associated with a certain level of objectivity in assessing the reliability of the method used. This has already been acknowledged in article 12(a)(vi) MLETR and in article 10(f) MLES.

114. Certification options include self-certification, certification by an independent third party, certification by an accredited independent third party, and certification by a public entity. The choice of the most appropriate form of certification is influenced by the type of service involved, the cost and the level of assurance sought. In a business-to-business context, business partners should be able to choose the option most appropriate for their needs, recognizing that each option would produce different effects.

115. The existence of a supervisory mechanism for IdM systems and services may be considered useful or even necessary to create confidence in IdM. However, establishing a supervisory body entails administrative and financial consequences that may be costly. The [draft instrument] does not mandate or facilitate the establishment of a supervisory regime.

116. Different approaches exist with respect to the involvement of public authorities in certification and supervision, which is a policy decision for the enacting jurisdiction. The approach taken in the [draft instrument] is based on model neutrality and references to certification and supervision do not exclude self-certification regimes. When public entities are both certifiers or supervisors and IdM service providers, the certificatory and supervisory functions may be separated from the provision of IdM services.

117. In some cases, such as when certain types of distributed ledger technology are used, any solution presupposing a central certification, accreditation or supervision body may not be appropriate because of challenges in identifying the entity able to request the certification, to be assessed and in charge of taking corrective and enforcement actions, among others.

References

A/CN.9/965, paras. 40–55 and 112–115; A/CN.9/971, paras. 50–61; A/CN.9/1005, para. 101; A/CN.9/1045, paras. 118–124; A/CN.9/1051, paras. 47–49; A/CN.9/WG.IV/WP.153, paras. 74–75.

7. Article 11. Designation of reliable IdM systems [and services]

118. Article 11 complements article 10 by offering the possibility to designate IdM systems [and services]. More precisely, it lists the conditions that an IdM system [or service] must satisfy to be included on a list of designated IdM systems [and services].

119. Designation of IdM systems [and services] using reliable methods is based on all relevant circumstances, including those listed in article 10 for the determination of the reliability of the method. Reference to the circumstances listed in article 10 ensures some degree of consistency between methods designated reliable ex ante and methods determined reliable ex post. Moreover, designation shall "be consistent with recognized international standards and procedures relevant for performing the designation process" to promote cross-border legal recognition and interoperability.

120. Information on designated IdM systems [and services] is critical to inform potential subscribers of their existence. The designating entity has an obligation to publish a list of the designated IdM systems [and services], including details of the IdM service provider, for instance on its website, or otherwise inform the public of the designation. The relevance of lists in ensuring transparency on the designation of

IdM services, including in the cross-border context, is acknowledged also in widely used technical standards.

121. Paragraph 2(a) refers to standards and procedures relevant for determining reliability and aims to ensure a certain uniformity in the outcome of ex ante and ex post assessments of reliability. On the other hand, paragraph 3 refers explicitly to standards and procedures relevant for designation, such as conformity assessments and audits, which are specific to the ex ante approach.

122. Similar to article 10(3), paragraph 4 specifies that the location where the IdM system [or service] is provided and the place of business of the IdM service provider are not relevant per se for the designation of a reliable service. Paragraph 4 is therefore also based on article 12(1) MLES, which establishes a general rule of non-discrimination in determining the legal effectiveness of a certificate or electronic signature. In practice, this provision allows a foreign IdM service provider to request designation of the IdM system [or service] to the competent authority of the enacting jurisdiction, as indicated also in article 25(3).

References

A/CN.9/965, paras. 40–55; A/CN.9/971, paras. 68–76; A/CN.9/1005, paras. 102 and 105; A/CN.9/1045, paras. 125–129.

8. Article 12. Liability of IdM service providers

123. The liability regime may have a significant impact on promoting the use of IdM and trust services and is a core element of the [draft instrument]. Article 12 establishes a single liability regime of IdM service providers towards subscribers based on the principle that an IdM service provider should be held liable for the consequences of failing to provide the services as required by law and agreed by contract.

124. Article 12 is based on three elements: (a) it does not affect the application of mandatory law, including mandatory obligations of the IdM service provider under the [draft instrument]; (b) it establishes liability of the IdM service provider for breach of its mandatory obligations regardless of whether those obligations have also a contractual footing; and (c) it acknowledges the possibility to limit liability under certain conditions.

125. The nature of the liability under article 12 is statutory and, as such, it is separate from liability under contract law. Its goal is to recognize that the service provider could be liable for failing to comply with its obligations under the [draft instrument] regardless of whether those obligations also had a contractual footing. The provision applies regardless of the public or private nature of the IdM service provider.

126. The liability of IdM service providers may arise from the use of both designated and non-designated IdM services. However, it is not absolute. For instance, an IdM service provider may not be liable to a subscriber if the loss was caused by the use of what the subscriber knew, or ought to have known, that was at the time a compromised credential.

127. Matters relating to liability and not dealt with in article 12 are left to applicable law outside the draft provisions. Those matters include standard of care and degree of fault, burden of proof, determination of the amount of damages and of compensation, etc.

128. Article 12 acknowledges the possibility to limit liability under certain conditions, namely that a limitation on the purpose or value of the transaction for which the IdM service is used exists, and that the subscriber has been notified of that limitation.

129. Limitations of liability may be necessary to contain the cost of insurance, among others. Limitations of liability are agreed upon in the contract between service provider and subscriber. In practice, they are typically reflected in the operational rules, policies and practices of the service provider.

130. The extent to which an IdM service provider may be able to limit its liability is determined by the applicable law. The [draft instrument] does not affect the application of any law that restricts the right of a service provider to limit its liability or set conditions for such limitations.

131. Paragraph 3(b) does not aim at introducing a new obligation to inform but signals that the provision does not override more stringent notice requirements under applicable law. That law will determine any applicable information requirement, such as notification or explicit approval.

132. Article 12 only deals with the liability of IdM service providers towards subscribers. A third party suffering a loss arising from the use of IdM services could seek redress under existing liability rules either against the service provider or against the subscriber. In the latter case, the subscriber could then claim against the IdM service provider.

133. Article 12 does not limit the ability of the service provider to limit liability towards third parties under other law. Article 6(d) requires the service provider to make its operational rules, policies and practices easily accessible also to third parties. However, the [draft instrument] does not specifically require the service provider to inform relying third parties of limitations of liability as the prior identification of those third parties may be challenging.

134. Article 12 applies to IdM service providers regardless of their public or private nature. An enacting jurisdiction may need to adapt this provision to any special rule on liability of public entities. Article 12 does not apply to public entities performing supervisory functions and managing civil records and vital statistics that may provide foundational identity credentials.

References

A/CN.9/936, paras. 83–86; A/CN.9/965, paras. 116–118; A/CN.9/971, paras. 98–107; A/CN.9/1005, para. 76; A/CN.9/1045, paras. 130–131; A/CN.9/1051, paras. 13–29.

C. Chapter III – Trust services (articles 13 to 24)

1. Article 13. Legal recognition of trust services

135. Article 13 establishes a general rule on non-discrimination against the result deriving from the use of a trust service, namely an assertion as to certain qualities of a data message. The reference to the result deriving from the use of a trust service aligns it with the approach taken in article 5, which gives legal recognition to electronic identification as the result of the use of IdM.

136. Article 13 applies to trust services regardless of whether they are named in the [draft instrument] and operates independently of the existence of a functional equivalence rule.

References

A/CN.9/971, paras. 112–115; A/CN.9/1005, paras. 19–26; A/CN.9/1045, paras. 16–17.

2. Article 14. Obligations of trust service providers

137. Article 14 establishes core obligations of trust service providers regardless of whether the trust service is named or not. Contractual agreements may specify and complement, but not deviate from these core obligations. This approach is akin to the one adopted in articles 6 and 7 on the obligations of IdM service providers.

138. The reference to operational rules, policies and practices “as appropriate to the purpose and design of the trust service” acknowledges that the obligations of the trust service providers vary in light of the diversity in design and function of each trust service.

139. The obligation to make policies and practices available also to third parties reflects existing practice acknowledging that such information is relevant to relying parties when deciding whether to accept the result deriving from the use of a trust service, in line with the principle of voluntary use of trust services (articles 2(2)(c) and 3(1)).

140. Limitations on the purpose or value of the transaction for which the trust service may be used are usually reflected in the operational rules governing the trust service, which comprise also the policies and practices of the trust service provider. Paragraph 1(c) aims therefore also at fulfilling the duty of transparency towards third parties with respect to applicable contractual limitations. A similar provision is found in article 9(1)(d)(ii) MLES.

References

A/CN.9/971, paras. 152–153; A/CN.9/1005, paras. 28–36 and 73; A/CN.9/1045, paras. 18–21, 57.

3. Article 15. Obligations of subscribers

141. Article 15 establishes the obligations of subscribers in case of compromise of the trust service. The [draft instrument] does not identify additional obligations of the subscribers with respect to the use of the trust service. An example of such obligations may be found in article 8(1)(a) and (c) MLES.

142. Article 15 establishes the obligations of subscribers in case trust services are compromised while article 14(2) establishes the obligations of trust service providers in case of data breach. The notion of "compromised trust service" refers to instances of unauthorized access to the trust service. Accordingly, article 15 presupposes the occurrence an event that affects the reliability of the trust service while article 14 presupposes a breach of security or loss of integrity that has a significant impact on the trust service.

143. The contract concluded between the trust service provider and the subscriber typically provides details on how to comply with the obligations listed in article 15. Such contractual agreements usually refer to the policies and practices of the trust service provider.

144. The [draft instrument] does not contain liability rules for subscribers. Therefore, contractual provisions, which may specify additional obligations of the subscribers, and general liability rules will determine the subscriber's liability.

145. Unlike certain provisions in earlier UNCITRAL texts (see article 11 MLES), article 15 does not establish obligations of third parties, which may be held liable under other law.

References

A/CN.9/1005, paras. 37–43; A/CN.9/1045, paras. 22–26.

4. Article 16. Electronic signatures

146. Article 16 deals with electronic signatures. All UNCITRAL legislative texts on electronic commerce contain provisions on the use of electronic signatures, which may be affixed by both natural and legal persons. The formulation of article 16 is inspired by that of article 9 MLETR, which, in turn, takes into account that of article 9(3) ECC.

147. The requirement for a paper-based signature is satisfied if a method is used to identify the signatory of the data message and to indicate the signatory's intention in respect of the signed data message. The reference to the use of the method "in respect of information contained in the data message" applies to both identification of the person and indication of the person's intention.

148. Electronic signatures may be used to pursue a variety of purposes such as identification of the originator of a message and association with its content. Several technologies and methods that may satisfy the requirements of an electronic signature are available. In a commercial setting, the parties may identify the most appropriate electronic signature technology and method in light of costs, level of security sought, allocation of risks and other considerations. Earlier UNCITRAL texts have discussed in depth purposes and methods of electronic signatures (Guide to Enactment to MLES, paras. 29–62; Promoting Confidence, paras. 24–66).

References

A/CN.9/971, paras. 116–119; A/CN.9/1005, paras. 44–51; A/CN.9/1045, para. 34; A/CN.9/1051, para. 50.

5. Article 17. Electronic seals

149. Electronic seals provide assurance of the origin and integrity of a data message that originates from a legal person. In practice, they combine the function of a generic electronic signature with respect to origin, and that of certain types of signature, typically based on the use of cryptographic keys, with respect to integrity. The existence of such electronic signatures is reflected in 6(3)(d) MLES. Accordingly, the description of the integrity requirement contained in article 17 is based on article 6(3)(d) MLES.

150. Article 17 is inspired by regional legislation, according to which "In addition to authenticating the document issued by the legal person, electronic seals can be used to authenticate any digital asset of the legal person, such as software code or servers." (eIDAS Regulation, recital 65).

151. The assurance of the origin of the data message may be achieved by establishing its provenance, which, in turn, requires identification of the legal person originating the data message. The method used for the identification of the legal person affixing the seal is the same used for identifying a signatory, and UNCITRAL provisions on electronic signatures have been usually enacted as applicable to both natural and legal persons.

152. Moreover, provisions contained in UNCITRAL texts, require integrity to achieve functional equivalence of the paper-based notion of "original". In particular, article 6(3)(d) 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.

153. In light of the above, it is possible that jurisdictions that have already enacted UNCITRAL provisions on electronic signatures that provide assurance as to integrity may not distinguish between the functions pursued with the use of an electronic signature and those pursued with the use of an electronic seal. This may also reflect the business practice of using hybrid methods combining electronic signatures and electronic seals.

Integrity

154. Integrity is an essential component of electronic seals and of electronic archiving and may be an optional component of other trust services. In earlier UNCITRAL texts, integrity is a requirement to achieve functional equivalence with the paper-based notion of "original" (article 8 MLEC). Articles 17 and 19 are inspired by article 8(3) MLEC with respect to requirements for ensuring integrity.

References

A/CN.9/971, paras. 124–128; A/CN.9/1005, paras. 52–54 and 58; A/CN.9/1045, paras. 35–36 and 56–58.

6. Article 18. Electronic timestamps

155. Electronic timestamps provide evidence of the date and the time when the stamp has been bound with data. Typically, the law attaches consequences to the fact that the date and time of a certain event may not be proven with a sufficient level of confidence. For instance, the date of conclusion of a contract may need to be proven for opposability to third parties.

156. Timestamps are typically affixed in connection with certain actions such as generation of an electronic record in its final form, signature, dispatch and receipt of an electronic communication, etc. The requirement to specify a time zone may but does not need to be satisfied by referring to Coordinated Universal Time (UTC).

157. Article 18 contains a reference to "data" besides "documents, records, information". That reference aims to capture instances when timestamps are associated with data that is not contained in a document or record, and that is not presented in an organized manner as information.

References

A/CN.9/971, paras. 129–134; A/CN.9/1005, para. 55.

7. Article 19. Electronic archiving

158. Article 19 deals with electronic archiving services, which provide legal certainty on the validity of retained electronic records. The method used for electronic archiving shall provide guarantee as to the integrity of the archived electronic records as well as to the date and time of the archiving. Moreover, the information archived should be accessible according to the requirement for functional equivalence with the paper-based notion of "writing" (article 6(1) MLEC).

159. Article 19 is inspired, among others, by article 10 MLEC, dealing with retention of data messages. However, article 10 MLEC refers to "retention" of data messages because it is concerned with satisfying the paper-based legal requirement to retain documents, while article 19 refers to "archiving" because it deals with the trust service provided to satisfy that requirement (i.e., electronic archiving).

160. Archived data messages do not need to have been sent or received and may be retained by the originator.

161. The transmission and retention of data messages may require for technical reasons additions and modifications to the data message that do not alter its integrity. Such additions and modifications are permitted so long as the content of the data message remains complete and unaltered. In particular, paragraph (a)(ii) accommodates file migration and format changes that are part of ordinary data retention practices. Its formulation is based on article 8(3)(a) MLEC.

162. Article 19 does not deal with the issue of whether archived electronic records should be capable of being migrated so that access is possible despite technological obsolescence. That result follows by applying the principle of technology neutrality and the requirements for functional equivalence to the notion of "integrity", so 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).

References

A/CN.9/971, paras. 135–138; A/CN.9/1005, paras. 56–61; A/CN.9/1045, paras. 37–41.

8. Article 20. Electronic registered delivery services

163. Article 20 provides assurance of the dispatch of an electronic communication by the sender and of its receipt by the addressee, of the time when dispatch and receipt occurred, of the integrity of the data exchanged, and of the identity of sender and recipient.

164. Electronic registered delivery services are the equivalent of registered mail services as both types of services are used to prove transmission of communications. To ensure security and privacy of electronic exchanges, the recipient should be identified before being granted access to the electronic communication.

165. Article 20 does not refer to notions that are used in earlier UNCITRAL texts such as “dispatch” and “receipt” (see article 10 ECC) because it has been drafted by focusing on the functional equivalence between registered mail services and electronic registered delivery services rather than the underlying notions.

References

A/CN.9/971, paras.139–141; A/CN.9/1005, paras. 62–64; A/CN.9/1045, paras. 42–44.

9. Article 21. Website authentication

166. Article 21 deals with website authentication, whose essential function is to associate a website with the person to whom the domain name has been assigned or licensed to confirm the trustworthiness of the website. Hence, website authentication comprises two elements: identification of the domain name holder for the website and association of that person with the website. Website authentication does not aim at identifying the website.

167. Article 21 is not a functional equivalence rule since a website exists only in electronic form and therefore website authentication does not have an offline equivalent.

168. The term “person who holds the domain name” refers to persons who have been assigned or licensed to use the domain name by a domain name registrar. That person does not need to be the website “owner”, content provider or operator.

169. Additional safeguards may be needed in cases where a domain name is used for a platform that hosts web pages created and managed by different persons. For instance, the platform operator may need to identify the persons according to a certain procedure to maintain the authentication of the website.

References

A/CN.9/971, paras. 142–144; A/CN.9/1005, paras. 65–66; A/CN.9/1045, paras. 47–48.

10. Article 22. Reliability requirements for trust services

170. Article 22 contains a non-exhaustive list of circumstances that may be relevant to determine the reliability of the method used according to the ex post approach. The list is inspired by lists contained in article 10 MLES and in article 12 MLETR.

171. Similar to the notion of reliable method used for IdM services (see para. 104 above), the notion of reliable method used in trust services is relative and varies according to the purpose pursued. The relative nature of reliability is reflected in paragraph 1(a), namely in the words “as reliable as appropriate”, which, according to a well-established UNCITRAL usage, aim to better reflect the various uses of trust services, as well as in the reference to “the purpose for which the trust service is being used”.

Levels of reliability

172. The MLES and several national laws on electronic signatures distinguish between trust services based on the level of reliability that they offer. Specifically, these laws attach greater legal effect to electronic signatures that satisfy certain requirements and therefore are deemed to offer a higher level of reliability. Moreover, certain laws may require that only electronic signatures offering a higher level of reliability may be designated. This approach has not been followed in the [draft instrument] and trust services may be designated regardless of the level of reliability they offer.

173. Since identity credentials offering a high level of assurance may be used for trust services with different levels of reliability, there is no direct correlation between level of assurance of an IdM service and level of reliability of a trust service.

References

A/CN.9/965, para. 106; A/CN.9/971, paras. 120–121; A/CN.9/1005, paras. 67–68 and 73; A/CN.9/1045, paras. 18–21, 27–29, 52–57, 61; A/CN.9/1051, paras. 45–46.

11. Article 23. Designation of reliable trust services

174. Article 23 complements article 22 by allowing designation of trust services according to the ex ante approach. More precisely, it lists the conditions that an IdM service must satisfy to be included on a list of designated IdM services presumed reliable for the purposes of articles 16 to 21.

175. Article 23 focuses on the designation of trust services on the understanding that the process for designating trust services necessarily involves an assessment of those methods. Similar to designation of IdM services, designation of trust services that are presumed using reliable methods does not pertain to generic types of trust service or to all the trust services offered by a specific trust service provider, but rather to a specific trust service provided by an identified service provider.

176. Since the only legal effect of designation is the presumption of reliability of the method used, the use of trust services that have been designated, but have lost such designation, prevents the concerned party from availing itself of that presumption, but does not have consequences on the determination of the reliability of the method.

177. Article 23 requires the designating authority to publish a list of designated trust services, including details of the trust service providers. The purpose of such obligation is to promote transparency and inform potential subscribers of the trust service. Enacting jurisdictions may wish to consider manners to aggregate those lists so that the information could be found in centralized supranational repository, along the lines of existing regional examples.

References

A/CN.9/971, paras. 150–152; A/CN.9/1005, paras. 69–73; A/CN.9/1045, paras. 30–33, 58–61.

12. Article 24. Liability of trust service providers

178. 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. Several factors, including the type of trust service provided, concur to determine the extent of that liability. As for other provisions of the [draft instrument], article 24 does not affect liability for non-compliance with obligations arising outside the [draft instrument].

179. In certain cases, identification of the trust service provider may be challenging or impossible (e.g., timestamping services used in conjunction with distributed ledger technology) and therefore liability may not be allocated. In those cases, the system may provide other manners to establish confidence in the use of the trust service.

180. Regarding earlier UNCITRAL texts, the MLES contains provisions dealing with legal consequences 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.

References

A/CN.9/1005, paras. 74–76; A/CN.9/1045, paras. 62–66.

D. Chapter IV – International aspects (articles 25 and 26)

1. Article 25. Cross-border legal recognition

181. Article 25 establishes a system for cross-border legal recognition of IdM and trust services based on granting the same legal treatment to domestic and foreign IdM systems, identity credentials, IdM services and trust services. It is based on the principle of non-discrimination against geographic origin.

182. One goal of article 25 to reduce the need for service providers to apply to be designated in multiple jurisdictions under article 23. This may be particularly useful in those jurisdictions that rely on the use of national technical standards that, as such, may not be identical to foreign technical standards. Mutual recognition of certification, where available, may play an important role in implementing this provision.

183. The reference to "level of reliability" in article 25 encompasses both the notion of level of assurance, a term of art for the assessment of IdM services, and that of level of reliability, a term of art for the assessment of trust services. In turn, those notions may be relevant for determining the reliability of a service or for designating a reliable service according to chapters II and III.

184. The [draft instrument] does not establish a common set of levels of assurance for IdM systems and of levels of reliability for trust services because of the challenges in agreeing on globally accepted definitions. Moreover, different laws and business practices in setting those definitions exist across jurisdictions, in particular with respect to the role of central authorities vis-à-vis that of contractual agreements.

185. On the other hand, the determination of the level of assurance of an IdM service and of the level of reliability of a trust service is a time-consuming and resource-intensive exercise, and not all jurisdictions may dispose of adequate resources. Those jurisdictions may particularly benefit from the possibility of recognizing foreign IdM and trust services by relying on foreign determinations and designations.

186. The reference to "IdM system, IdM service or identity credential, as appropriate," aims to capture all possible aspects relevant for cross-border recognition. In practice, it may be preferable to focus on each IdM service to avoid recognizing all IdM services supported by an IdM system as equally reliable even though one or more may be of a lower level of reliability. In addition, recognition of identity credentials should avoid IdM credentials that have remained unchanged despite the IdM service used to issue them having been compromised.

187. Recognition of foreign IdM and trust services may require the service provider to adjust its terms of services. For instance, mandatory law of the recognizing jurisdiction may affect the ability of the service provider to limit liability.

188. Paragraph 1 presents two alternatives on the equivalence of the required level of reliability. The first requires at least the same level of reliability; the second, that it provides a substantially equivalent level of reliability. The reference to an "at least equivalent level of reliability" includes levels of reliability higher than the one required.

189. The notion of "substantially equivalent level of reliability" aims to capture instances where the level of reliability defined in different jurisdictions does not match exactly, which is a likely situation given the absence of universally agreed definitions of specific levels of reliability. Another concern that this notion may address relates to the possible obstacles to trade arising from demanding compliance with strict technical requirements.

190. If systems, services or credentials offer a substantially equivalent level of reliability, their reliability as determined applying the circumstances in articles 10 and 22 will likewise be equivalent. A "substantially equivalent level of reliability" includes levels of reliability higher than the one required. The notion of "substantially equivalent level of reliability" is drawn from article 12(2) MLES.

191. Paragraph 3 further clarifies how designating authorities may designate foreign IdM and trust services. It expands on the mechanisms provided in articles 11(4) and 23(4), which provide for non-geographic discrimination in the designation process, by introducing the possibility for the designating authority of the enacting jurisdiction to rely on the designation of IdM and trust services made by a foreign designating authority.

192. When adopting implementing regulations, the enacting jurisdiction may decide whether paragraph 3 should operate based on automatic recognition (e.g. IdM and trust services designated by the foreign authority would automatically have legal status as designated in the enacting jurisdiction), or in the form of a presumption (e.g. IdM and trust services designated by the foreign authority would be presumed reliable in the enacting jurisdiction, but would not have legal status as designated in that jurisdiction without further action by the designating authority).

193. Mechanisms based on article 25(3) may replace arrangements based on the conclusion of ad hoc mutual recognition agreements between supervisory bodies.

References

A/CN.9/936, paras. 75–77; A/CN.9/1005, para. 120; A/CN.9/1045, paras. 67–74; A/CN.9/1051, paras. 57–66.

2. Article 26. Cooperation

194. Institutional cooperation mechanisms may significantly contribute to achieving mutual legal recognition and technical interoperability of IdM systems and trust services. Such mechanisms exist in different forms and may have private or public nature. Cooperation may consist of exchanges of information, experience and good practice, in particular with respect to technical requirements, including levels of assurance and levels of reliability.

195. Moreover, article 26 may facilitate common definitions of technical standards, including levels of assurance and levels of reliability, that support a determination of equivalence.

References

A/CN.9/965, paras. 119–120; A/CN.9/1005, para. 122; A/CN.9/1045, para. 75; A/CN.9/WG.IV/WP.153, paras. 95–98.