United Nations A/CN.9/1112

General Assembly

Distr.: General
21 February 2022

Original: English

United Nations Commission on International Trade Law
Fifty-fifth session
New York, 27 June–15 July 2022

Draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services

Note by the Secretariat

1. At its sixty-second session (Vienna, 22–26 November 2021), Working Group IV (Electronic Commerce) concluded its third reading of the draft provisions on the use and cross-border recognition of identity management and trust services and their explanatory note.

2. At that session, the Working Group requested the secretariat to revise the draft provisions and the explanatory note to reflect its deliberations and decisions and to transmit the revised text to the Commission, in the form of a model law, for consideration at its fifty-fifth session, in 2022. The secretariat was also asked to circulate the revised text to all Governments and relevant international organizations for comment, and to compile the comments received for the consideration of the Commission (A/CN.9/1087, para. 11).

3. The revised model is set out in Annex I to this document and the revised explanatory note is set out in Annex II to this document. Revisions incorporate the deliberations of the Working Group at its sixty-second session as reported in document A/CN.9/1087.

V.22-00938 (E) 240222 250222

Annex I

Draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services

Chapter I. General provisions

Article 1. Definitions

For the purposes of this Law:

(a) "Attribute" means an item of information or data associated with a person;

(b) "Data message" means information generated, sent, received or stored by electronic, magnetic, optical or similar means;

(c) "Electronic identification" ["Authentication"], in the context of identity management services, means a process used to achieve sufficient assurance in the binding between a person and an identity;

(d) "Identity" means a set of attributes that allows a person to be uniquely distinguished within a particular context;

(e) "Identity credentials" means the data, or the physical object upon which the data may reside, that a person may present for electronic identification;

(f) "Identity management services" means services consisting of managing identity proofing or electronic identification;

(g) "Identity management service provider" means a person who enters into an arrangement for the provision of identity management services with a subscriber;

(h) "Identity management system" means a set of functions and capabilities to manage identity proofing and electronic identification;

(i) "Identity proofing" means the process of collecting, verifying, and validating sufficient attributes to define and confirm the identity of a person within a particular context;

(j) "Relying party" means a person who acts on the basis the result of identity management services or trust services;

(k) "Subscriber" means a person who enters into an arrangement for the provision of identity management services or trust services with an identity management service provider or a trust service provider;

(l) "Trust service" means an electronic service that provides assurance of certain qualities of a data message and includes the methods for creating and managing electronic signatures, electronic seals, electronic time stamps, website authentication, electronic archiving and electronic registered delivery services;

(m) "Trust service provider" means a person who enters into an arrangement for the provision of one or more trust services with a subscriber.

Article 2. Scope of application

1. This Law applies to the use and cross-border recognition of identity management and trust services in the context of commercial activities and trade-related services.

2. Nothing in this Law requires the identification of a person.

3. Nothing in this Law affects a legal requirement that a person be identified or that a trust service be used in accordance with a procedure defined or prescribed by law.

4. Other than as provided for in this Law, nothing in this Law affects the application to identity management services or trust services of any law applicable to data protection and privacy.

Article 3. Voluntary use of identity management and trust services

1. Nothing in this Law requires a person to use an identity management service or trust service or to use a particular identity management service or trust service without the person's consent.

2. For the purposes of paragraph 1, consent may be inferred from the person's conduct.

Article 4. Interpretation

1. In the interpretation of this Law, regard is to be had to its international origin 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 Law which are not expressly settled in it are to be settled in conformity with the general principles on which it is based.

Chapter II. Identity management

Article 5. Legal recognition of identity management

Subject to article 2, paragraph 3, electronic identification shall not be denied legal effect, validity, enforceability or admissibility as evidence on the sole ground that:

(a) The identity proofing and electronic identification are in electronic form; or

(b) The identity management system is not designated pursuant to article 11.

Article 6. Obligations of identity management service providers

An identity management service provider shall, at a minimum:

(a) Have in place operational rules, policies and practices, as appropriate to the purpose and design of the identity management system, to address, at a minimum, requirements to:

(i) Enrol persons, including by:

a. Registering and collecting attributes;

b. Carrying out identity proofing and verification; and

c. Binding the identity credentials to the person;

(ii) Update attributes;

(iii) Manage identity credentials, including by:

a. Issuing, delivering and activating credentials;

b. Suspending, revoking and reactivating credentials; and

c. Renewing and replacing credentials;

(iv) Manage the electronic identification of persons, including by:

a. Managing electronic identification factors; and

b. Managing electronic identification mechanisms;

(b) Act in accordance with its operational rules, policies and practices, and any representations that it makes with respect to them;

(c) Ensure the online availability and correct operation of the identity management system;

(d) Make its operational rules, policies and practices easily accessible to subscribers and third parties;

(e) Provide easily accessible means that enable a relying party to ascertain, where relevant:

(i) Any limitation on the purpose or value for which the identity management service may be used; and

(ii) Any limitation on the scope or extent of liability stipulated by the identity management service provider; and

(f) Provide and make publicly available means by which a subscriber may notify the identity management service provider of a security breach pursuant to article 8.

Article 7. Obligations of identity management service providers in case of data breach

1. If a breach of security or loss of integrity occurs that has a significant impact on the identity management system, including the attributes managed therein, the identity management service provider shall, in accordance with the law:

(a) Take all reasonable steps to contain the breach or loss, including, where appropriate, suspending the affected service or revoking the affected identity credentials;

(b) Remedy the breach or loss; and

(c) Notify the breach or loss.

2. If a person notifies the identity management service provider of a breach of security or loss of integrity, the identity management service provider shall:

(a) Investigate the potential breach or loss; and

(b) Take any other appropriate action under paragraph 1.

Article 8. Obligations of subscribers

The subscriber shall notify the identity management service provider, by utilizing means made available by the identity management service provider pursuant to article 6 or by otherwise using reasonable means, if:

(a) The subscriber knows that the subscriber’s identity credentials have been compromised; or

(b) The circumstances known to the subscriber give rise to a substantial risk that the subscriber’s identity credentials may have been compromised.

Article 9. Identification of a person using identity management

Subject to article 2, paragraph 3, where the law requires the identification of a person for a particular purpose, or provides consequences for the absence of identification, that requirement is met with respect to identity management services if a method is used for the electronic identification of the person for that purpose.

Article 10. Reliability requirements for identity management services

1. For the purposes of article 9, the method shall be:

(a) As reliable as appropriate for the purpose for which the identity management service is being used; or

(b) Proven in fact to have fulfilled the function described in article 9.

2. In determining the reliability of the method, all relevant circumstances shall be taken into account, which may include:

(a) Compliance of the identity management service provider with the obligations listed in article 6;

(b) Compliance of the operational rules, policies and practices of the identity management service provider with any applicable recognized international standards and procedures relevant for the provision of identity management services, including level of assurance frameworks, in particular rules on:

(i) Governance;

(ii) Published notices and user information;

(iii) Information security management;

(iv) Record-keeping;

(v) Facilities and staff;

(vi) Technical controls; and

(vii) Oversight and audit;

(c) Any supervision or certification provided with regard to the identity management service;

(d) Any relevant level of reliability of the method used;

(e) The purpose for which identification is being used; and

(f) Any relevant agreement between the parties, including any limitation on the purpose or value of the transactions for which the identity management service might be used.

3. In determining the reliability of the method, no regard shall be had:

(a) To the geographic location where the identity management service is provided; or

(b) To the geographic location of the place of business of the identity management service provider.

4. A method used by an identity management service designated pursuant to article 11 is presumed to be reliable.

5. Paragraph 4 does not limit the ability of any person:

(a) To establish in any other way the reliability of a method; or

(b) To adduce evidence of the non-reliability of a method used by an identity management service designated pursuant to article 11.

Article 11. Designation of reliable identity management services

1. [*A person, organ or authority, whether public or private, specified by the enacting jurisdiction as competent*] may designate identity management services that are presumed reliable.

2. The [*person, organ or authority, whether public or private, specified by the enacting jurisdiction as competent*] shall:

(a) Take into account all relevant circumstances, including the factors listed in article 10, in designating an identity management service; and

(b) Publish a list of designated identity management services, including details of the identity management service provider.

3. Any designation pursuant to paragraph 1 shall be consistent with recognized international standards and procedures relevant for performing the designation process, including level of assurance frameworks.

4. In designating an identity management service, no regard shall be had:

(a) To the geographic location where the identity management service is provided; or

(b) To the geographic location of the place of business of the identity management service provider.

Article 12. Liability of identity management service providers

1. The identity management service provider shall be liable for loss caused to the subscriber or to the relying party due to a failure to comply with its obligations under articles 6 and 7.

2. Paragraph 1 shall be applied in accordance with rules on liability under the law and is without prejudice to:

(a) any other basis of liability under the law, including liability for failure to comply with contractual obligations; or

(b) any other legal consequences of a failure of the identity management service provider to comply with its obligations under this Law.

3. Notwithstanding paragraph 1, the identity management service provider shall not be liable to a subscriber for loss arising from the use of an identity management service to the extent that:

(a) That use exceeds the limitations on the purpose or value of the transactions for which the identity management service is used; and

(b) Those limitations are contained in the arrangement between the identity management service provider and the subscriber.

4. Notwithstanding paragraph 1, the identity management service provider shall not be liable to a relying party for loss arising from the use of an identity management service to the extent that:

(a) That use exceeds the limitations on the purpose or value of the transaction for which the identity management service is used; and

(b) The identity management service provider has complied with its obligations under article 6, subparagraph (e) with respect to that transaction.

Chapter III. Trust services

Article 13. Legal recognition of trust services

The result deriving from the use of a trust service shall not be denied legal effect, validity, enforceability or admissibility as evidence on the sole ground that:

(a) It is in electronic form; or

(b) The trust service is not designated pursuant to article 23.

Article 14. Obligations of trust service providers

1. A trust service provider shall, at a minimum:

(a) Have in place operational rules, policies and practices, including a plan to ensure continuity in case of termination of activity, as appropriate to the purpose and design of the trust service;

(b) Act in accordance with its operational rules, policies and practices, and any representations that it makes with respect to them;

(c) Make its operational rules, policies and practices easily accessible to subscribers and third parties;

(d) Provide and make publicly available means by which a subscriber may notify the trust service provider of a security breach pursuant to article 15; and

(e) Provide easily accessible means that enable a relying party to ascertain, where relevant:

(i) Any limitation on the purpose or value for which the trust service may be used; and

(ii) Any limitation on the scope or extent of liability stipulated by the trust service provider.

2. If a breach of security or loss of integrity occurs that has a significant impact on a trust service, the trust service provider shall in accordance with the law:

(a) Take all reasonable steps to contain the breach or loss, including, where appropriate, suspending or revoking the affected service;

(b) Remedy the breach or loss; and

(c) Notify the breach or loss.

Article 15. Obligations of subscribers

The subscriber shall notify the trust service provider, by utilizing means made available by the trust service provider pursuant to article 14, paragraph 1 or by otherwise using reasonable means, if:

(a) The subscriber knows that data or means used by the subscriber for access and usage of the trust service has been compromised; or

(b) The circumstances known to the subscriber give rise to a substantial risk that the trust service may have been compromised.

Article 16. Electronic signatures

Where the law requires a signature of a person, or provides consequences for the absence of a signature, that requirement is met in relation to a data message if a method is used:

(a) To identify the person; and

(b) To indicate the person’s intention in respect of the information contained in the data message.

Article 17. Electronic seals

Where the law requires a legal person to affix a seal, or provides consequences for the absence of a seal, that requirement is met in relation to a data message if a method is used:

(a) To provide reliable assurance of the origin of the data message; and

(b) To detect any alteration to the data message after the time and date of affixation, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display.

Article 18. Electronic timestamps

Where the law requires a document, record, information or data to be associated with a time and date, or provides consequences for the absence of a time and date, that requirement is met in relation to a data message if a method is used:

(a) To indicate the time and date, including by reference to the time zone; and

(b) To associate that time and date with the data message.

Article 19. Electronic archiving

Where the law requires a document, record or information to be retained, or provides consequences for the absence of retention, that requirement is met in relation to a data message if a method is used:

(a) To make the information contained in the data message accessible so as to be usable for subsequent reference;

(b) To indicate the time and date of archiving and associate that time and date with the data message;

(c) To retain the data message in the format in which it was generated, sent or received, or in another format which can be demonstrated to detect any alteration to the data message after that time and date, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display; and

(d) To retain such information, if any, as enables the identification of the origin and destination of a data message and the time and date when it was sent or received.

Article 20. Electronic registered delivery services

Where the law requires a document, record or information to be delivered by registered mail or similar service, or provides consequences for the absence of delivery, that requirement is met in relation to a data message if a method is used:

(a) To indicate the time and date when the data message was received for delivery and the time and date when it was delivered;

(b) To detect any alteration to the data message after the time and date when the data message was received for delivery to the time and date when it was delivered, apart from the addition of any endorsement or information required by this article, and any change that arises in the normal course of communication, storage and display; and

(c) To identify the sender and the recipient.

Article 21. Website authentication

Where the law requires website authentication, or provides consequences for the absence of website authentication, that requirement is met if a method is used:

(a) To identify the person who holds the domain name for the website; and

(b) To associate that person to the website.

Article 22. Reliability requirements for trust services

1. For the purposes of articles 16 to 21, the method shall be:

(a) As reliable as appropriate for the purpose for which the trust service is being used; or

(b) Proven in fact to have fulfilled the functions described in the article.

2. In determining the reliability of the method, all relevant circumstances shall be taken into account, which may include:

(a) Compliance of the trust service provider with the obligations listed in article 14;

(b) Compliance of the operational rules, policies and practices of the trust service provider with any applicable recognized international standards and procedures relevant for the provision of trust services;

(c) Any relevant level of reliability of the method used;

(d) Any applicable industry standard;

(e) The security of hardware and software;

(f) Financial and human resources, including existence of assets;

(g) The regularity and extent of audit by an independent body;

(h) The existence of a declaration by a supervisory body, an accreditation body or a voluntary scheme regarding the reliability of the method;

(i) The purpose for which the trust service is being used; and

(j) Any relevant agreement between the parties, including any limitation on the purpose or value of the transactions for which the trust service might be used.

3. In determining the reliability of the method, no regard shall be had:

(a) To the geographic location where the trust service is provided; or

(b) To the geographic location of the place of business of the trust service provider.

4. A method used by a trust service designated pursuant to article 23 is presumed to be reliable.

5. Paragraph 4 does not limit the ability of any person:

(a) To establish in any other way the reliability of a method; or

(b) To adduce evidence of the non-reliability of a method used by a trust service designated pursuant to article 23.

Article 23. Designation of reliable trust services

1. [*A person, organ or authority, whether public or private, specified by the enacting jurisdiction as competent*] may designate trust services that are presumed reliable.

2. The [*person, organ or authority, whether public or private, specified by the enacting jurisdiction as competent*] shall:

(a) Take into account all relevant circumstances, including the factors listed in article 22, in designating a trust service; and

(b) Publish a list of designated trust services, including details of the trust service provider.

3. Any designation pursuant to paragraph 1 shall be consistent with recognized international standards and procedures relevant for performing the designation process.

4. In designating a trust service, no regard shall be had:

(a) To the geographic location where the trust service is provided; or

(b) To the geographic location of the place of business of the trust service provider.

Article 24. Liability of trust service providers

1. The trust service provider shall be liable for loss caused to the subscriber or to the relying party due to a failure to comply with its obligations under article 14.

2. Paragraph 1 shall be applied in accordance with rules on liability under the law and is without prejudice to:

(a) any other basis of liability under the law, including liability for failure to comply with contractual obligations; or

(b) any other legal consequences of a failure of the trust service provider to comply with its obligations under this Law.

3. Notwithstanding paragraph 1, the trust service provider shall not be liable to a subscriber for loss arising from the use of a trust service to the extent that:

(a) That use exceeds the limitations on the purpose or value of the transactions for which the trust service is used; and

(b) Those limitations are contained in the arrangement between the trust service provider and the subscriber.

4. Notwithstanding paragraph 1, the trust service provider shall not be liable to a relying party for loss arising from the use of a trust service to the extent that:

(a) That use exceeds the limitations on the purpose or value of the transaction for which the trust service is used; and

(b) The trust service provider has complied with its obligations under article 14, subparagraph 1(e) with respect to that transaction.

Chapter IV. International aspects

Article 25. Cross-border recognition of electronic identification

1. Electronic identification provided outside [*the enacting jurisdiction*] shall have the same legal effect in [*the enacting jurisdiction*] as electronic identification provided in [*the enacting jurisdiction*] if the method used by the identity management system, identity management service or identity credential, as appropriate, offers at least an equivalent level of reliability.

2. In determining whether an identity management system, identity management service or identity credential, as appropriate, offers at least an equivalent level of reliability, regard shall be had to recognized international standards.

3. For the purposes of paragraph 1, an identity management system, identity management service or identity credential shall be presumed to offer at least an equivalent level of reliability if [*the person, organ or authority specified by the enacting jurisdiction pursuant to article 11*] has determined that equivalence, taking into account article 10, paragraph 2.

Article 26. Cross-border recognition of the result of the use of trust services

1. The result deriving from the use of a trust service provided outside [*the enacting jurisdiction*] shall have the same legal effect in [*the enacting jurisdiction*] as the result deriving from the use of a trust service provided in [*the enacting jurisdiction*] if the method used by the trust service offers at least an equivalent level of reliability.

2. In determining whether a trust service offers at least an equivalent level of reliability, regard shall be had to recognized international standards.

3. For the purposes of paragraph 1, the trust service shall be presumed to offer at least an equivalent level of reliability if [*the person, organ or authority specified by the enacting jurisdiction pursuant to article 23*] has determined that equivalence, taking into account article 22, paragraph 2.

Article 27. Cooperation

[*The person, organ or authority specified by the enacting jurisdiction as competent*] may cooperate with foreign entities by exchanging information, experience and good

practice relating to identity management and trust services, in particular with respect to:

(a) Recognition of the legal effects of foreign identity management systems and trust services, whether granted unilaterally or by mutual agreement;

(b) Designation of identity management systems and trust services; and

(c) Definition of levels of assurance of identity management systems and of levels of reliability of trust services.

Annex II

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

I. Introduction

A. Purpose of this Explanatory Note

1. In preparing and adopting the UNCITRAL Model Law on the Use and Cross border Recognition of Identity Management and Trust Services (hereinafter referred to as "the Model Law"), the United Nations Commission on International Trade Law (UNCITRAL) considered that the Model Law would be more effective in harmonising and modernising legislation if accompanied by background and explanatory information.

2. This Explanatory Note, drawn from the *Travaux préparatoires* of the Model Law, aims to assist those interested in the adoption, use, and uniform interpretation of the Model Law such as policymakers, legislators, academics, practitioners, judges and arbitrators, commercial operators and users of identity management and trust services. For instance, at the time of enactment such information could assist jurisdictions in tailoring the Model Law to their needs with respect to the interaction between the provisions of the Model Law and the regulatory regime of IdM and trust services.

B. Objectives

3. In the last twenty years there has been an exponential growth in the value of online commercial activity (i.e., electronic transactions between businesses, businesses and consumers and businesses and governments). This growth, which has been further accelerated by the need to mitigate the effects of the COVID-19 pandemic,[1] is accompanied by a similar increase in data transactions and calls for an adequate legal and technical framework.

4. The growth of online commercial activities builds on trust – and needs to be supported by a continued sense of trust – in the electronic environment. One important component of that trust is the ability to identify each party in a reliable manner, especially in the absence of any prior in-person interaction. The importance of identity is acknowledged in Sustainable Development Goal 16, whose target 9 calls for the provision of legal identity for all human beings, including in electronic form. In the digital economy, this becomes the right to a digital identity.

5. Over the years, various solutions have been suggested to address the need for online identification. This has led to the development of 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 (hereinafter, "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.

6. Another important component of online trust is the ability to rely with sufficient confidence on the quality of data, which underpins data exchanges. Trust services that provide assurance on qualities of a data message such as its origin, its integrity and

[1] UNCTAD, *Digital Economy Report: Cross-border data flows and development: For whom the data flow*, UN Doc. UNCTAD/DER/2021, p. 16–17.

the time of processing a certain related action have emerged as solutions to provide that confidence.

7. Obstacles to the broader use of IdM and trust services may be of different nature. For instance, access to IdM and trust services may be limited due to cost, lack of awareness and technical constraints. 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.[2]

8. The main objective of the Model Law is to address these obstacles through the development of uniform legal rules that serve several purposes. Uniform rules may improve efficiency by promoting acceptance of the result of the application of IdM and trust services across systems; lower transactions costs by facilitating compliance with regulatory requirements; increase legal predictability and certainty of electronic transactions on the basis of a common treatment of issues, including through cross-border recognition mechanisms; and contribute to bridging the digital divide through easier availability of common solutions.

9. In particular, a legal framework for IdM and trust services will promote the secure operationalization of digital identity and data transactions. 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

10. The Model Law applies to the use and cross-border recognition of IdM and trust services in the context of commercial activities and trade-related services. Enacting jurisdictions may decide to expand the scope of application of the Model Law to non-commercial activities.

11. Many different pieces of legislation may be relevant for data exchanges. The Model Law does not aim to affect those existing laws, namely law applicable to data privacy and protection. It also does not introduce new obligations to use IdM and trust services, or any specific IdM or trust service, and does not affect any such existing requirement (see paras. 102–104 below).

12. The IdM provisions of the Model Law apply to the identification of physical and legal persons. The provisions on trust services apply to all information in the form of a data message. Both sets of provisions apply regardless of the private or public nature of the service provider, of the subscriber and of the relying party.

D. Structure

13. The Model Law 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 contained in chapter II may be relevant for 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.

14. Chapter I contains the definition of certain terms used in the Model Law; 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 Model Law and other laws, including requirements to identify or to use specified

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

trust services; and provisions on the autonomous interpretation, including for gap-filling purposes, of the Model Law in light of its uniform nature and international origin.

15. 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 IdM and non-discrimination against electronic identification . Article 6 lists the core obligations of IdM service providers; in doing so, it identifies the core obligations of IdM service providers, which correspond to the basic components of IdM systems and 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.

16. 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.

17. Chapter IV deals with enabling cross-border recognition of IdM and trust services, which is one of the main goals of the Model Law. The Model Law 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, 26 and 27, 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 relevant. Contractual agreements may also be relevant in enabling cross-border use of IdM and trust services.

E. Background

1. Drafting History

18. The Model Law originates from a request formulated by the Commission at its forty-eighth session, in 2015. At that session, the Commission requested the secretariat to conduct preparatory work on legal aspects of IdM and trust services, including through the organization of colloquiums and expert group meetings, for future discussion at the Working Group level,[3] and to share the result of such preparatory work with Working Group IV, with a view to seeking recommendations

[3] *Official Records of the General Assembly*, *Seventieth Session, Supplement No. 17* (A/70/17), paras. 354–355 and 358.

on the exact scope, possible methodology and priorities for the consideration of the Commission.[4]

19. In response to that request, at its forty-ninth session, in 2016, the Commission had before it a note by the secretariat on legal issues related to IdM and trust services (A/CN.9/891) that summarized the discussions during the UNCITRAL Colloquium on Legal Issues Related to Identity Management and Trust Services, held in Vienna on 21–22 April 2016.[5] The Commission agreed that the topic of IdM and trust services should be retained on the work agenda of the Working Group.[6]

20. Having received a mandate from the Commission, the Working Group held preliminary discussions on the topic at its fifty-fourth session (Vienna, 31 October–4 November 2016). The Working Group agreed that its future work on IdM and trust services should be limited to the use of IdM systems for commercial purposes and that it should take into account both private and public IdM service providers. The Working Group also agreed that, while work on IdM could be taken up before work on trust services, the identification and definition of terms relevant for both IdM and trust services should take place simultaneously given the close relationship between the two. It further agreed that focus should be placed on multi-party IdM systems and on the identification of natural and legal person, and that the Working Group should continue its work by further clarifying the goals of the project, specifying its scope, identifying applicable general principles and drafting necessary definitions (A/CN.9/897, paras. 118–120 and 122).

21. In line with its prior decisions, at its fifty-fifth session (New York, 24–28 April 2017) the Working Group discussed, among other things, the objectives, general principles, and scope of its work on IdM and trust services (A/CN.9/902, paras. 29–85).

22. The Commission reaffirmed the mandate given to the Working Group (see para. 19 above) at its fiftieth session, in 2017, and requested the secretariat to consider convening expert group meetings. States and international organizations were invited to share their expertise.[7] Accordingly, the secretariat convened an expert group meeting on legal aspects of IdM and trust services in Vienna on 23 and 24 November 2017.

23. Building also on the outcome of the expert group meeting, at its fifty-sixth session (New York, 16–20 April 2018), the Working Group identified the following issues as relevant for its discussion of legal aspects of IdM and trust services: scope of work; general principles; definitions; mutual recognition requirements and mechanisms; certification of IdM and trust services; levels of assurance for IdM and trust services; liability; institutional cooperation mechanisms; transparency; obligation to identify; data retention; and supervision of service providers (A/CN.9/936, paras. 61–94).

24. On the recommendation of the Working Group (A/CN.9/936, para. 95), at its fifty-first session, in 2018, the Commission requested the Working Group to conduct work with a view to preparing a text aimed at facilitating cross-border recognition of IdM and trust services, on the basis of the principles and issues identified by the Working Group (see para. 23 above).[8]

25. Accordingly, the Working Group continued its consideration of the issues that it had identified (A/CN.9/965, paras. 10–129) at its fifty-seventh session (Vienna, 19–23 November 2018).

26. A first set of draft provisions on the cross-border recognition of IdM and trust services (A/CN.9/WG.IV/WP.157) accompanied by explanatory remarks

[4] Ibid., para. 358.
[5] Ibid., *Seventy-first Session, Supplement No. 17* (A/71/17), para. 228.
[6] Ibid., paras. 235–236.
[7] Ibid., *Seventy-second Session, Supplement No. 17* (A/72/17), para. 127.
[8] Ibid., *Seventy-third Session, Supplement No. 17* (A/73/17), para. 159.

(A/CN.9/WG.IV/WP.158) was submitted for the consideration of the Working Group at its fifty-eighth session (New York, 8–12 April 2019). The Working Group considered the draft provisions on scope of application, recognition and reliability of IdM systems and trust services, types of trust services to be covered, and obligations and liability of IdM and trust service providers (A/CN.9/971, paras. 13–153).

27. At that session, the Working Group requested the secretariat to prepare, in consultation with experts, concrete proposals on matters relating to the reliability of IdM systems (A/CN.9/971, para. 67). Further to that request, the secretariat convened an expert group meeting in Vienna on 22–23 July 2019 to discuss standards and procedures that qualify an IdM system for legal recognition, as well as other matters covered in the draft provisions, notably the reliability of IdM systems, and the obligations and liability of IdM service providers.

28. The Commission expressed its satisfaction with the progress made by the Working Group at its fifty-second session, in 2019.[9] It noted that the Working Group should work towards an instrument that could apply to both domestic and cross-border use of IdM and trust services, and that the outcome of the work had implications for matters beyond commercial transactions.[10]

29. The Working Group considered a revised set of draft provisions (A/CN.9/WG.IV/WP.160), which incorporated the outcome of the secretariat's consultations with experts (see para. 27 above), at its fifty-ninth session (Vienna, 25–29 November 2019). The Working Group conducted a complete read-through of the draft provisions, focusing on those relating to trust services (A/CN.9/1005, paras. 10–122). It also held preliminary discussions on the form of the instrument, with a strong preference being expressed for the instrument taking the form of a model law as opposed to a convention (ibid., para. 123).

30. The Commission expressed again its satisfaction with the progress made by the Working Group at its fifty-third session, in 2020.[11]

31. Having before it a second revised set of draft provisions (A/CN.9/WG.IV/WP.162), the Working Group conducted a complete reading of those provisions (A/CN.9/1045, paras. 16–138) at its sixtieth session (Vienna, 19–23 October 2020). It also agreed to the possibility of holding informal consultations to discuss outstanding topics.

32. Informal consultations were held remotely with delegates and observers on 15–17 March 2021 to discuss liability, the relationship of the draft provisions with existing UNCITRAL texts, cross-border recognition, and definitions and other terminological issues.

33. The Working Group was informed of the outcome of the informal consultations at its sixty-first session (New York, 6–9 April 2021). In view of the limitations arising from the hybrid format of the session (including reduced meeting times), in considering a third revised set of draft provisions (A/CN.9/WG.IV/WP.167) it focused its deliberations on the issues discussed during the consultations (A/CN.9/1051, paras. 13–67).

34. The Commission at its fifty-fourth session, in 2021, heard that, despite reduced meeting times, the Working Group had made significant progress towards completion of the instrument. The Commission expressed its satisfaction and encouraged the Working Group to finalise its work and to submit it for its consideration at its fifty-fifth session, in 2022.[12]

35. The Working Group carried out at its sixty-second session (Vienna, 22–26 November 2021) another reading of the draft provisions (A/CN.9/1087, paras. 12–114) on the basis of a revised set (A/CN.9/WG.IV/WP.170) accompanied

[9] Ibid., *Seventy-fourth Session, Supplement No. 17* (A/74/17), para. 175.
[10] Ibid., para. 172.
[11] Ibid., *Seventy-fifth Session, Supplement No. 17* (A/75/17), part two, paras. 41 and 51(d).
[12] Ibid., *Seventy-sixth Session, Supplement No. 17* (A/76/17), chap. IX.

by an explanatory note (A/CN.9/WG.IV/WP.171). The Working Group requested the secretariat to revise the draft provisions and the explanatory note to reflect its deliberations and decisions and to transmit the revised text to the Commission, in the form of a model law, for consideration at its fifty-fifth session. The secretariat was asked to circulate the revised text to all Governments and relevant international organizations for comment, and to compile the comments received for the consideration of the Commission (A/CN.9/1087, para. 11).

36. [To be completed.]

2. Relationship with earlier UNCITRAL texts

37. There is no provision on trust services in earlier UNCITRAL texts. However, those texts set out rules on functional equivalence that may be relevant for certain trust services. Article 7 the UNCITRAL Model Law on Electronic Commerce ("MLEC"),[13] article 6 of the UNCITRAL Model Law on Electronic Signatures ("MLES"),[14] article 9(3) of the United Nations Convention on the Use of Electronic Communications in International Contracts ("ECC")[15] and article 9 the Model Law on Electronic Transferable Records ("MLETR")[16] set out the requirements that electronic signatures must comply with in order to be functionally equivalent to paper-based ones. Those provisions require identification of the signatory, which may involve the use of electronic identification and, more generally, IdM. Article 16 of the Model Law is based on article 9 MLETR.

38. Similarly, article 10 MLEC sets out the requirements for functional equivalence of retention of information, and article 19 of the Model Law is based on article 10(1) MLEC. Other UNCITRAL provisions that have been used as sources of articles of the Model Law are identified in the comment to the respective article. However, it may not be necessary to use a trust service named in the Model Law to satisfy the functional equivalence rules contained in earlier UNCITRAL texts.

39. Several matters relevant for the Model Law, such as assessment of reliability, liability and cross-border recognition mechanisms, have been discussed in detail in a guidance document on the international use of electronic signatures.[17]

F. Key concepts and principles

40. This section explains several key concepts and principles that underpin the Model Law. Further explanation of defined terms used in the Model Law 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.

---

[13] UNCITRAL, *Model Law on Electronic Commerce with Guide to Enactment, 1996, with additional article 5 bis as adopted in 1998* (1999), United Nations publication, Sales No. E.99.V.4.

[14] UNCITRAL, *Model Law on Electronic Signatures with Guide to Enactment* (2002), United Nations publication, Sales No. E.02.V.8.

[15] United Nations, *Treaty Series*, vol. 2898, p. 3.

[16] UNCITRAL, *Model Law on Electronic Transferable Records* (2018), United Nations publication Sales No. E.17.V.5.

[17] UNCITRAL secretariat, *Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods* (2007), United Nations publication, Sales No. E.09.V.4.

1. Fundamental principles

41. Like earlier UNCITRAL texts, the Model Law is based on the principles of party autonomy, technology neutrality, functional equivalence and non-discrimination against the use of electronic means, subject to adjustments.[18]

42. The principle of party autonomy allows parties to a contract to choose the applicable rules with the limits of mandatory law. It is based on the acknowledgment that those parties may be in the best position to determine the most appropriate rules for the given transaction.

43. The principle of non-discrimination, first formulated in article 5 MLEC and known also as principle of legal recognition, ensures that information is not denied legal effect, validity or enforceability solely on the grounds of its electronic form.

44. The principle of technology neutrality ensures that the law does not mandate or favour the use of any specific technology or method, thus making laws futureproof. Technology neutrality is necessary to achieve interoperability, which effectively enables dataflows. The legal underpinning of this principle is the broad definition of "data message", first set out in article 2(a) MLEC, which aims to capture all existing and future technologies.

45. The principle of functional equivalence lays out the criteria by which electronic transactions are deemed to satisfy form requirements applicable to paper-based documents such as that a document shall be in writing, original or signed. It 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. 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.

46. While the Model Law does not explicitly identify those general principles, they frame key provisions of the text. The principle of party autonomy is contained in article 3, and, the principle of non-discrimination, as it applies to IdM and trust services, is embodied in articles 5 and 13, respectively. Moreover, the principle of functional equivalence has informed articles 9, on electronic identification, and articles 16-21, on named trust services. However, some of the trust services covered in the Model Law may not have a paper-based equivalent and therefore the principle of functional equivalence would not apply to them.

2. Identity management (IdM)

47. Identification is the process of distinguishing a person from others by reference to information relating to that person (i.e., attributes). That information may be collected or observed. 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 a person claiming a particular identity and presenting attributes for its verification.

48. Accordingly, under the Model Law 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

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

"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 whose credentials are presented is the person to whom the credentials were issued in the first stage.

49. IdM systems are used to manage the identification processes associated with each of the two 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, an IdM system may offer different IdM services. Parties (i.e., the party seeking to identify and the party seeking to be identified) may select the appropriate IdM service according to need.

50. IdM systems may be operated by public or private entities. 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. In application of the principle of technology neutrality (see para. 44 above), the Model Law does not presuppose the use of any technology or model and may therefore be applied to all types of IdM systems and services.

51. 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 reduce costs, thus ensuring long-term sustainability.

3. Trust services

52. Trust services are online services that provide assurance as to certain qualities of data messages, such as source, integrity, and time of processing a certain action with respect to data. Assurance of data quality is critical to establish trust in data exchanges, which are the backbone of digital trade. The Model Law identifies certain trust services commonly used and acknowledges that other trust services may exist or may be developed in future.

53. The notion of trust service in the Model Law is concerned with the delivery of a service and not merely with the service itself. For instance, an electronic signature may be affixed by using a service that uses methods for creating and managing an electronic signature. The Model Law specifies whether it is concerned with the methods used for the delivery of the electronic signature service, rather than with the electronic signature that results from the application of that service.

4. Determination of reliability

54. Consistent with earlier UNCITRAL texts, several provisions of the Model Law refer to the use of a reliable method for the delivery of IdM and trust services. The Model Law 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.

(a) Ex ante designation of reliability

55. One possible approach to assessing the reliability of a method requires for such assessment to take 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 Model Law refers to this approach as designation of reliability and lists in articles 11 (applicable to IdM services) and 23 (applicable to trust services) the requirements for that designation, which include the same circumstances relevant for determination of reliability.

56. The object of designation is not generic types of IdM and trust services, or all IdM and trust services offered by an IdM service provider or a trust service provider, but rather a particular service provided by a specific service provider.

57. 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. However, its governance presupposes the existence of an institutional mechanism, i.e., an entity competent for the administering the designation process.

58. The enacting jurisdiction that wishes to implement the ex-ante approach 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 useful to assess services using outcome-based standards and may therefore be relevant for their designation.

59. The Model Law presupposes the existence of the institutional mechanism necessary to implement the ex-ante approach but does not make provision for its establishment or administration. 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.

60. The mechanism for designation should adjust rapidly to technological evolution to avoid hindering innovation. Otherwise, it may discriminate those IdM and trust services that, although available and based on reliable methods, have not been designated. Moreover, the further specification of the conditions for designation should not result in the imposition of technology-specific requirements.

(b) Ex post determination of reliability

61. Another possible approach to assessing the reliability of a method postpones such assessment to the moment when a dispute on the reliability has arisen. Therefore, the assessment is carried out only after the method has been used (“ex-post”). The Model Law refers to this approach as determination of reliability and lists in articles 10 (applicable to IdM services) and 22 (applicable to trust services) the requirements for that determination, including a non-exhaustive list of relevant circumstances.

62. The ex-post approach generally enables IdM transactions without prior assessment of reliability and limits the need for assessment of reliability to cases of actual dispute. It also provides maximum flexibility to parties in the choice of technologies and methods. Moreover, it may be administered in a decentralized manner and does not require the establishment of an institutional mechanism, thus avoiding associated costs.

63. On the other hand, the ex-post approach may not offer a higher level of predictability on the validity of the method used before its actual use, thus exposing the parties to the risk that the method may be 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 lead to inconsistent decisions.

(c) Combined approach

64. The Model Law combines determination and designation, thus allowing the recognition of any IdM and trust service but also providing guidance on which IdM

and trust services offer a higher degree of confidence on their reliability ("two-tier" approach). In doing so, the Model Law 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' preferred solution.

65. Not all UNCITRAL texts 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. The combined approach adopted in the Model Law builds upon articles 6 and 7 MLES.

5. Liability issues

66. The liability regime may have a significant impact on promoting the use of IdM and trust services and is a core element of the Model Law. Historically, different solutions have been adopted by legislators, ranging from the absence of a dedicated liability regime to the adoption of provisions dealing with standards of conduct and liability rules applicable to service providers only, or to all concerned parties (service providers, subscribers and relying parties).[19] The latter approach has been adopted in the MLES.[20]

67. Allocation of liability with respect to IdM and trust services is mainly done by means of contractual agreements or by statute. The latter approach may be preferred to ensure that certain provisions may not be opted out contractually. Moreover, statutory rules may apply also in absence of a contractual agreement, i.e., with respect to relying parties.

68. Articles 12 and 24 establish a uniform liability regime of service providers towards subscribers and relying parties based on the principle that a service provider should be held liable for the consequences of failing to provide its services as required by law. Accordingly, articles 12 and 24 establish a statutory basis of liability that operates alongside contractual and extracontractual liability. Moreover, the Model Law allows service providers to limit liability with respect to both subscribers and relying parties.

69. The Model Law deals neither with the degree of fault required to engage liability nor with the type and amount of recoverable damages.[21] Ordinary rules of the enacting jurisdiction would therefore apply to such issues if no special rule applicable to IdM and trust service providers is adopted at the time of enactment of the Model Law.

6. International aspects

70. The international dimension is essential to the use of IdM and trust services and, more generally, of electronic transactions. Two types of obstacles may however hinder that use: technical incompatibility leading to lack of interoperability, and legal obstacles to cross-border recognition.[22]

71. Legal obstacles may arise from conflicting national approaches, especially when the law mandates or favour a particular technology, method or product. In that case, domestic legal requirements may impede the recognition of non-compliant types of IdM and trust services. Moreover, the emergence of national technical standards – which may occur also under the "two-tier" approach, when those standards are associated with legal presumptions – may lead to a patchwork of requirements that has also the effect of hindering cross-border use.

72. Legally enabling cross-border use of IdM and trust services is one of the main goals pursued by the Model Law. This is done through the application of the principles

[19] *Promoting confidence in electronic commerce*, para. 175.
[20] For details see MLES, Explanatory Note, paras. 77–81.
[21] On these issues, see *Promoting confidence in electronic commerce*, paras. 177–193 (basis of liability: ordinary negligence, presumed negligence and strict liability) and paras. 194–201 (parties entitled to claim damages and extent of recoverable damages).
[22] *Promoting confidence in electronic commerce*, paras. 137–152.

of technology neutrality and non-discrimination against geographic origin,[23] which inform articles 10(3), 11(4), 22(3) and 23(4) of the Model Law. Moreover, chapter IV deals specifically with cross-border recognition matters. As a result, the Model Law not only discourages the adoption of technology-specific legislation but also encourages the development of interoperable technical standards, including through cooperation.

73. The Model Law, in line with the approach adopted in pre-existing UNCITRAL texts, goes beyond the mere reference to place of origin as a relevant factor for granting legal recognition to foreign IdM and trust services. More precisely, it requires ex-post determination of reliability of foreign IdM and trust services on the basis of the same circumstances to be used for similar domestic IdM and trust services. It also provides mechanisms for designation of reliability of foreign IdM and trust services on the basis of the same circumstances to be used for similar domestic IdM and trust services. In short, technical reliability, rather than place of origin, should determine whether legal recognition is to be granted.

74. The Model Law 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 Model Law as a template for establishing an institutional arrangement with international partners, including under a dedicated agreement.

75. Chapters on electronic commerce of free trade agreements typically contain provisions on electronic signatures or other forms of electronic identification, often referred to as "authentication methods", and increasingly require mutual recognition of electronic identification methods. Moreover, digital economy agreements feature a module dedicated to digital identity aimed at enabling cross-border interoperability. The enactment of the Model Law may assist in implementing those provisions of free trade and digital economy agreements.

II. Article-by-article commentary

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

1. Article 1. Definitions

76. Article 1 contains definitions of terms used in the Model Law.

"Attribute"

77. "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.

78. Attributes may contain personal data whose treatment is the object of data privacy and protection law. The Model Law 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.

[23] Technology neutrality and a non-discriminatory approach to foreign signatures and services had already been identified as principles underpinning an emerging consensus on the legal mechanisms for cross-border recognition of electronic signatures in the document *Promoting confidence in electronic commerce*, para. 149.

“Data message”

79. The definition of “data message” may be found in all existing UNCITRAL texts on electronic commerce, where it is used to implements the principle of technology neutrality (see para. 44 above). 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”]

80. The term “electronic identification” refers to the verification of the binding between the purported identity of a physical or legal person 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.

81. The disclosure of the name of the physical or legal person may not be necessary to satisfy electronic identification requirements when the verification of other attributes suffices. This is in line with the approach adopted in pre-existing UNCITRAL texts, namely the MLES, under which “for the purpose of defining ‘electronic signature’ under the Model Law, the term ‘identification’ could be broader than mere identification of the signatory by name”.[24]

82. 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”

83. 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”

84. “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).[25]

[24] MLES, Explanatory Note, para. 117.

[25] 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”).

References

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

"IdM services"

85. 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; A/CN.9/1087, para. 19.

"IdM service provider"

86. 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. The reference to the existence of an arrangement with a subscriber reminds that the IdM service provider is responsible for the full suite of services provided, regardless of whether the related functions are performed directly or contracted to third parties.

References

A/CN.9/971, para. 97; A/CN.9/1005, para. 111; A/CN.9/1045, para. 88; A/CN.9/1087, para. 22.

"IdM system"

87. 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; A/CN.9/1087, para. 19.

"Identity proofing"

88. 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. The subject may be a physical or a legal person. The term "identity proofing" is used instead of the term "identification" to address the concerns on the multiple meanings of "identification".

References

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

"Relying party"

89. The term "relying party" refers to a physical or a legal person who actually acts on the basis of the result of IdM services or trust services. For instance, the relying party is a person who acts on the basis of an electronic signature, and not on the trust service used to create the electronic signature. The definition is based on that contained in article 2(f) MLES.

References

A/CN.9/1087, paras. 55 and 72.

"Subscriber"

90. The term "subscriber" refers to the person to whom services are provided and does not include relying parties. It presupposes the existence of a relationship between the service provider and the subscriber that may be of contractual or other nature (e.g., mandated by law). 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; A/CN.9/1087, para. 23.

"Trust service"

91. 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 Model Law. The adoption of a non-exhaustive lists allows for the application of the general rules on trust services to future types of trust services.

92. 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 its 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"

93. 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 Model Law does not identify the functions to be carried out by trust service providers. The reference to the existence of an arrangement with a subscriber reminds that the trust service provider is responsible for the full suite of services provided, regardless of whether the related functions are performed directly or contracted to third parties.

94. The Model Law 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

A/CN.9/1087, para. 22.

2. Article 2. Scope of application

95. Article 2 delimits the scope of application of the Model Law 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.

96. As the use of IdM and trust services has implications beyond commercial transactions, enacting jurisdictions may expand the scope of the Model Law to all types of electronic transactions involving business, government, and consumers.

97. 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 Model Law does not introduce any new obligations to identify.

98. 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, regulators often require the use of a specified IdM procedure or trust service such as identity credentials issued by a public authority.

99. Given its enabling nature, the Model Law, like existing UNCITRAL legislative texts on electronic commerce, 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; A/CN.9/1087, para. 27.

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

100. Article 3 indicates that the Model Law 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.

101. 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 necessarily coincide with consent to treatment of personal information under data privacy and protection law.

102. 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.

103. Moreover, by indicating that the Model Law does not require the use of any particular IdM or trust service, article 3 implements the principle of technology neutrality, including with respect to neutrality of models and systems.

104. An obligation to use IdM and trust services, or a specific IdM or trust service, may exist in other law. Such obligation may be imposed, for instance, 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; A/CN.9/1087, para. 28.

4. Article 4. Interpretation

105. 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).

106. Paragraph 1 aims to promote uniform interpretation across enacting jurisdictions by drawing the attention of judges and other adjudicating bodies to the fact that domestic enactments of the Model Law 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.

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

108. Similar to other UNCITRAL legislative texts on electronic commerce, the Model Law 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 Model Law, subject to adjustments (see paras. 41–45 above). 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 Model Law that the parties may not derogate to. Moreover, as noted (para. 46 above), 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

109. 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, it 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.

110. 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.

111. 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.

112. 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 Model Law.

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

113. 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. The words “at a minimum” in the chapeau of article 6 indicate that the IdM service provider may not derogate from performance of these core obligations and that it remains liable towards subscribers and relying parties also when it avails itself of contractors for the delivery of the services. Non-performance of these obligations may engage liability according to article 12 and affect the reliability of the IdM service, including a designated one.

114. The obligations contained in article 6 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.

115. 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. Accordingly, the words “at a minimum” in subparagraph (a) indicate that the IdM service provider is required to have in place rules, policies and practices addressing the requirements to perform the listed functions. Article 6 does not prevent the IdM service provider from outsourcing any function or from allocating risk among its contractors or other business partners.

116. The principle that the service provider should be bound by its representations and commitments has already 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”.

117. 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”.

118. 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. The reference to easy accessibility, which is contained also in letter (e), aims at facilitating access to information of parties, such as micro or small enterprises, that may be less familiar with technical matters.

119. Letter (e) sets the obligations that the IdM service providers must fulfil to limit its liability towards relying parties, thus complementing article 12. This mechanism aims to prevent challenges arising from requiring prior identification of relying parties.

120. Similarly, letter (f) complements article 8 by setting the obligations that the IdM service provider must fulfil with respect to notification of security breaches by a subscriber.

References

A/CN.9/936, para. 69; A/CN.9/1045, paras. 85–95; A/CN.9/1087, paras. 30-33, 55 and 61.

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

121. 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.

122. 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 also defined in data privacy and protection law.

123. The notion of "significant impact" is used in regional[26] and national laws. Several factors may contribute to the assessment of the impact. Breach notification forms may 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 from data privacy and protection authorities.

124. 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.

125. 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.

126. 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.

127. 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 other laws – namely, data privacy and protection law –, in contractual agreements and in the operational rules, policies and practices of the IdM service provider. In that case, all actions listed, not just notification, should be performed in accordance with applicable law.

References

A/CN.9/971, paras. 84–87; A/CN.9/1005, paras. 32–36 and 94; A/CN.9/1045, paras. 96–101; A/CN.9/1087, para. 35.

[26] Article 19(2) eIDAS Regulation.

4. Article 8. Obligations of subscribers

128. 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).

129. 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. The subscriber's failure to comply with its obligations under article 8 does not necessarily release the IdM service provider from liability.

130. 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.

131. 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. The notion of "compromised identity credentials" refers to instances of unauthorized access to the identity credentials.

132. 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, and 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.

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; A/CN.9/1087, paras. 36-37.

5. Article 9. Identification of a person using IdM

133. 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.

134. The method used to fulfil the rule in article 9 must comply with article 10, paragraph 1, i.e., be as reliable as appropriate for the purpose for which the IdM service is being used or proven in fact to have fulfilled the function pursued with the use of the method.

135. 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.

136. Article 9 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.

137. 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. 98 above).

138. 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 the identity credentials.

139. Articles 9 and 16 to 21 of the Model Law 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 permits and attaches legal consequences to certain actions.

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; A/CN.9/1087, para. 38.

6. Article 10. Reliability requirements for IdM services

140. 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). It refers to the method used in an IdM service, rather than to the method used in an IdM system, because a single IdM system could support multiple IdM services that use methods with different levels of reliability.

141. 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.

142. 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.

143. The Model Law generally requires the use of reliable methods, and paragraph 1(b) does not aim to promote the use of unreliable methods, or to validate the use of those methods. Rather, it acknowledges that, from a technical perspective, function (in the case of article 9, identification) and reliability are two independent attributes, and clarifies that under the Model Law identification may be achieved in fact or by using a reliable method. In other words, achievement of identification in fact pre-empts the need to ascertain the reliability of the method used.

144. 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.

145. 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 effect of a certificate or electronic signature.[27]

146. According to paragraph 4, the designation of a reliable IdM service under 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 subparagraph 5(b) the presumption of reliability attached to designation may be rebutted.

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

(a) Level of assurance framework

148. Article 10 and article 11 refer to the notion of "level of assurance frameworks" or similar frameworks otherwise named. The level of assurance framework 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 Model Law neither defines levels of assurance nor requires them to be defined or used.

149. 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.

150. Levels of assurance frameworks may be used to address the market need for guidance on the degree of trustworthiness of the IdM service offered. An IdM service provider making no reference to levels of assurance in its operational rules, policies and practices could be considered as offering services with the lowest level of assurance. However, a globally accepted definition of level of assurance framework may not yet have been agreed upon, and different national or regional definitions may have to be used.

151. 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

152. 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

[27] For a discussion of the interaction between articles 12(1) and 12(2) MLES, see A/CN.9/483, paras. 28–36.

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.

153. 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.

154. 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.

155. Different approaches exist with respect to the involvement of public authorities in certification and supervision, which is a policy decision for the enacting jurisdiction. 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.

156. The Model Law does not mandate or facilitate the establishment of a supervisory regime. The approach taken in the Model Law is based on model neutrality and references to certification and supervision do not exclude self-certification regimes.

157. 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, the entity to be assessed and the entity 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.9/1087, paras. 42–46 and 105–106; A/CN.9/WG.IV/WP.153, paras. 74–75.

7. Article 11. Designation of reliable IdM services

158. Article 11 complements article 10 by offering the possibility to designate IdM services. More precisely, it lists the conditions that an IdM service must satisfy to be included on a list of designated IdM services. Like article 10, article 11 refers to the method used in an IdM service, rather than to the method used in an IdM system, because a single IdM system could support multiple IdM services with different levels of reliability and that therefore may or may not be designated.

159. Designation of IdM 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.

160. The dissemination of information on designated IdM services is critical to make potential subscribers aware of their existence. The designating entity has an obligation to publish a list of the designated IdM services, including details of the IdM service provider, for instance on its website. 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. Other methods may be used to inform the public of designated IdM services, but those methods should complement rather than replace the publication of a list.

161. 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.

162. Similar to article 10(3), paragraph 4 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 designation of a reliable service. Paragraph 4 is 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 service to the competent authority of the enacting jurisdiction.

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; A/CN.9/1087, paras. 47-49.

8. Article 12. Liability of IdM service providers

163. As noted (para. 68 above), article 12 sets an uniform liability regime based on the principle that an IdM service provider should be held liable for the consequences of failing to provide services to subscribers and relying parties. Its goal is to recognize that the service provider could be liable for failing to comply with its obligations under the Model Law regardless of whether those obligations had a contractual footing. The provision applies regardless of the public or private nature of the IdM service provider.

164. 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 Model Law; (b) it establishes liability of the IdM service provider for breach of its mandatory obligations regardless of whether those obligations have also a contractual basis; and (c) it acknowledges the possibility to limit liability under certain conditions.

165. The nature of the liability under article 12 is statutory and, as such, operates alongside contractual and extracontractual liability. Accordingly, the operation of provisions on contractual and extracontractual liability relevant for IdM service providers and found in domestic law is not affected by article 12, as indicated in paragraph 2(a).

166. 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.

167. 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, and determination of the amount of damages and of compensation.

168. Article 12 acknowledges the possibility to limit liability under certain conditions. Limitations of liability may be necessary to contain the cost of insurance, among others, and are typically reflected in the operational rules, policies and practices of the service provider. Article 12 also acknowledges the practice of IdM service providers to limit their liability differently depending on the party (i.e. subscriber or relying party) and type of service (e.g. high or low transaction values). It does not affect the ability of the IdM service provider to rely on other laws to give effect to a liability cap as long as it complies with its obligations under the Model Law, including those relevant for limitation of liability.

169. With respect to the subscriber, paragraph 3 allows to limit the liability of the IdM service provider under two conditions. Firstly, the use of the IdM service exceeds the limitation on the purpose or value of the transaction and on the amount of liability applicable to the transaction for which the IdM service is used. Secondly, the limitations are contained in the arrangement between the IdM service provider and the subscriber. In line with the definition of "subscriber", the reference to "arrangement" aims to capture all types of relationship between IdM service provider and subscriber, of contractual or other nature.

170. Likewise, paragraph 4 allows to limit the liability of the IdM service provider towards the relying party under two conditions. Firstly, the use of the IdM service exceeds the limitation on the purpose or value of the transaction and on the amount of liability applicable to the transaction for which the IdM service is used. Secondly, the IdM service provider has complied with its obligations under article 6(e) relating to making easily accessible the limitations to the relying parties with respect to the specific transaction.

171. Article 12 only deals with the liability of IdM service providers towards subscribers and relying parties. Another 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.

172. 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; A/CN.9/1087, paras. 52–73.

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

1. Article 13. Legal recognition of trust services

173. 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.

174. Article 13 applies to trust services regardless of whether they are named in the Model Law 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

175. Article 14 establishes core obligations of trust service providers regardless of whether the trust service provided 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. Similar to article 7(1), all obligations listed in article 14(2) shall be performed in accordance with applicable law, if any.

176. 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 may vary in light of the diversity in design and function of each trust service.

177. 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 (article 3(1)).

178. Subparagraph (1)(e) establishes a mechanism for making relying parties aware of limitations on purpose or value for which the trust service may be used, and of limitations on the scope or extent of liability, similar to that contained in article 6(e) and complementing article 24.

179. Paragraph 2 establishes the obligations of trust service providers in case of data breach. It presupposes the occurrence of a breach of security or loss of integrity that has a significant impact on the trust service.

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; A/CN.9/1087, paras. 74-76.

3. Article 15. Obligations of subscribers

180. Article 15 establishes the obligations of subscribers in case of compromise of the trust service. The underlying notion of "compromised trust service" refers to instances of unauthorized access to the trust service and presupposes the occurrence of an event that affects the reliability of the trust service.

181. Article 15 acknowledges that the subscriber is unlikely to have immediate knowledge of issues affecting the trust service as a whole but may be aware of visible information being compromised and might be aware of risks involving information not directly visible, such as a private key. For that reason, paragraphs (a) and (b) have two different objects.

182. 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 operational rules, policies and practices of the trust service provider.

183. The Model Law 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.

184. The Model Law 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.

185. Unlike article 11 MLES, article 15 does not establish obligations of relying parties, which may be held liable under other law.

References

A/CN.9/1005, paras. 37–43; A/CN.9/1045, paras. 22–26; A/CN.9/1087, paras. 77–78.

4. Article 16. Electronic signatures

186. 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.[28] The formulation of article 16 is inspired by that of article 9 MLETR, which, in turn, takes into account that of

[28] See also generally the document *Promoting confidence in electronic commerce*.

article 9(3) ECC, and establishes the requirements for the functional equivalence between handwritten and electronic signatures. Accordingly, the term "identify" in article 16 should be interpreted in line with the settled meaning in similar UNCITRAL provisions and their enactments.

187. 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.

188. 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. [29]

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; A/CN.9/1087, paras. 82–84.

5. Article 17. Electronic seals

189. 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.

190. 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).

191. 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 usually been enacted as applicable to both natural and legal persons.

192. 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.

193. 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.

[29] *MLES, Guide to Enactment*, paras. 29–62; *Promoting confidence in electronic commerce*, paras. 24–66.

Integrity

194. 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; A/CN.9/1087, paras. 85–86.

6. Article 18. Electronic timestamps

195. 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.

196. 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).

197. 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

198. 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).

199. 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).

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

201. 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. Paragraph (c) accommodates file migration and format changes that are part of ordinary data retention practices. Its formulation is based on article 8(3)(a) MLEC.

202. 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

203. 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.

204. 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.

205. 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

206. 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 in order 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.

207. 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.

208. 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.

209. 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

210. 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.

211. Similar to the notion of reliable method used for IdM services (see para. 141 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 subparagraph 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

212. The MLES and several regional and 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 Model Law and trust services may be designated regardless of the level of reliability they offer.

213. 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; A/CN.9/1087, paras. 87 and 105–106.

11. Article 23. Designation of reliable trust services

214. 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.

215. 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.

216. 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 ex post of the reliability of the method.

217. 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

218. 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.

219. Article 24 is drafted in a manner similar to article 12, on the liability of IdM service providers, and therefore the considerations made under article 12 may apply also to article 24. In particular, article 24, like article 12, establishes a statutory basis of liability that operates alongside contractual and extracontractual liability, and the operation of domestic law provisions on contractual and extracontractual liability relevant for trust service providers are not affected by article 24, as indicated in paragraph 2(a).

220. 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.

221. Among 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.[30]

References

A/CN.9/1005, paras. 74–76; A/CN.9/1045, paras. 62–66; A/CN.9/1087, para. 89.

D. Chapter IV – International aspects (articles 25 to 27)

1. Article 25. Cross-border recognition of electronic identification

222. Article 25 establishes a mechanism for cross-border legal recognition of electronic identification that aims to grant the same legal treatment to domestic and foreign IdM systems, IdM services and identity credentials. It is based on the principle of non-discrimination against geographic origin and focuses on electronic identification as the result of the use of IdM systems, IdM services and identity credentials.

223. One goal of article 25 is to reduce the need for service providers to apply for designation under article 23 in multiple jurisdictions. 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.

224. Levels of reliability defined in different jurisdictions may not match exactly. Such mismatch is a likely situation given the absence of universally agreed definitions of specific levels of reliability. To overcome challenges to cross-border recognition arising from that mismatch, article 25 refers to the notion of "at least equivalent level of reliability", which includes levels of reliability that are the same or higher than the one required. That notion should not be interpreted as demanding compliance with strict technical requirements, which may result in obstacles to mutual recognition and, ultimately, to trade.

225. The reference to "IdM system, IdM service or identity credential, as appropriate," aims to capture all possible aspects relevant for cross-border recognition of electronic identification. In practice, it may be preferable to focus on a specific IdM service to avoid recognizing all IdM services supported by an IdM system as equally reliable even though one or more of them may offer a lower level of reliability.

[30] For a discussion of specific instances of liability in a public key infrastructure framework, see *Promoting confidence in electronic commerce*, paras. 211–232.

Moreover, recognition of identity credentials should avoid those credentials that have remained unchanged despite the IdM service used to issue them having been compromised.

226. Recognition of foreign IdM systems, services and identity credentials 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.

227. Paragraph 3 further clarifies how designating authorities may designate foreign IdM and trust services. It expands on the mechanism provided in article 11(4), which provides 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 made by a foreign designating authority and by including IdM systems and credentials as possible objects of designation. Paragraph 3 therefore implements the ex-ante approach.

228. In making its determination of equivalence, the competent authority should take into account the list of circumstances relevant for determining the reliability of the methods used in IdM services contained in article 10(2) to ensure consistency among determinations of reliability.

229. The determination of the reliability of an IdM service, an IdM system or an identity credential is a time-consuming and resource-intensive exercise, and not all jurisdictions may dispose of adequate resources. Those jurisdictions with less resources may particularly benefit from the possibility of recognizing foreign IdM services and systems and identity credentials by relying on foreign determinations and designations. Mechanisms leveraging on paragraph 3 may also replace arrangements based on the conclusion of ad hoc mutual recognition agreements between supervisory bodies.

230. When adopting implementing regulations, the enacting jurisdiction may decide whether paragraph 3 should operate based on automatic recognition (e.g. IdM 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 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).

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; A/CN.9/1087, paras. 90–101.

2. Article 26. Cross-border recognition of the result of the use of trust services

231. Article 26 introduces a mechanism for cross-border recognition of the result of the use of trust services similar to that established in article 25 for electronic identification. Accordingly, the considerations made under article 25 may apply to article 26.

232. Article 26 is generally compatible with the use of existing mechanisms for cross-border recognition of the result of the use of trust services such as cross-recognition and cross-certification between public key infrastructures.[31]

References

A/CN.9/1087, paras. 90–101.

[31] For more information on cross-recognition and cross-certification see *Promoting confidence in electronic commerce*, paras. 163–172.

3. Article 27. Cooperation

233. 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 practices, in particular with respect to technical requirements, including levels of assurance and levels of reliability.

234. Moreover, article 26 may facilitate agreement on common definitions of technical standards, including levels of assurance and levels of reliability, that support a determination of equivalence. In business practice, the notions of level of assurance and of level of reliability are used as terms of art, respectively, for the assessment of IdM and trust services. The Model Law 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.

235. Cooperation should take place on a voluntary basis and in line with the applicable national laws and regulations. The reference to “foreign entities” aims to capture all entities, regardless of their legal nature, that may contribute to achieving the envisaged goals.

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; A/CN.9/1087, paras. 108–109.