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

UNITED NATIONS

Further information may be obtained from:

UNCITRAL secretariat, Vienna International Centre
P.O. Box 500, 1400 Vienna, Austria

Telephone: (+43-1) 26060-4060
Telefax: (+43-1) 26060-5813
Website: https://uncitral.un.org
Email: uncitral@un.org

UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW

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

UNITED NATIONS
Vienna, 2023

NOTE

Symbols of United Nations documents are composed of capital letters combined with figures. Mention of such a symbol indicates a reference to a United Nations document.

UNITED NATIONS PUBLICATION
Sales No.: E.23.V.10
ISBN 978-92-1-300082-3
eISBN 978-92-1-002853-0

The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Links to Internet sites contained in the present publication are provided for the convenience of the reader and are accurate at the time of issue. The United Nations takes no responsibility for their continued accuracy after issue or for the content of any external website.

Publishing production: English, Publishing and Library Section, United Nations Office at Vienna.

Contents

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

Resolution adopted by the General Assembly on 7 December 2022

77/101. Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services

The General Assembly,

Recalling its resolution 2205 (XXI) of 17 December 1966, by which it established the United Nations Commission on International Trade Law with a mandate to further the progressive harmonization and unification of the law of international trade and in that respect to bear in mind the interests of all peoples, in particular those of developing countries, in the extensive development of international trade,

Recalling also its resolution 60/21 of 23 November 2005, by which it adopted the United Nations Convention on the Use of Electronic Communications in International Contracts and called upon all Governments to consider becoming party to the Convention, and its resolutions 51/162 of 16 December 1996, 56/80 of 12 December 2001 and 72/114 of 7 December 2017, in which it recommended that all States give favourable consideration to the Model Law on Electronic Commerce, the Model Law on Electronic Signatures and the Model Law on Electronic Transferable Records of the Commission, respectively,

Mindful that the Convention, the Model Law on Electronic Commerce, the Model Law on Electronic Signatures and the Model Law on Electronic Transferable Records are of significant assistance to States in enabling and facilitating electronic commerce in international trade,

Convinced that confidence, legal certainty and predictability in electronic commerce, including across borders, will be enhanced by the harmonization of certain rules on the legal recognition of identity management and trust services on a technology-neutral basis and, when appropriate, according to the functional equivalence approach,

Recalling that, at its forty-ninth session, in 2016, the Commission mandated its Working Group IV (Electronic Commerce) to undertake work on the use and cross-border recognition of identity management and trust services,[1]

Noting that the Working Group devoted 10 sessions, from 2017 to 2022, to that work, and that the Commission considered at its fifty-fifth session, in 2022, a draft model law on the use and cross-border recognition of identity management and trust services prepared by the Working Group, together with comments on the draft received from Governments and international organizations invited to sessions of the Working Group,[2]

Believing that a model law on the use and cross-border recognition of identity management and trust services will constitute a useful addition to existing Commission texts in the area of electronic commerce by assisting States in enhancing their legislation governing the use of identity management and trust services, or formulating such legislation where none currently exists, in particular with respect to cross-border aspects,

1. *Expresses its appreciation* to the United Nations Commission on International Trade Law for completing and adopting the Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services;[3]

2. *Requests* the Secretary-General to publish the Model Law together with an explanatory note, including electronically, in the six official languages of the United Nations, and to disseminate it broadly to Governments and other interested bodies;

3. *Recommends* that all States give favourable consideration to the Model Law when revising or adopting legislation relevant to identity management and trust services, and invites States that have used the Model Law to advise the Commission accordingly;

4. *Also recommends* that States continue to consider becoming parties to the United Nations Convention on the Use of Electronic Communications in International Contracts[4] and to give favourable consideration to the use of the Model Law on Electronic Commerce,[5] the Model Law on Electronic Signatures[6] and the

[1] *Official Records of the General Assembly, Seventy-first Session, Supplement No. 17* (A/71/17), paras. 235–236.

[2] Ibid., *Seventy-seventh Session, Supplement No. 17* (A/77/17), chap. VI.

[3] Ibid., annex II.

[4] Resolution 60/21, annex; see also United Nations, *Treaty Series*, vol. 2898, No. 50525.

[5] Resolution 51/162, annex.

[6] Resolution 56/80, annex.

Model Law on Electronic Transferable Records[7] when revising or adopting legislation on electronic commerce;

5. *Appeals* to the relevant bodies of the United Nations system and other relevant international and regional organizations to coordinate their legal activities in the area of electronic commerce, including paperless trade facilitation, with those of the Commission, to avoid duplication of efforts and to promote efficiency, consistency and coherence in the modernization and harmonization of legislation on electronic commerce.

47th plenary meeting
7 December 2022

[7] *Official Records of the General Assembly, Seventy-second Session, Supplement No. 17* (A/72/17), annex I.

Decision of the United Nations Commission on International Trade Law

The United Nations Commission on International Trade Law,

Recalling General Assembly resolution 2205 (XXI) of 17 December 1966, which established the United Nations Commission on International Trade Law with the purpose of furthering the progressive harmonization and unification of the law of international trade in the interests of all peoples, in particular those of developing countries,

Mindful that the UNCITRAL Model Law on Electronic Transferable Records,[8] the United Nations Convention on the Use of Electronic Communications in International Contracts (2005),[9] the UNCITRAL Model Law on Electronic Signatures (2001)[10] and the UNCITRAL Model Law on Electronic Commerce (1996)[11] are of significant assistance to States in enabling and facilitating electronic commerce in international trade,

Mindful also of the importance of providing a legal foundation for mutual trust to promote confidence in electronic commerce, particularly across borders, and of the increasing relevance of identity management and trust services to that end,

Convinced that legal certainty and commercial predictability in electronic commerce, including across borders, will be enhanced by the harmonization of certain rules on the legal recognition of identity management and trust services on a technologically neutral basis and, when appropriate, according to the functional equivalence approach,

Believing that a UNCITRAL model law on the use and cross-border recognition of identity management and trust services will constitute a useful addition to existing UNCITRAL texts in the area of electronic commerce by significantly assisting States in enhancing their legislation governing the use of identity management and trust services, or in formulating such legislation where none currently exists, particularly with respect to cross-border aspects,

---

[8] *Official Records of the General Assembly, Seventy-second Session, Supplement No. 17* (A/72/17), annex I.

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

[10] General Assembly resolution 56/80, annex.

[11] General Assembly resolution 51/162, annex.

Recalling that, at its forty-ninth session, in 2016, it mandated Working Group IV (Electronic Commerce) to undertake work on the use and cross-border recognition of identity management and trust services,[12]

Having considered, at its fifty-fifth session, in 2022, a draft model law on the use and cross-border recognition of identity management and trust services and an explanatory note thereto, prepared by the Working Group,[13] together with comments on the draft received from Governments and international organizations,[14]

Expressing its appreciation to Working Group IV for its work in developing the draft UNCITRAL model law on the use and cross-border recognition of identity management and trust services and to intergovernmental and invited non-governmental organizations for their support and participation in that work,

1. *Adopts* the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services, as contained in annex II to the report of the United Nations Commission on International Trade Law on the work of its fifty-fifth session;

2. *Approves* in principle the draft explanatory note to the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services, requests the Secretariat to finalize it by reflecting deliberations and decisions at the fifty-fifth session of the Commission, and authorizes Working Group IV (Electronic Commerce), at its sixty-fourth session, in 2022, to review the parts relating to the deliberations and decisions at the fifty-fifth session of the Commission;

3. *Requests* the Secretary-General to publish the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services together with an explanatory note, including electronically and in the six official languages of the United Nations, and to disseminate it broadly to Governments and other interested bodies;

4. *Recommends* that all States give favourable consideration to the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services when revising or adopting legislation relevant to identity management and trust services, and invites States that have used the Model Law to advise the Commission accordingly.

1170th meeting
7 July 2022

[12] *Official Records of the General Assembly, Seventy-first Session, Supplement No. 17* (A/71/17), paras. 235–236.

[13] A/CN.9/1112, annexes I and II.

[14] A/CN.9/1113 and A/CN.9/1113/Add.1.

UNCITRAL 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", 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 and 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 of 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 privacy and protection.

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, the result of 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 service 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, relying parties and other 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 reliable method in accordance with article 10, paragraph 1, or article 10, paragraph 4, is used for the identity proofing and 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) Deemed to be as reliable as appropriate if proven in fact by or before a court or competent adjudicative body to have fulfilled the function described in article 9, by itself or together with further evidence.

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 assurance 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 transaction 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, relying parties and other 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 have 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 reliable method in accordance with article 22, paragraph 1, or article 22, paragraph 4, 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 reliable method in accordance with article 22, paragraph 1, or article 22, paragraph 4, 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 reliable method in accordance with article 22, paragraph 1, or article 22, paragraph 4, 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 reliable method in accordance with article 22, paragraph 1, or article 22, paragraph 4, 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 reliable method in accordance with article 22, paragraph 1, or article 22, paragraph 4, 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 reliable method in accordance with article 22, paragraph 1, or article 22, paragraph 4, 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) Deemed to be as reliable as appropriate if proven in fact by or before a court or competent adjudicative body to have fulfilled the functions described in the article, by itself or together with further evidence.

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 the 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 transaction 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, paragraph 1 *(e)*, with respect to that transaction.

Chapter IV. Cross-border recognition

Article 25. Cross-border recognition of the result of electronic identification

1. The result of 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:

(a) At least an equivalent level of assurance, where the assurance levels recognized by such jurisdictions are identical; or

(b) Substantially equivalent or higher level of assurance, in all other cases.

2. For the purposes of determining satisfaction of paragraph 1, regard shall be had to recognized international standards.

3. An identity management system, identity management service or identity credential shall be presumed to satisfy paragraph 1 if [*the person, organ or authority*

specified by the enacting jurisdiction pursuant to article 11] has determined the 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:

(a) At least an equivalent level of reliability, where the reliability levels recognized by such jurisdictions are identical; or

(b) Substantially equivalent or higher level of reliability, in all other cases.

2. For the purposes of determining satisfaction of paragraph 1, regard shall be had to recognized international standards.

3. The trust service shall be presumed to satisfy paragraph 1 if [*the person, organ or authority specified by the enacting jurisdiction pursuant to article 23*] has determined the 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.

Guide to enactment of the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services

I. Introduction

A. Purpose of the guide

1. In preparing and adopting its 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 harmonizing and modernizing legislation if accompanied by background and explanatory information.

2. The aim of the present guide, drawn from the *travaux préparatoires* of the Model Law, is to assist those interested in the adoption, use and uniform interpretation of the Model Law, such as policymakers, legislators, academics, practitioners, judges, arbitrators, and commercial operators and users of identity management and trust services. For instance, in the process of enacting legislation based on the Model Law, the information contained in the present guide 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 relating to identity management (IdM) and trust services.

B. Objectives

3. In the past 20 years, there has been exponential growth in the value of online commercial activity (i.e. electronic transactions between businesses, businesses and consumers and businesses and governments). That growth, which has been further accelerated by the need to mitigate the effects of the coronavirus disease

(COVID-19) pandemic,[15] has been accompanied by a similar increase in data transactions and calls for an adequate legal and technical framework.

4. The growth of online commercial activities is built 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, under which target 16.9 calls for the provision of legal identity for all human beings, including in electronic form. In the digital economy, that translates into the right to a digital identity.

5. Over the years, various solutions have been suggested to address the need for online identification, which has led to the development of systems, methods, technologies and devices to create and manage the digital identities of natural and legal persons. Addressing the legal aspects of IdM at the global level has the potential not only to bridge those different solutions, but also to encourage interoperability between IdM systems regardless of whether they are operated by the private sector or governments.

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

7. Obstacles to the broader use of IdM and trust services may vary in nature. For instance, access to IdM and trust services may be limited owing to cost, lack of awareness and technical constraints. Obstacles of a legal nature include: *(a)* a lack of legislation giving legal effect to IdM and trust services; *(b)* divergent legal approaches to IdM, including laws that are based on technology-specific requirements; *(c)* legislation requiring paper-based identification documents for entering into online commercial transactions; and *(d)* the absence of mechanisms for cross-border legal recognition of IdM and trust services (A/CN.9/965, para. 52).

8. The main objective of the Model Law is to address those obstacles through the development of uniform legal rules that serve several purposes. Uniform rules can 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 the legal predictability and certainty

[15] *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow* (UNCTAD/DER/2021), pp. 16–17.

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 by making common solutions more readily available.

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, such a framework will also contribute to sustainable development and social inclusion in accordance with Sustainable Development Goal 9, which deals with fostering innovation, among other activities. Moreover, as noted in paragraph 4 above, IdM is directly relevant to the achievement of target 16.9, on providing legal identity for all, as online identity is a means of proving personal identity.

10. IdM is also instrumental in achieving several other targets under the Sustainable Development Goals. For instance, with respect to access to finance, IdM may be used to satisfy know-your-customer requirements for banking and to maintain efficient credit and land registries, which are activities relevant to implementing target 1.4, on ensuring that all have access to new technology and financial services, among other things. The efficient use of IdM for the fulfilment of know-your-customer requirements may also assist in reducing the costs of remittance transfers and illicit financial flows, which are the aims of targets 10.c and 16.4, respectively.

11. Trust services are relevant to all activities relating to innovation, as new technologies such as artificial intelligence are fuelled by the input of large, reliable data sets. Thus, trust services are relevant to achieving target 9.b, on supporting technology development, research and innovation in developing countries.

C. Scope

12. 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 also decide to expand the scope of application of the Model Law to non-commercial activities.

13. Many different pieces of legislation may be relevant to data exchanges. The Model Law does not affect those existing laws, namely, those applicable to data privacy and protection. Nor does it introduce new obligations to use IdM and trust services, or any specific IdM or trust service, or affect any such existing requirement (see paras. 106–108 below).

14. 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 data messages. Both sets of provisions apply regardless of the private or public nature of the service provider, the subscriber and the relying party.

D. Structure

15. The Model Law consists of four chapters, which deal with general provisions, IdM, trust services and cross-border recognition. Chapters I and IV apply to both IdM and trust services. 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 to the corresponding provision in chapter III to the extent that the provisions coincide. In particular, this may apply to articles 13, 14, 15, 22, 23 and 24 with respect to articles 5, 6 and 7, 8, 10, 11 and 12, respectively.

16. Chapter I contains definitions 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 particular services; provisions on the relationship between the Model Law and other laws, including requirements to identify or to use specified trust services; and provisions on the autonomous interpretation, including for gap-filling purposes, of the Model Law in light of its uniform nature and international origin.

17. Chapter II establishes the basic elements of the legal regime applicable to IdM, lists certain core obligations of IdM service providers and subscribers and sets out rules on the liability of IdM service providers. Article 5 establishes the principles of legal recognition of IdM and non-discrimination against electronic identification. Article 6 lists and thus 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 IdM service providers in the case of a data breach and is complemented by article 8, on the obligations of subscribers in cases where identity credentials are compromised. Article 9 contains a rule for functional equivalence between offline identification and identification carried out using IdM 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. Lastly, article 12 deals with the liability of IdM service providers.

18. 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 out the obligations of trust service providers, and article 15 deals with the obligations of trust service subscribers in cases where 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 and website authentication) and the 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 the ex post determination of reliability of the method used for the trust service and article 23 on its designation ex ante. Lastly, article 24 contains rules on the liability of trust service providers.

19. Chapter IV deals with enabling the 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 the legal recognition of IdM and trust services, but provides for several mechanisms based on a decentralized approach. Besides articles 25 to 27, the dedicated provisions in articles 10 (3), 11 (4), 22 (3) and 23 (4), relating to non-discrimination against geographic origin in determining the reliability of IdM and trust services and in designating reliable IdM and trust services, are relevant. Contractual agreements may also be relevant in enabling the cross-border use of IdM and trust services.

E. Background

1. Drafting history

20. 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, and to share the result of such preparatory work with Working Group IV (Electronic Commerce), with a view to seeking recommendations on the exact scope, possible methodology and priorities for the consideration of the Commission.[16]

21. 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,

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

held in Vienna on 21 and 22 April 2016.[17] The Commission agreed that the topic of IdM and trust services should be retained on the work agenda of the Working Group.[18]

22. Having received a mandate from the Commission, the Working Group held preliminary discussions on the topic at its fifty-fourth session, held in Vienna from 31 October to 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 to 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 persons, 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).

23. In line with its prior decisions, at its fifty-fifth session, held in New York from 24 to 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).

24. At its fiftieth session, in 2017, the Commission reaffirmed the mandate given to the Working Group (see para. 20 above) and requested the secretariat to consider convening expert group meetings. States and international organizations were invited to share their expertise.[19] Accordingly, the secretariat convened an expert group meeting on legal aspects of IdM and trust services in Vienna on 23 and 24 November 2017.

25. Building also on the outcome of the expert group meeting, at its fifty-sixth session, held in New York from 16 to 20 April 2018, the Working Group identified the following issues as relevant to 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).

[17] Ibid., *Seventy-first Session, Supplement No. 17* (A/71/17), paras. 228–229.
[18] Ibid., paras. 235–236.
[19] Ibid., *Seventy-second Session, Supplement No. 17* (A/72/17), para. 127.

26. 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. 25 above).[20]

27. 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, held in Vienna from 19 to 23 November 2018.

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

29. 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 and 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.

30. At its fifty-second session, in 2019, the Commission expressed its satisfaction with the progress made by the Working Group.[21] 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.[22]

31. The Working Group then 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. 29 above), at its fifty-ninth session, held in Vienna from 25 to 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

[20] Ibid., *Seventy-third Session, Supplement No. 17* (A/73/17), para. 159.
[21] Ibid., *Seventy-fourth Session, Supplement No. 17* (A/74/17), para. 175.
[22] Ibid., para. 172.

of the instrument, and a strong preference was expressed for the instrument taking the form of a model law as opposed to a convention (ibid., para. 123).

32. At its fifty-third session, in 2020, the Commission again expressed its satisfaction with the progress made by the Working Group and confirmed that the Working Group should proceed with the preparation of a model law on legal issues related to identity management and trust services.[23]

33. 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, held in Vienna from 19 to 23 October 2020. It also agreed on the possibility of holding informal consultations to discuss outstanding topics.

34. Informal consultations were held remotely with delegates and observers from 15 to 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.

35. The Working Group was informed of the outcome of the informal consultations at its sixty-first session, held in New York from 6 to 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), the Working Group focused its deliberations on the issues discussed during the consultations (A/CN.9/1051, paras. 13–67).

36. At its fifty-fourth session, in 2021, the Commission was informed 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 finalize its work and to submit it for consideration by the Commission at its fifty-fifth session, in 2022.[24]

37. At its sixty-second session, held in Vienna from 22 to 26 November 2021, the Working Group carried out another reading of the draft provisions (A/CN.9/1087, paras. 12–114) on the basis of a revised set of draft provisions (A/CN.9/WG.IV/WP.170), accompanied 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, in the form of a model law, to the Commission for consideration at its fifty-fifth session, in 2022. The secretariat was asked to circulate the revised text to all Governments and relevant international organizations for

[23] Ibid., *Seventy-fifth Session, Supplement No. 17* (A/75/17), part two, paras. 41 and 51 *(d)*.
[24] Ibid., *Seventy-sixth Session, Supplement No. 17* (A/76/17), chap. IX.

comment, and to compile the comments received for the consideration of the Commission (A/CN.9/1087, para. 11). Also at its sixty-second session, the Working Group agreed that certain pending issues should be considered in informal intersessional consultations, and that the secretariat should report back to the Working Group on those consultations at its sixty-third session for further deliberations (A/CN.9/1087, para. 113).

38. At its sixty-third session, held in New York from 4 to 8 April 2022, the Working Group heard a report on those consultations and discussed those pending issues (A/CN.9/1093, paras. 14–44). At that session, the view was expressed that additional important issues were pending. No decision was made on any of the pending issues, and delegations were again invited to submit comments on those issues to the Commission.

39. At its fifty-fifth session, in 2022, the Commission considered the text of the draft model law on the use and cross-border recognition of identity management and trust services and the explanatory note (A/CN.9/1112, annexes I and II), reflecting the discussions and deliberations of the Working Group up to its sixty-second session, as well as a compilation of comments submitted by Governments and relevant international organizations (A/CN.9/1113 and A/CN.9/1113/Add.1).

40. The Commission established a Committee of the Whole and referred to it the consideration of the draft model law (A/77/17, para. 13). At its 1170th meeting, on 7 July 2022, the Commission considered and adopted the report of the Committee of the Whole, adopted by consensus the Model Law and approved in principle its explanatory note (A/77/17, para. 149). It also requested the secretariat to finalize the explanatory note by reflecting the Commission's deliberations and decisions, and authorized the Working Group to review at its sixty-fourth session the parts of the explanatory note relating to the deliberations and decisions of the Commission at its fifty-fifth session (ibid.). The Working Group reviewed those parts of the explanatory note accordingly (A/CN.9/1125, paras. 91–100).

2. Relationship with earlier UNCITRAL texts

41. There is no provision on trust services in earlier UNCITRAL texts. However, those texts do set out rules on functional equivalence that may be relevant to certain trust services. Article 7 of the UNCITRAL Model Law on Electronic Commerce,[25] article 6 of the UNCITRAL Model Law on Electronic Signatures,[26]

[25] *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.

[26] *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001* (United Nations publication, Sales No. E.02.V.8).

article 9 (3) of the United Nations Convention on the Use of Electronic Communications in International Contracts[27] and article 9 of the UNCITRAL Model Law on Electronic Transferable Records[28] set out the requirements with which electronic signatures must comply 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 of the Model Law on Electronic Transferable Records.

42. Similarly, article 19 of the Model Law is based on article 10 (1) of the Model Law on Electronic Commerce, which sets out the requirements for functional equivalence in the retention of information. Other UNCITRAL provisions that have been used as sources of articles of the Model Law are identified in the commentary on each 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.

43. Several matters relevant to the Model Law, such as the 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.[29]

F. Key concepts and principles

44. The present section contains explanations of several key concepts and principles that underpin the Model Law. Further explanations of defined terms used in the Model Law are given in the commentary on article 1 below, and a more expansive list of terms and concepts relevant to IdM and trust services, compiled on the basis of definitions contained in internationally agreed legal and technical texts, is available in document A/CN.9/WG.IV/WP.150. As indicated in that document, those texts may employ different defined terms for the same concept or define the same term differently.

1. Fundamental principles

45. Like earlier UNCITRAL texts, the Model Law is based on the principles of party autonomy, technological neutrality, functional equivalence and

[27] United Nations, *Treaty Series*, vol. 2898, No. 50525.

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

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

non-discrimination against the use of electronic means, subject to adjustments (A/CN.9/902, paras. 52 and 63).

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

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

48. The principle of technological neutrality ensures that the law does not mandate or favour the use of any specific technology or method, thus making laws future-proof. Technological neutrality is necessary in order to achieve interoperability, which effectively enables data flows. The legal underpinning of this principle is the broad definition of "data message", first set out in article 2 *(a)* of the Model Law on Electronic Commerce, which aims to capture all existing and future technologies.

49. The principle of functional equivalence lays out the criteria according to which electronic transactions are deemed to satisfy form requirements applicable to paper-based documents, such as the requirement that a document be in writing, original or signed. This principle presupposes the existence of legal requirements that directly or indirectly prescribe some physical or paper-based activity, such as the use of paper-based credentials to identify a person. It then requires analysis of the purposes and functions of those requirements with a view to determining how those purposes or functions could be fulfilled by electronic means.

50. While the Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services does not explicitly identify those general principles, they do 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 formed the basis for article 9, on identification using IdM, and articles 16 to 21, on named trust services. However, some of the trust services covered in the Model Law may not have paper-based equivalents, and therefore the principle of functional equivalence would not apply to them.

2. Identity management

51. Identification is the process of uniquely distinguishing a person from others within a particular context by reference to information relating to that person (i.e. attributes). That information may be collected or observed. Identification involves verifying that attributes collected or observed 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.

52. Identification is particularly important for building trust in online transactions.[30] At its core, identification involves verifying that collected or observed attributes match an "identity" previously established for the person being identified ("identity proofing" when referring to establishing the unique identity of a person; and "electronic identification", or what in some jurisdictions has been referred to as "authentication", when referring to the subsequent verification of credentials attesting to that identity in a particular transaction).

53. 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), and second, the presentation and verification of those credentials by electronic means in connection with a particular transaction (i.e. electronic identification):

(a) The first stage of IdM involves the collection of attributes that may comprise a person's "foundational identity", that is, basic attributes that are usually recorded by government agencies in civil registration and vital statistics systems, or in foundational identification systems for natural persons and in company and business registries for legal persons. These attributes may be presented in the form of government-issued or government-recognized credentials (e.g. a certificate of registration) verified with the issuing agency. The extent to which the credential might be recognized depends on a consideration of the purpose for which that credential was issued. This process, which may be carried out either using electronic means or 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 one to whom the credentials were issued in the first stage.

54. IdM systems are used to manage the identification processes associated with each of the two stages, as well as to manage the attributes collected, the credentials

[30] World Bank, *World Development Report 2021: Data for Better Lives* (Washington D.C., 2021).

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 those 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 their needs.

55. 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 technological neutrality (see para. 48 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.

56. IdM service providers, subscribers, relying parties and other entities concerned 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 a "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

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

58. The notion of a "trust service" in the Model Law is concerned with the provision of a service and not merely with the service itself. For instance, an electronic signature may be affixed using a service that employs methods for creating and managing electronic signatures. To avoid doubt, each provision of the Model Law specifies whether it is concerned with the methods used for the provision of the electronic signature service or with the electronic signature that results from the application of that service.

4. Assessment of reliability

59. Consistent with earlier UNCITRAL texts, several provisions of the Model Law refer to the use of a reliable method for the provision of IdM and trust services. The Model Law provides for two mechanisms to assess the reliability of the method: articles 10 and 22 provide indicative lists of factors relevant to the determination of reliability, and articles 11 and 23 provide for a mechanism for the designation of reliable methods.

(a) Ex ante designation of reliability

60. One possible approach to assessing the reliability of a method requires such an 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 to the determination of reliability.

61. 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.

62. The ex ante approach provides a higher level of certainty and predictability as to the legal effect of IdM and trust services, including when used across borders, by means of presumptions and reversal of the burden of proof. Typically, methods used to deliver designated services are presumed reliable, thus relieving the party concerned of the need to prove their reliability and shifting that burden to the party that alleges their unreliability. However, the governance of the ex ante mechanism presupposes the existence of an institutional mechanism, that is, an entity competent for administering the designation process.

63. 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 that certify products, processes and services. Certification (including self-certification) is useful for assessing services using outcome-based standards and may therefore be relevant to their designation.

64. 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 a mechanism must include various elements, such as criteria for evaluating services, details of the evaluation process used in

decision-making, and funding sources. Depending on several factors, including institutional arrangements, governance of the 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.

65. The mechanism for designation should adjust rapidly to technological evolution to avoid hindering innovation. Otherwise, it may discriminate against 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

66. Another possible approach to assessing the reliability of a method postpones such assessment to the time 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 such determination, including non-exhaustive lists of relevant circumstances.

67. The ex post approach generally enables IdM transactions without a prior assessment of reliability and limits the need for such an assessment to cases of actual dispute. It also provides parties with a maximum of flexibility in their 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 the associated costs.

68. On the other hand, the ex post approach may not offer a higher level of predictability regarding the validity of the method employed 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

69. The Model Law combines the mechanisms of determination and designation, thus allowing the recognition of any IdM and trust service and providing guidance as to which IdM and trust services offer a higher degree of confidence in their

reliability (the "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, thus ultimately enabling the parties' preferred solution.

70. 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 of the Model Law on Electronic Signatures.

5. Liability issues

71. 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 on the Use and Cross-border Recognition of Identity Management and Trust Services. 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).[31] The latter approach was adopted in the Model Law on Electronic Signatures.[32]

72. Liability with respect to IdM and trust services is mainly allocated by means of contractual agreements or by statute. The latter approach may be preferred to ensure that parties cannot contractually opt out of certain provisions. Moreover, statutory rules may apply in the absence of a contractual agreement, that is, with respect to relying parties.

73. Articles 12 and 24 establish a uniform liability regime for 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 under certain conditions. Such limitations of liability may be permitted by the enacting jurisdiction and should not be contrary to its public order legislation.

[31] *Promoting Confidence in Electronic Commerce*, para. 175.

[32] For details, see *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001*, part two, paras. 77–81.

74. The Model Law deals neither with the degree of fault required to engage liability nor with the type and amount of recoverable damages.[33] The ordinary rules of the enacting jurisdiction will 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. Cross-border recognition

75. 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 such use: technical incompatibility leading to a lack of interoperability, and legal obstacles to cross-border recognition.[34]

76. Legal obstacles may arise from conflicting national approaches, especially when the law mandates or favours 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 also occur under the "two-tier" approach, when those standards are associated with legal presumptions – may lead to a patchwork of requirements that also has the effect of hindering cross-border use.

77. Legally enabling the 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 of technological neutrality and non-discrimination against geographic origin,[35] 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.

78. In line with the approach adopted in earlier UNCITRAL texts, the Model Law goes beyond the mere reference to place of origin as a relevant factor in 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.

---

[33] 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 damages recoverable).

[34] *Promoting Confidence in Electronic Commerce*, paras. 137–152.

[35] Technological neutrality and a non-discriminatory approach to foreign signatures and services were already identified as principles underpinning an emerging consensus on the legal mechanisms for cross-border recognition of electronic signatures in the publication *Promoting Confidence in Electronic Commerce*, para. 149.

It also provides mechanisms for the ex ante 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.

79. 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 the regional and bilateral levels. 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.

80. Chapters on electronic commerce in 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 and 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

Chapter I. General provisions

Article 1. Definitions

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

Attribute

82. "Attribute" means an item of information or data relating to a person. Examples of attributes of a natural person include the 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 the corporate name, principal office address, registration name and jurisdiction of registration. The notion of an attribute is used in the definition of identity.

83. Attributes may contain personal data, the treatment of which 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.

Data message

84. The definition of "data message" can be found in all existing UNCITRAL texts on electronic commerce, where it is used to implement the principle of technological neutrality (see para. 48 above). The term is the main reference point for defining 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

85. 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 concerns about the multiple meanings attributed to the latter term. In technical usage, the term "authentication" refers to presenting evidence of identity.

86. 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 previous UNCITRAL texts, namely, the Model Law on Electronic Signatures, 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".[36]

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

References

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

Identity

88. 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

89. "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

[36] *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001*, part two, para. 117.

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, for example in art. 3 (2) of the eIDAS Regulation.[37]

References

A/CN.9/1005, paras. 109–110; A/CN.9/1045, para. 137.

IdM services

90. The definition of "IdM services" reflects the understanding that IdM comprises two stages (or phases): "identity proofing" and "electronic identification". The term refers to services that relate to either or both stages. Article 6 *(a)*, on the core obligations of the IdM service provider, describes the various phases and steps involved in the provision of IdM services.

References

A/77/17, para. 114; A/CN.9/1005, paras. 84 and 112; A/CN.9/1087, para. 19.

IdM service provider

91. 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 of 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 serves as a reminder 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.

92. The IdM service provider may also be a relying party if it deployed the IdM service for its own purposes (e.g. for the identification of its employees). In that case, the obligations associated with each role would apply.

References

A/77/17, para. 115; A/CN.9/971, para. 97; A/CN.9/1005, para. 111; A/CN.9/1045, para. 88; A/CN.9/1087, para. 22.

[37]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") (*Official Journal of the European Union*, L 257, 28 August 2014).

IdM system

93. 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 International Telecommunication Union (ITU) terminology, namely, recommendation ITU-T X.1252, clause 6.43. Unlike the definition of "IdM services", the definition of "IdM system" necessarily comprises 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

94. 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 concerns about the multiple meanings of "identification".

References

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

Relying party

95. The term "relying party" refers to a physical or a legal person who 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 basis of the trust service used to create the electronic signature. The definition is based on that contained in article 2 *(f)* of the Model Law on Electronic Signatures.

96. The Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services does not set forth obligations for relying parties. However, such obligations may arise from other laws or agreements, including any arrangement between the subscriber and the relying party. One such obligation may pertain to taking reasonable steps to ascertain the reliability of the methods used in delivering the relevant service, for instance by verifying the ex ante designation of the service. Another obligation may relate to compliance with the security procedures and policies and practices of the service provider.

97. The service provider may limit its liability towards the relying party for losses arising from the use of the service if that use has exceeded the limitations on the purpose or value of the transaction for which the service may be used, and if the service provider has complied with its obligations to make such limitations ascertainable by the relying party (arts. 12 (4) and 24 (4)). Thus, the relying party has an interest in verifying any limitations on the purpose or value of the service and in respecting those limitations.

98. The relying party may be contractually bound by the operational rules required by article 6, or may be a third party with respect to the relationship between the subscriber and the service provider defined by those operational rules. Moreover, the service provider can also be a relying party if it deploys the service for its own purposes (e.g. for the identification of its employees). In that case, the obligations associated with each role would apply.

References

A/77/17, paras. 115 and 147; A/CN.9/1087, paras. 55 and 72; A/CN.9/1125, para. 94.

Subscriber

99. 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 a 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. 38–40 and 96; A/CN.9/1045, paras. 18 and 22; A/CN.9/1087, para. 23.

Trust service

100. 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.

101. The reference to "methods for creating and managing" clarifies that the notion of a "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

102. The trust service provider is a natural or a legal person that provides trust services. A certification service provider within the meaning of the Model Law on Electronic Signatures provides an example of a trust service provider with respect to electronic signatures. Unlike in the case of IdM service providers (art. 6), the Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services does not identify the functions to be carried out by trust service providers. The reference to the existence of an arrangement with a subscriber serves as a reminder 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.

103. 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.

Article 2. Scope of application

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

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

106. In line with the general principle underlying UNCITRAL texts on electronic commerce that favours avoiding or minimizing modifications to existing substantive law, paragraph 2 clarifies that the Model Law does not introduce any new obligations to identify.

107. Paragraph 3 preserves those legal requirements that demand the use of a certain procedure for identification or the use of a specified trust service. Examples of such (typically regulatory) requirements include requests for a specific identity document (e.g. a passport) or for an identity document with certain features corresponding to relevant attributes (e.g. an identity card with a photograph and the date of birth of the holder). Identification requirements may also demand that identification be carried out by a certain person with specific functions. When electronic identification is permitted, regulators often require the use of a specified IdM procedure or trust service, such as identity credentials issued by a public authority.

108. 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 laws 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.

Article 3. Voluntary use of identity management and trust services

109. Article 3 indicates that the Model Law does not impose the use of IdM or trust services on persons who have not agreed to using such 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. Consent may be

inferred from circumstances such as the previous experience and expertise of the parties in using IdM and trust services and the type of transaction, and inferred consent may be rebutted.

110. 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 the treatment of personal information under data privacy and protection law.

111. Article 3, which is based on article 8 (2) of the Electronic Communications Convention, 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.

112. 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 technological neutrality, including with respect to the neutrality of models and systems.

113. An obligation to use IdM and trust services, or a specific IdM or trust service, may exist in other laws. Such an obligation may be imposed, for instance, in transactions with public entities or in transactions involving compliance with regulatory obligations.

References

A/77/17, para. 147; A/CN.9/965, paras. 22 and 110; A/CN.9/1005, para. 116; A/CN.9/1045, para. 79; A/CN.9/1087, paras. 27–28.

Article 4. Interpretation

114. Article 4 is based on provisions found in several earlier UNCITRAL treaties and model laws, including those on electronic commerce (art. 3 of the Model Law on Electronic Commerce; art. 4 of the Model Law on Electronic Signatures; art. 5 of the Electronic Communications Convention; art. 3 of the Model Law on Electronic Transferable Records).

115. 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.

116. Paragraph 2 aims to preserve uniformity in the interpretation and application of 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, without prejudice to the application of mandatory rules.

117. Like 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, technological neutrality, functional equivalence and party autonomy generally underpin UNCITRAL legislative texts on electronic commerce and have also been identified as relevant to the Model Law, subject to adjustments (see paras. 45–50 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 from which the parties may not derogate. Moreover, as noted in paragraph 50 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.

Chapter II. Identity management

Article 5. Legal recognition of identity management

118. Article 5 gives legal recognition to IdM by indicating that the electronic form of identity proofing and electronic identification must not, by itself, prevent their legal effect, validity, enforceability or admissibility as evidence. Thus, the article 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.

119. Article 5 prohibits discrimination against the legal recognition of the result of the application of both stages of the IdM process, that is, identity proofing and electronic identification. Its title refers to "legal recognition", rather than to "non-discrimination", to maintain uniformity with the titles of corresponding provisions in existing UNCITRAL texts.

120. Subparagraph *(b)* specifies that the fact that an 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 ex ante and to those that are not designated ex ante and are therefore subject to evaluation ex post. The Model Law therefore takes a neutral position with respect to the approach chosen to assess reliability. However, subparagraph *(b)* does not imply that any given IdM service uses reliable methods and therefore provides a sufficient level of assurance for identification using IdM: 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.

121. The reference to article 2 (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 (3) qualifies not only article 5 but also all other provisions of the Model Law.

References

A/77/17, paras. 117–118; A/CN.9/965, paras. 107–108; A/CN.9/1005, paras. 79–86; A/CN.9/1045, paras. 17 and 82–84; A/CN.9/1093, para. 16; A/CN.9/1125, para. 92.

Article 6. Obligations of identity management service providers

122. 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 those core obligations and that it remains liable towards subscribers and relying parties even when it avails itself of contractors for the provision of the services. In addition, the obligations under article 6, to the extent that they may apply to the particular IdM system and IdM service provider, may not be derogated by contract. Non-performance of those obligations may engage liability according to article 12 and affect the reliability of IdM services, including designated ones.

123. The obligations contained in article 6 are described in a technology-neutral manner, as the implementation of the principle of technological neutrality in the context of IdM calls for minimum IdM system requirements that refer to system properties rather than to specific technologies.

124. 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 functions or from allocating risk among its contractors or other business partners.

125. The principle that the service provider should be bound by its representations and commitments was already enshrined in article 9 (1) *(a)* of the Model Law on Electronic Signatures, 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".

126. IdM systems may vary significantly in terms of purpose and design, and in terms of the services offered. In turn, the design of the IdM system may also depend 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 approach to designing IdM systems is reflected in the words "as appropriate to the purpose and design".

127. 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. That business practice is acknowledged through the obligation to "have in place operational rules, policies and practices". Because of their legal and practical importance, subparagraph *(d)* requires that operational rules, policies and practices be easily accessible to subscribers, relying parties and other third parties. The reference to easy accessibility, which is also included in subparagraph *(e)*, is aimed at facilitating access to information for parties, such as micro or small enterprises, that may be less familiar with technical matters. The reference to relying parties is meant to eliminate any doubt regarding the applicability of subparagraph *(d)* to those parties, which are a subset of third parties.

128. Subparagraph *(e)* sets out the obligations that IdM service providers must fulfil to limit their liability towards relying parties, thus complementing article 12. The aim of that mechanism is to prevent difficulties arising from requiring the identification of all possible relying parties prior to their reliance.

129. Subparagraphs *(d)* and *(e)* identify the respective target classes of users, which is useful for the purpose of raising the level of compliance of IdM service providers with those provisions. Since under the Model Law IdM service providers

are not liable to third parties (i.e. parties that are neither service providers nor subscribers) that are not relying parties, subparagraph *(e)* does not apply to third parties that are not relying parties, while subparagraph *(d)* applies to all third parties.

130. Subparagraph *(f)* complements article 8 by setting out the obligations that the IdM service provider must fulfil with respect to the notification of security breaches by a subscriber.

References

A/77/17, para. 119; A/CN.9/936, para. 69; A/CN.9/1045, paras. 85–95; A/CN.9/1087, paras. 30–33, 55 and 61; A/CN.9/1093, paras. 35–36 and 40.

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

131. Article 7 establishes fundamental obligations for IdM service providers in the case of a data breach that has a significant impact on the IdM system. The obligations under article 7 apply regardless of the 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 have an impact on the attributes managed in the IdM system.

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

133. The notion of "significant impact" is used in regional[38] 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.

134. 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.

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

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

136. 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 they also exhibit significant differences.

137. Certain aspects of the obligations contained in article 7, such as the identification of the parties to be notified of the breach, the timing and content of the notification and the disclosure of the breach and of its technical details, may be specified in other laws (i.e. 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 notifications, 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.

Article 8. Obligations of subscribers

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

139. The obligation of the subscriber in the case of a security breach arises if the identity credentials have been compromised or if 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 the case of a 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 the applicable obligations under article 8 does not necessarily release the IdM service provider from liability.

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

141. The phrase "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.

142. Subparagraph *(b)* aims to address those cases where the subscriber does not have actual knowledge of the compromise but has reason to believe that it may have happened. The paragraph is inspired by article 8 (1) *(b)* (ii) of the Model Law on Electronic Signatures, which contains similar obligations for the signatory, and is aimed 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 subscriber that give rise to a justified doubt as to whether the identity credentials operate appropriately.

References

A/CN.9/936, para. 89; A/CN.9/971, paras. 88–97; A/CN.9/1005, paras. 37–43 and 95–96; A/CN.9/1045, paras. 102–105; A/CN.9/1087, paras. 36–37.

Article 9. Identification of a person using identity management

143. 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.

144. The method used to fulfil the rule in article 9 must be reliable in accordance with article 10, paragraph 1, or article 10, paragraph 4. The reliability of the method may be assessed ex post or evaluated in the context of ex ante designation. The standard of reliability is not absolute but relative to the specific purpose.

145. 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. Therefore, article 9 can operate only with reference to a paper-based equivalent.

146. 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.

147. Article 9 does not affect requirements to identify according to a specific method or procedure, as set out in article 2 (3). Such requirements may relate to regulatory compliance, for example in the case of banking and anti-money-laundering regulations (see para. 107 above).

148. 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 or paper-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 on the basis of article 9 includes verification of the required attributes. The need to verify the relevant attributes is also reflected 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 involved in managing identity credentials rather than with the attributes contained in the identity credentials.

149. 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 of the Electronic Communications Convention, has been drafted to accommodate functional equivalence rules in cases where the law does not require certain actions but permits and attaches legal consequences to them.

References

A/77/17, paras. 124–126; 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, paras. 38–41; A/CN.9/1125, para. 95.

Article 10. Reliability requirements for identity management services

150. 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.

151. 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 identity management 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 by electronic means. That function may be pursued for different purposes, each associated with a different level of reliability.

152. Paragraph 1 *(b)* contains a clause aimed at preventing repudiation of the IdM service and at curbing frivolous litigation. Repudiation occurs when a subject declares not having performed an action. With respect to IdM services, the risk is that, after having achieved identification of a party in fact, that party or some other party could bring a legal challenge with respect to the method not being as reliable as appropriate in the abstract and could, through that challenge, invalidate the identification in fact.

153. For the mechanism contained in paragraph 1 *(b)* to operate, the method must have in fact fulfilled the identification function, that is, it must have associated the person seeking identification with the identity credentials. The Model Law requires the use of reliable methods, and paragraph 1 *(b)* should not be misconstrued to tolerate 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 discrete attributes.

154. Paragraph 1 *(b)* builds on article 9 (3) *(b)* (ii) of the Electronic Communications Convention by adding two elements. The first is that a method proven to achieve identification in fact, by itself or together with further evidence, is deemed to be as reliable as appropriate and thus satisfies the reliable method requirements in article 9. The second is that the determination that the method has fulfilled the identification function must be made by an adjudicative body, which could be a court, an administrative tribunal, an arbitral panel or any other entity in charge of settling disputes. The words "by or before" accommodate all options available under national law with respect to the presentation and evaluation of evidence and determination of facts, which could be carried out by the adjudicative body itself or by the parties.

155. Paragraph 2 contains a list of circumstances, described in technology-neutral terms, that may be relevant to 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.

156. 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 to the determination of reliability. This provision is aimed at facilitating the cross-border recognition of IdM services and is inspired by article 12 (1) of the Model Law on Electronic Signatures, which establishes a general rule of non-discrimination in determining the legal effect of a certificate or electronic signature.[39]

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

158. Paragraph 5 clarifies the relationship between articles 10 and 11 by specifying that the existence of a designation mechanism does not preclude ex post determination of reliability of the method. The provision is inspired by article 6 (4) of the Model Law on Electronic Signatures.

(a) Level of assurance framework

159. Articles 10 and 11 refer to the notion of "level of assurance frameworks" or similar frameworks otherwise named. Level of assurance frameworks describe the requirements that IdM systems and services must meet in order to provide a certain level of assurance in their reliability. The Model Law uses the term "level of assurance" with respect to IdM, and the term "level of reliability" (see para. 226 below) with respect to trust services.

160. More precisely, a "level of assurance" means a designation of the degree of confidence in the identity proofing and electronic identification processes, that is: *(a)* the degree of confidence in the vetting process used to establish the identity of a subject to whom a credential was issued; and *(b)* the degree of confidence that the subject using the credential is the subject to whom the credential was issued. The level of assurance thus reflects the reliability of methods, processes and technologies used.

161. 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

[39] For a discussion of the interaction between articles 12 (1) and 12 (2) of the UNCITRAL Model Law on Electronic Signatures, see A/CN.9/483, paras. 28–36.

identification processes and whether those processes are adequate for specific purposes. The Model Law neither defines levels of assurance nor requires them to be defined or used. Nevertheless, defining levels of assurance could facilitate the international recognition of IdM services.

162. Level of assurance frameworks provide for different levels of assurance that are associated with different requirements, which may be referred to by a number (e.g. from 1 to 4) or by a designation (e.g. "low", "substantial" and "high"). Levels of assurance should be described in generic terms to preserve technological neutrality.

163. Level 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 that makes no reference to levels of assurance in its operational rules, policies and practices could be considered to be 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.

164. 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. A 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

165. Article 10 lists among the possibly relevant circumstances the existence of "supervision or certification provided with regard to the identity management service", if any. Certification and supervision may significantly assist in establishing confidence in IdM service providers and their services, including for the purpose of determining the reliability of the method used, as they are associated with a certain level of objectivity in assessing the reliability of the method used. This was already acknowledged in article 12 *(a)* (vi) of the Model Law on Electronic Transferable Records and in article 10 *(f)* of the Model Law on Electronic Signatures.

166. 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.

167. 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.

168. 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 certification and supervision functions may be separated from the provision of IdM services.

169. 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.

170. In some cases, such as when certain types of distributed ledger technology are used, a solution presupposing the existence of 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 other issues.

References

A/77/17, paras. 127–132; 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.9/1093, para. 34; A/CN.9/WG.IV/WP.153, paras. 74–75; A/CN.9/1125, para. 96.

Article 11. Designation of reliable identity management services

171. Article 11 complements article 10 by offering the possibility of designating IdM services. More precisely, it lists the conditions that an IdM service must satisfy in order to be included in 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 that exhibit different levels of reliability and therefore may or may not be designated.

172. The 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. The reference to the circumstances listed in article 10 ensures some degree of consistency between methods designated as reliable ex ante and methods determined to be reliable ex post. Moreover, designation must "be consistent with recognized international standards and procedures relevant for performing the designation process" in order to promote cross-border legal recognition and interoperability.

173. The dissemination of information on designated IdM services is critical to making potential subscribers aware of the existence of such services. The designating entity has an obligation to publish, for instance on its website, a list of designated IdM services, including details of each IdM service provider. The relevance of lists in ensuring transparency on the designation of IdM services, including in the cross-border context, is also acknowledged 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.

174. Paragraph 2 *(a)* refers to standards and procedures relevant to determining reliability and is aimed at ensuring 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 to designation, such as conformity assessments and audits, that are specific to the ex ante approach.

175. 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 to the designation of a reliable service. Paragraph 4 is based on article 12 (1) of the Model Law on Electronic Signatures, which establishes a general rule of non-discrimination in determining the legal effect of a certificate or electronic signature. In practice, this provision allows foreign IdM service providers to request designation of IdM services by 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.

Article 12. Liability of identity management service providers

176. As noted in paragraph 73 above, article 12 sets out a 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. The

purpose of article 12 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 have a contractual footing. The provision applies regardless of the public or private nature of the IdM service provider.

177. 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 the liability of the IdM service provider for breaches of its mandatory obligations, regardless of whether those obligations also have a contractual basis; and *(c)* it acknowledges the possibility of limiting liability under certain conditions.

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

179. 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, was a compromised credential at the time.

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

181. Article 12 acknowledges the possibility of limiting liability under certain conditions. Limitations of liability may be necessary to contain the cost of insurance, among other considerations, 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 the 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 the service provider complies with its obligations under the Model Law, including those relevant to the limitation of liability.

182. With respect to the subscriber, paragraph 3 makes it possible to limit the liability of the IdM service provider under two conditions: firstly, if 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; and secondly, if 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 providers and subscribers, including those of a contractual or other nature.

183. Likewise, paragraph 4 makes it possible to limit the liability of the IdM service provider towards the relying party under two conditions: firstly, if 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; and secondly, if the IdM service provider has complied with its obligations under article 6 *(e)* relating to making the limitations easily accessible to the relying parties with respect to the specific transaction.

184. Article 12 deals only 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 assert a claim against the IdM service provider.

185. Article 12 applies to IdM service providers regardless of whether they are public or private. An enacting jurisdiction may need to adapt this provision to any special rules governing the 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.

Chapter III. Trust services

Article 13. Legal recognition of trust services

186. 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 this article with the approach taken in article 5, which gives legal recognition to electronic identification as the result of the use of an IdM service.

187. 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.

Article 14. Obligations of trust service providers

188. 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, those core obligations. This approach is akin to the one adopted in articles 6 and 7 on the obligations of IdM service providers. Similar to those set out in article 7 (1), all of the obligations listed in article 14 (2) are to be fulfilled in accordance with any applicable law.

189. The reference to operational rules, policies and practices "as appropriate to the purpose and design of the trust service" acknowledges that the obligations of trust service providers may vary in light of the diversity of trust services in terms of design and function.

190. The obligation to make policies and practices available also to third parties, including relying parties (see para. 127 above), reflects existing practice by 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 (art. 3 (1)).

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

192. Paragraph 2 establishes the obligations of trust service providers in the case of a 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 and 57; A/CN.9/1087, paras. 74–76.

Article 15. Obligations of subscribers

193. Article 15 establishes the obligations of subscribers in the case of a compromise of the trust service. The underlying notion of a "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 service.

194. 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 that is not directly visible, such as a private key. For that reason, paragraphs *(a)* and *(b)* have two different objects.

195. 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.

196. 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 can be found in article 8 (1) *(a)* and *(c)* of the Model Law on Electronic Signatures.

197. The Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services does not contain liability rules for subscribers. Therefore, contractual provisions, which may specify additional obligations for subscribers, and general liability rules will determine the subscriber's liability.

198. Unlike article 11 of the Model Law on Electronic Signatures, article 15 does not establish obligations for relying parties, which may be held liable under other laws or agreements.

References

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

Article 16. Electronic signatures

199. 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.[40] The formulation of article

[40] See also *Promoting Confidence in Electronic Commerce*.

16 is inspired by that of article 9 of the Model Law on Electronic Transferable Records, which itself takes into account the wording of article 9 (3) of the Electronic Communications Convention, 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.

200. The requirement of a paper-based signature is satisfied if a reliable method (see para. 223 below) 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 relation to a data message" applies to both the identification of the person and the indication of the person's intention.

201. Electronic signatures may be used to pursue a variety of purposes, such as the identification of the originator of a message and association of the originator with the message's 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 the costs, the level of security sought, the allocation of risks and other considerations. Earlier UNCITRAL texts contain in-depth discussions of the purposes and methods of electronic signatures.[41]

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.

Article 17. Electronic seals

202. 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 its 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 article 6 (3) *(d)* of the Model Law on Electronic Signatures. Accordingly, the description of the integrity requirement contained in article 17 is based on article 6 (3) *(d)* of the Model Law on Electronic Signatures.

203. Article 17 is inspired by regional legislation, specifically recital 65 of the eIDAS Regulation, according to which, "in addition to authenticating the

[41] *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001*, part two, paras. 29–62; and *Promoting Confidence in Electronic Commerce*, paras. 24–66.

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."

204. 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. In practice, the reliable method used for the identification of the legal person affixing the seal is the same as the one used for identifying a signatory, and UNCITRAL provisions on electronic signatures have usually been enacted as applicable to both natural and legal persons.

205. Moreover, provisions contained in UNCITRAL texts require integrity to achieve functional equivalence to the paper-based notion of an "original". In particular, article 6 (3) *(d)* of the Model Law on Electronic Signatures 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.

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

Integrity

207. 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 in order to achieve functional equivalence with the paper-based notion of an "original" (art. 8 of the Model Law on Electronic Commerce). Articles 17 and 19 are inspired by article 8 (3) of the Model Law on Electronic Commerce with respect to requirements for ensuring integrity.

References

A/CN.9/971, paras. 124–128; A/CN.9/1005, paras. 52–54 and 56–58; A/CN.9/1045, paras. 35–36; A/CN.9/1087, paras. 85–86.

Article 18. Electronic timestamps

208. Electronic timestamps provide evidence of the date and the time at which the stamp was bound to certain 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 the sake of opposability to third parties.

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

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

References

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

Article 19. Electronic archiving

211. Article 19 deals with electronic archiving services, which provide legal certainty of the validity of retained electronic records. The reliable method used for electronic archiving must assure the integrity of the archived electronic records as well as the date and time of archiving. Moreover, the information archived should be accessible according to the requirement for functional equivalence with the paper-based notion of "writing" (art. 6 (1) of the Model Law on Electronic Commerce).

212. Article 19 is inspired by, among others, article 10 of the Model Law on Electronic Commerce, which deals with the retention of data messages. However, article 10 of that Model Law refers to the "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).

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

214. For technical reasons, the transmission and retention of data messages may require additions and modifications to the data message that do not alter its integrity. Such additions and modifications are permitted as long as the content of the data message remains complete and unaltered. Subparagraph *(c)* accommodates file migration and format changes that are part of ordinary data retention practices.

Its formulation is based on article 8 (3) *(a)* of the Model Law on Electronic Commerce.

215. 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 capability is achieved by applying the principle of technological 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 (art. 8 (1) *(b)* of the Model Law on Electronic Commerce).

References

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

Article 20. Electronic registered delivery services

216. 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 the sender and recipient.

217. 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 the security and privacy of electronic exchanges, the recipient should be identified before being granted access to the electronic communication.

218. Article 20 does not refer to notions used in earlier UNCITRAL texts, such as "dispatch" and "receipt" (see art. 10 of the Electronic Communications Convention), because it was drafted with a focus on 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.

Article 21. Website authentication

219. Article 21 deals with website authentication, the essential function of which 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: the identification of the domain name holder for the website and the association of that person with the website. Website authentication does not aim at identifying the website.

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

221. The term "person who holds the domain name" refers to the person who has 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.

222. 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.

Article 22. Reliability requirements for trust services

223. In line with the approach taken with respect to IdM services (art. 10), article 22 requires the use of reliable methods in the provision of trust services. The method used must be reliable in accordance with article 22, paragraph 1, or article 22, paragraph 4. The reliability of the method may be assessed ex post or evaluated in the context of ex ante designation. The standard of reliability is not absolute but relative to the specific purpose. Article 22 contains a non-exhaustive list of circumstances that may be relevant to determining the reliability of the method used according to the ex post approach. The list is based on lists contained in article 10 of the Model Law on Electronic Signatures and in article 12 of the Model Law on Electronic Transferable Records.

224. Similar to the notion of a reliable method used for IdM services (see paras. 150–151 above), the notion of a reliable method used in trust services is relative and varies according to the purpose pursued. The relative nature of reliability is reflected in paragraph 1 *(a)*, namely, in the words "as reliable as appropriate", which, according to well-established UNCITRAL usage, are intended 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". Paragraph 1 *(b)* is aimed at preventing the repudiation of trust services that have proven to have achieved their function in fact, thus curbing frivolous litigation (see paras. 152–154 above). Paragraph 1 *(b)* refers to the functions described in articles 16 to 21 that are actually relevant to the transaction in question.

225. The provisions of the Model Law do not purport to modify previous UNCITRAL texts or to offer an interpretation of their provisions. In that regard, article 22 (1) *(b)* in relation to article 16, on the one hand, and article 9 (3) *(b)* of the Electronic Communications Convention, on the other hand, exhibit different levels of detail. Moreover, the provisions of the Model Law relate to trust services, which provide assurance of data quality, and as such they may also find application in the absence of form requirements.

Levels of reliability

226. The Model Law on Electronic Signatures and several regional and national laws on electronic signatures distinguish between trust services on the basis of the level of reliability that they offer. Specifically, those laws attach greater legal effect to electronic signatures that satisfy certain requirements and are therefore 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 on the Use and Cross-border Recognition of Identity Management and Trust Services, and trust services may be designated at any appropriate level of reliability they offer.

227. Since identity credentials offering a high level of assurance may be used for trust services with different levels of reliability, a direct correlation between the level of assurance of an IdM service and the level of reliability of a trust service is not necessary.

References

A/77/17, paras. 135–137; A/CN.9/965, para. 106; A/CN.9/971, paras. 120–121; A/CN.9/1005, paras. 67–68; A/CN.9/1045, paras. 18–21, 27–29, 52–57 and 61; A/CN.9/1051, paras. 45–46; A/CN.9/1087, paras. 87 and 105–106; A/CN.9/1125, para. 99.

Article 23. Designation of reliable trust services

228. Article 23 complements article 22 by allowing the designation of trust services according to the ex ante approach. More precisely, it lists the conditions

that a trust service must satisfy to be included in a list of designated trust services presumed reliable for the purposes of articles 16 to 21.

229. Article 23 focuses on the designation of trust services, on the understanding that the process for designating those services necessarily involves an assessment of the methods used. Similar to the designation of IdM services, the designation of trust services that are presumed to use 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.

230. Since the only legal effect of designation is the presumption of reliability of the method used, the use of trust services that were previously designated but have lost that designation prevents the party concerned from availing itself of that presumption, but does not have consequences for the ex post determination of the reliability of the method.

231. Article 23 requires the designating authority to publish a list of designated trust services, including details of the trust service providers. The purpose of that obligation is to promote transparency and inform potential subscribers of the trust service. Enacting jurisdictions may wish to consider ways to aggregate those lists so that the information can be found in a 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 and 58–61.

Article 24. Liability of trust service providers

232. 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.

233. 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 also apply 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 to trust service providers are not affected by article 24, as indicated in paragraph 2 *(a)*.

234. 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 ways to establish confidence in the use of the trust service.

235. Among earlier UNCITRAL texts, the of the Model Law on Electronic Signatures contains provisions dealing with the 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 of the Model Law on Electronic Signatures acknowledges the possibility for certification service providers to limit the scope or extent of their liability.[42]

References

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

Chapter IV. Cross-border recognition

Article 25. Cross-border recognition of the result of electronic identification

236. Article 25 establishes a mechanism for cross-border legal recognition of IdM with a view to granting the same legal treatment to domestic and foreign IdM systems, IdM services and identity credentials. The article is based on the principle of non-discrimination against geographic origin and focuses on the result of the use of IdM systems, IdM services and identity credentials. Since the different functions performed in the provision of an IdM service (such as those listed in art. 6) could be performed in different jurisdictions, article 25 may apply to all or only some of the functions carried out by the IdM service provider, depending on the geographic location where each function is performed.

237. One goal of article 25 is to reduce the need for service providers to apply for designation under article 11 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.

[42] For a discussion of specific instances of liability in a public key infrastructure framework, see *Promoting Confidence in Electronic Commerce*, paras. 211–232.

238. Levels of assurance defined in different jurisdictions may or may not match exactly given that agreed definitions of specific levels of assurance may be available in certain regions, but not yet at the global level.

239. Paragraph 1 *(a)* applies when definitions of specific levels of assurance recognized by both jurisdictions are identical. In that case, the method used must offer "at least an equivalent level of assurance" to prevent the use of methods that offer a level of assurance lower than the one required for a particular legal effect in the recognizing jurisdiction.

240. To promote cross-border recognition when definitions of specific levels of assurance recognized by both jurisdictions are otherwise than identical, paragraph 1 (b) refers to the notion of a "substantially equivalent or higher level of assurance", which includes levels of assurance that are substantially the same, but not identical, or higher than the one required in the recognizing jurisdiction. Hence, the notion of "substantial equivalence" should not be interpreted as demanding compliance with strict technical requirements, which may result in obstacles to mutual recognition and, ultimately, to trade. For the same reason, the words "level of assurance" should not be interpreted narrowly to exclude levels of assurance that are achieved through the application of criteria for assurance, recognizing that different legal systems may define levels in different ways. This notion may become less relevant once globally agreed definitions of levels of assurance are available.

241. The reference to the "identity management system, identity management service, or identity credential, as appropriate" aims to capture all possible aspects relevant to the cross-border recognition of IdM. 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 assurance. Moreover, the recognition of identity credentials should avoid those credentials that have remained unchanged even though the IdM service used to issue them has been compromised.

242. The recognition of foreign IdM systems, services and identity credentials may require the service provider to adjust its terms of service. For instance, mandatory law in the recognizing jurisdiction may affect the ability of the service provider to limit liability.

243. Paragraph 3 further clarifies how designating authorities may designate foreign IdM and trust services. It expands on the mechanism set out in article 11 (4), which provides for non-discrimination against geographic origin 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.

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

245. 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 have adequate resources at their disposal. 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 based on paragraph 3 may also replace arrangements based on the conclusion of ad hoc mutual recognition agreements between supervisory bodies.

246. When adopting implementing regulations, the enacting jurisdiction may decide whether paragraph 3 should operate on the basis of 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/77/17, paras. 138–144; 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; A/CN.9/1093, para. 17; A/CN.9/1125, paras. 92 and 100.

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

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

248. 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.[43]

[43] For more information on cross-recognition and cross-certification, see *Promoting Confidence in Electronic Commerce*, paras. 163–172.

References

A/CN.9/1087, paras. 90–101.

Article 27. Cooperation

249. Institutional cooperation mechanisms may significantly contribute to achieving the mutual legal recognition and technical interoperability of IdM systems and trust services. Such mechanisms exist in different forms and may be private or public in 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.

250. Moreover, article 27 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 or 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 out those definitions exist across jurisdictions, in particular with respect to the role of central authorities vis-à-vis that of contractual agreements.

251. 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.

ISBN 978-92-1-300082-3

2300891