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

(UNOFFICIAL ADVANCE COPY)

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 has been compromised; or

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

Article 16. Electronic signatures

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