United Nations A/CN.9/WG.IV/WP.157

General Assembly

Distr.: Limited
28 January 2019

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Fifty-eighth session
New York, 8–12 April 2019

Draft Provisions on the Cross-border Recognition of IdM and Trust Services

Note by the Secretariat

Contents

V.19-00493 (E)

Please recycle

I. Introduction

1. At the 57th session of the Working Group, it was requested that future documents prepared by the Secretariat should contain draft provisions on core issues in order to facilitate the progress of the Working Group's work on legal issues related to IdM and trust services.

2. In line with this request, Annex I to this note contains draft provisions on a range of issues that the Working Group has discussed so far. Where possible, these provisions build on the discussions by the Working Group at its 57th session (A/CN.9/WG.IV/WP.153). Additional commentary on these and other relevant issues is contained in working paper A/CN.9/WG.IV/WP.158.

Annex I

Draft Provisions on the Cross-border Recognition of IdM and Trust Services

Chapter I. Sphere of application

Article 1. Scope of application

[**Option A for paragraph (1)**

1. This [draft instrument] applies to the use of IdM systems and trust services in relation to commercial transactions between parties whose places of business are in different States [when the rules of private international law lead to the application of the law of an enacting jurisdiction].

[**Option B for paragraph (1)**

1. This [draft instrument] applies to the cross-border recognition of [IdM systems] [identity credentials] and trust services that are used in the context of commercial activities.[1]

2. This [draft instrument] also applies to the use of IdM systems and trust services in the context of trade-related government services.[2]

3. This [draft instrument] applies to the verification of identity of physical and legal persons as well as of physical and digital objects.

Article 2. Matters not affected by this [draft instrument]

1. Nothing in this [draft instrument] requires a person to verify the identity of a subject or to use a trust service, or to verify the identity of a subject or to use a trust service offering a particular level of reliability.

2. Other than as provided for in this [draft instrument], nothing in this [draft instrument] affects the application to [IdM and trust services] of any rule of law applicable to [IdM and trust services] [including any rule of law applicable to privacy and data protection][3].

Article 3. Voluntary use of IdM and trust services

1. Nothing in this [draft instrument] requires a subject [to use an IdM system] [to accept identity credentials] or to use a trust service without the subject's consent.

2. For the purposes of paragraph 1, the consent of a subject may be inferred from the subject's conduct [and other circumstances][4].

---

[1] Different views have been expressed within the Working Group as to the "object" of legal recognition for its work on IdM. At its 57th session, the Working Group considered IdM systems, identity credentials, and identity transactions as possible objects of legal recognition.

[2] This draft provision aims at highlighting that IdM and trust services can be used outside a purely commercial setting.

[3] The words "including any rule of law applicable to privacy and data protection" aim at addressing the concerns of the working group on the application of privacy and data protection laws.

[4] The words "and other circumstances" refer to instances where the subject is not capable of autonomous conduct, i.e., a physical or digital object. In those cases, the consent will not be attributable to the subject, but to the physical or legal person legally responsible for that subject (A/CN.9/965, para. 109).

Chapter II. General provisions

Article 4. Definitions

For the purposes of this [draft instrument]:

(a) "Attribute" means an item of information or data associated with a subject;[5]

(b) "Identification" means the process of collecting, verifying, and validating sufficient identity attributes about a subject to define and confirm its identity within a specific context;[6]

(c) "Identity" means a set of the attributes about a subject that [allows the subject to be sufficiently distinguished] [[uniquely] describes the subject] within a given context;[7]

(d) "Identity credentials" means [a set of data that is presented as evidence of a claimed identity] [the data, or the physical object upon which the data may reside, that a subject may present to verify or authenticate its identity in an online context][8;9]

(e) "[e-]IdM" or "[electronic] identity management" means a set of processes to manage the identification, authentication [and authorization] of subjects in an online context;[10]

(f) "IdM system operator" means a person that operates an IdM system;

(g) "Level of assurance" means a designation of the degree of confidence in the identification and authentication processes – i.e., (a) the degree of confidence in the vetting process used to establish the identity of 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 assurance reflects the reliability of methods, processes and technologies used;[11]

(h) "Relying party" means a person that may act on the basis of IdM or trust services;

---

[5] See A/CN.9/WG.IV/WP.150, paragraph 13.

[6] See A/CN.9/WG.IV/WP.150, paragraph 29. The Working Group may wish to consider whether this definition should be stated to include enrolment in an IdM system and the issuance of identity credentials.

[7] See A/CN.9/WG.IV/WP.150, paragraph 38. In discussing the definition of "identity", the Working Group may wish to consider whether the requirement of uniqueness is needed for the purposes of the Working Group's work on the topic on the basis that (a) uniqueness is a quality of foundational identity, and (b) foundational identity is currently excluded from the scope of work (A/CN.9/965, para. 10).

[8] This definition is adapted from the definition in § 59.1-550 of the Electronic Identity Management Act of Virginia (Title 59.1 Chapter 50 of the Virginia Code).

[9] See A/CN.9/WG.IV/WP.150, paragraph 21. The term "identity credentials" is broadly synonymous with "electronic identification means" as defined in article 3(2) of 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) to mean "a material and/or immaterial unit containing person identification data and which is used for authentication for an online service".

[10] See A/CN.9/WG.IV/WP.150, paragraph 35. At the 57th session of the Working Group, it was said that this definition might indicate that the cumulative reference to "identification", "authentication" and "authorization" is necessary, whereas any of these elements would be sufficient. For that reason, it was stated that the definition of "electronic identification" in the eIDAS Regulation is preferable (A/CN.9/965, para. 91). The term "electronic identification" is defined in article 3(1) of the eIDAS Regulation to mean "the process of using person identification data [i.e., "identity credentials as defined in this document] in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person".

[11] See A/CN.9/WG.IV/WP.150, paragraph 42.

(i) "Subject" means the person or object that is identified in a particular identity credential and that can be authenticated and vouched for by an identity provider;[12]

(j) "Trust service"[13] means an electronic service that provides a certain level of reliability in the qualities of data;

(k) "Trust service provider" means a person that provides one or more trust services.

Article 5. Interpretation

1. The interpretation of the present [draft instrument] shall be guided by the following general principles:

(a) Non-discrimination against the use of electronic means;

(b) Technology neutrality;

(c) Functional equivalence;

(d) […]

2. In the interpretation of this [draft instrument], regard is to be had to its international character and to the need to promote uniformity in its application and the observance of good faith.

3. Questions concerning matters governed by this [draft instrument] which are not expressly settled in it are to be settled in conformity with the general principles on which it is based [or, in the absence of such principles, in conformity with the law applicable by virtue of the rules of private international law].[14]

Article 6. Non-discrimination against the use of electronic means

1. The use of [identity credentials] [an IdM system] shall not be denied legal effect, validity, enforceability or admissibility as evidence on the sole ground that [those identity credentials are] [the results of the verification of identity are] [that IdM system is] in electronic form.[15]

2. A trust service shall not be denied legal effect, validity, enforceability or admissibility as evidence on the sole ground that the trust service is in electronic form.

Article 7. Technology neutrality

Nothing in this [draft instrument] shall be applied so as to exclude, restrict or deprive of legal effect any [technology, method or system] used for IdM or the provision of trust services that satisfies the requirements referred to in this [draft instrument] [, or otherwise meets the requirements of applicable law].[16]

---

[12] See A/CN.9/WG.IV/WP.150, paragraph 38.

[13] The Working Group may wish to consider whether reference in the English language should be made to "trusted service" to avoid any ambiguity with respect to the well-settled legal notion of "trust" (A/CN.9/965, paras. 14 and 101).

[14] The addition of the words "or, in the absence of such principles, in conformity with the law applicable by virtue of the rules of private international law" may be particularly useful in a cross-border context.

[15] The choice between "identity credentials" and "IdM system" is linked to whether the object of legal recognition is identity credentials or IdM systems (see footnote 1 above and A/CN.9/WG.IV/WP.158, section on legal recognition). Alternatively, if the object of legal recognition is the outcome of the identification process (i.e., the "identity transaction"), the provision could refer to this process instead.

[16] The words "or otherwise meets the requirements of applicable law", which may be found in article 3 of the UNCITRAL Model Law on Electronic Signatures, United Nations publication, Sales No. E.02.V.8 (MLES), refer to the possibility that law other than the draft instrument could prescribe, in certain identified cases, the use of requirements different from those set forth in the draft instrument.

Chapter III. Identity management

Article 8. Legal recognition of IdM

[**Option A for article 8**

Where the law or a party requires[17] the identification of a subject in accordance with a certain method, that requirement is met with respect to IdM if a reliable method is used to verify the relevant attributes of the subject in accordance with the same level as assured by that method.][18]

[**Option B for article 8**

Where the parties wish or are required by law to perform the identification of a subject, the use of an IdM system for this purpose has the equivalent legal effect as the application of non-electronic procedures recognized for this purpose if the IdM system uses a reliable method to verify the attributes of the subject relevant for this purpose.][19]

Article 9. Reliability standards for recognition of IdM

In determining the reliability of the IdM system for the purposes of the requirement referred to in article 8, all relevant circumstances shall be taken into account, including:

(a) Any agreement between the parties;

(b) Any supervision or certification provided with regard to the IdM system;

(c) The level of assurance associated with the IdM system;[20]

(d) […]

Article 10. [Presumption] of reliability of IdM

1. An IdM system [satisfies] [is presumed to be reliable for the purposes of satisfying] the requirement referred to in article 8 if the following conditions are met:

(a) [Description of the minimum set of appropriate rules on how IdM systems should work, including on audit, insurance, certification, liability, termination, and other issues relevant for determining the level of assurance];

(b) [Description of mechanisms to ensure and verify that participants follow the rules]; and

(c) [Description of mechanisms to ensure publicity of the compliance of the IdM system with the minimum set of appropriate rules].[21]

[2. Paragraph 1 does not limit the ability of any person:

(a) To establish in any other way, for the purpose of satisfying the requirement referred to in article 8, the reliability of the IdM system; or

(b) To adduce evidence of the non-reliability of the IdM system.][22]

---

[17] The Working Group may wish to consider whether functional equivalence provisions should extend to instances where the law "permits" the thing, and to confirm that references to "require" implies a reference to legal consequences for the absence of the thing.

[18] See A/CN.9/965, paragraph 77. The Working Group may wish to clarify whether reference to "certain method" is intended to establish a link with paper-based identification means.

[19] See A/CN.9/965, paragraph 78.

[20] This provision is designed to accommodate an ex post approach to recognition.

[21] This provision is compatible with both an ex ante and ex post approach to recognition.

[22] This draft provision is based on article 6(3) MLES. It applies if paragraph 1 establishes a presumption of reliability.

Article 11. Determination of reliability of IdM systems

1. [A person, organ or authority, whether public or private, specified by the enacting State] may determine which IdM systems satisfy the requirement referred to in article 8.[23]

2. Any determination made under paragraph 1 shall be consistent with recognized international standards.

Article 12. Obligations of IdM system operators

1. An IdM system operator shall:

(a) Attribute the relevant identity credentials to the appropriate person;[24]

(b) Ensure the online availability and correct operation of IdM processes.

2. An IdM system operator shall, without delay [and, in any event, within […] days after having become aware of it], notify [the oversight authority] [its affected customers[25] and relying parties] of any breach of security or loss of integrity that has a [significant] impact on the identity credentials or authentication processes provided or on the personal data maintained therein.

3. In case of significant breach of security or loss of integrity, the IdM system operator shall suspend the provision of the affected services [until […]].

4. A user[26] of an IdM system shall notify the IdM system operator if:

(a) The identity credentials or authentication processes have been compromised; or

(b) The circumstances known to the user give rise to a substantial risk that the identity credentials or authentication processes may have been compromised.[27]

Article 13. Liability of IdM system operators

1. Without prejudice to liability that may arise under law, the IdM system operator shall [be liable] [bear the legal consequences] for damages caused [intentionally or negligently] to any person due to a failure to comply with its obligations under this [draft instrument].

2. The IdM system operator shall not be liable for damages arising from the use of services that exceeds the limitations [on the purpose or value of the transactions for which the IdM system may be used] if the IdM system operator has provided reasonably accessible means that enable a [user[28] or] third party to ascertain those limitations.[29]

3. An IdM system operator shall [be presumed not to be liable] [not be liable] if [the issuance of the identity credential or assignment of an identity attribute] is in compliance with:

(a) [Applicable identity management standards;]

---

[23] This provision, which is based on article 7 MLES, is designed to accommodate an ex ante approach to recognition.

[24] The Working Group may wish to consider whether this obligation should be extended to the attribution of attributes.

[25] The Working Group may wish to consider defining the notions of “user” and “customer”.

[26] The Working Group may wish to consider defining the notions of “user” and “customer”.

[27] The draft provision has optional language to provide for a time limit in which the notification must be made, to identify the parties to be notified and to establish the level of impact on services, identity credentials or personal data that triggers the duty to notify. It is also possible to establish a duty to suspend the IdM system until the breach or loss are contained, or, alternatively, a new certification or similar process is achieved.

[28] The Working Group may wish to consider defining the notions of “user” and “customer”.

[29] The draft provision aims at upholding contractual agreements on limitation of liability.

(b) [Applicable terms of any contractual agreement; and]

(c) [Any written rules and policies of the identity trust framework of which it is a member].

[4. Paragraph 3 does not apply if the IdM system operator committed an act or omission that constitutes [gross negligence or wilful misconduct].]

Chapter IV. Trust services

Article 14. Legal recognition of trust services

Electronic signatures[30]

[**Option A for paragraph (1)**

1. Where the law requires[31] a signature of a person, that requirement is met if a reliable method is used to identify the person and to indicate the person's intention in respect of the information contained in the [electronic communication].[32]]

[**Option B for paragraph (1)**

1. Where the law requires a signature of a person, that requirement is met if:

(a) A method is used to identify the person and to indicate the person's intention in respect of the information contained in the [electronic communication]; and

(b) The method used is either:

(i) As reliable as appropriate for the purpose for which the [electronic communication] was generated or communicated, in the light of all the circumstances, including any relevant agreement; or

(ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.[33]]

Electronic timestamps

2. Where the law requires [certain documents, records or information] to be associated with a time and date, that requirement is met [in relation to an electronic communication] if a reliable method is used to associate the time and date with [the electronic communication].[34]

[30] The Working Group may wish to consider whether electronic seals should be treated as a discrete trust service or may be considered a subset of electronic signatures.

[31] The Working Group may wish to consider whether functional equivalence provisions should extend to instances where the law "permits" the thing, and to confirm that references to "require" implies a reference to legal consequences for the absence of the thing.

[32] This draft provision, based on article 9 of the UNCITRAL Model Law on Electronic Transferable Records, United Nations publication, Sales No. E.17.V.5. (MLETR), may be adapted to identify the functions pursued with the use of each trust service. The draft provision does not offer guidance on reliability standards, which may be given in a separate provision applicable to all trust services (see, e.g., art. 12 MLETR).

[33] This option, based on article 9(3) of the United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005), offers generic guidance on reliability standards. Subparagraph (b)(ii) includes a safety clause aimed at avoiding repudiation if the electronic signature has in fact achieved its function.

[34] The Working Group may wish to consider whether reference should be made to electronic communication, data messages or other notion.

Electronic archiving

3. Where the law requires that [certain documents, records or information] be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

(a) The information contained therein is accessible so as to be usable for subsequent reference;

(b) The data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) Such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.[35]

Electronic registered delivery services

4. Where the law requires proof of dispatch and receipt of [a certain document, record or information], that requirement is met [in relation to an electronic communication] if a reliable method is used to transmit [the electronic communication].[36]

Website authentication

5. Where the law requires identification of a website owner, that requirement is met if a reliable method is used to identify the person that owns the website and to link that person to the website.

Electronic escrow

6. Where the law requires the use of escrow services, that requirement is met if a reliable method is used to [place under custody the assets in escrow and to release them to the entitled party].

Article 15. Presumption of reliability of trust services[37]

1. A method is presumed to be reliable for the purpose of satisfying the requirement referred to in article 14 if:

(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) 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, any alteration made to that information after the time of signing is detectable.[38]

---

[35] This condition does not extend to information the sole purpose of which is to enable the message to be sent or receive: see paragraph 2, of article 10, of the UNCITRAL Model Law on Electronic Commerce, United Nations publication, Sales No. E.99.V.4.

[36] The Working Group may wish to consider whether reference should be made to electronic communication, data messages or other notion.

[37] In its current form, this draft provision applies to electronic signatures, but it could be adapted to apply to other trust services.

[38] This draft provision may be used whenever a trust service is required to offer assurance as to integrity.

2. Paragraph 1 does not limit the ability of any person:

(a) To establish in any other way, for the purpose of satisfying the requirement referred to in article 14, the reliability of an electronic signature; or

(b) To adduce evidence of the non-reliability of an electronic signature.[39]

Article 16. Determination of reliability of trust services[40]

1. [A person, organ or authority, whether public or private, specified by the enacting State] may determine which electronic signatures satisfy the provisions of article 14.

2. Any determination made under paragraph 1 shall be consistent with recognized international standards.

Article 17. Obligations of trust service providers

1. A trust service provider shall ensure the availability and correct operation of the trust services that it provides.

2. A trust service provider shall, without delay [and, in any event, within […] days after having become aware of it], notify [the oversight authority] [its affected customers[41] and relying parties] of any breach of security or loss of integrity that has a [significant] impact on the trust services provided or on the personal data maintained therein.

3. In case of significant breach of security or loss of integrity, the trust service provider shall suspend the provision of the affected services [until […]].

4. A user[42] of a trust service shall notify the trust service provider if:

(a) The trust service creation data have been compromised; or

(b) The circumstances known to the user give rise to a substantial risk that the trust service creation data may have been compromised.[43]

Article 18. Liability of trust service providers

1. Without prejudice to liability that may arise under law, the trust service provider shall [be liable] [bear the legal consequences] for damages caused [intentionally or negligently] to any person due to a failure to comply with its obligations under this [draft instrument].

2. The trust service provider shall not be liable for damages arising from the use of services that exceeds the limitations [on the purpose or value for which the trust service may be used] if the trust service provider has provided reasonably accessible means that enable a [user[44] or] third party to ascertain those limitations.[45]

---

[39] This draft provision is based on article 6(3) MLES. It contains a presumption of reliability for those signatures that meet certain standards. These standards contain a reference to integrity, if the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates.

[40] This draft provision enables the possibility to carry out an ex ante assessment of reliability of electronic signatures. In its current form, the draft provision applies to electronic signatures, but it could be adapted to apply to other trust services.

[41] The Working Group may wish to consider defining the notions of “user” and “customer”.

[42] The Working Group may wish to consider defining the notions of “user” and “customer”.

[43] The draft provision has optional language to provide for a time limit in which the notification must be made, to identify the parties to be notified and to establish the level of impact on services or personal data that triggers the duty to notify. It is also possible to establish a duty to suspend the trust services until the breach or loss are contained, or, alternatively, a new certification or similar process is achieved.

[44] The Working Group may wish to consider defining the notions of “user” and “customer”.

[45] The draft provision aims at upholding contractual agreements on limitation of liability.

Chapter V. International aspects

Article 19. Legal recognition of foreign IdM and trust services

1. In determining whether, or to what extent, [an IdM system is] [identity credentials are] or a trust service is legally effective, no regard shall be had:

(a) To the geographic location where [the credentials are issued or used] [the IdM system is operated] or the trust service is provided;

(b) To the geographic location of the place of business of the [issuer] [IdM system operator], trust service provider or the subject.

2. [An IdM system operated] [Identity credentials issued] or trust service provided outside [the enacting jurisdiction] shall have the same legal effect in [the enacting jurisdiction] as [an IdM system operated] [identity credentials issued] or trust service provided in [the enacting jurisdiction] if they offer [a substantially equivalent] [the same] level of reliability.

3. In determining whether [identity credentials] [an IdM system] or a trust service offers [a substantially equivalent] [the same] level of reliability, regard shall be had to [recognized international standards].[46]

Article 20. Cooperation

[A person, organ or authority, whether public or private, specified by the enacting State] [shall] [may] cooperate with foreign entities by exchanging information, experience and good practice relating to IdM and trust services, in particular with respect to:

(a) Certification of IdM systems and trust services;

(b) Definition of levels of assurance of IdM systems and of levels of reliability of trust services; and

(c) Examination of relevant developments.

[46] The Working Group may wish to confirm that, if the above provision is enacted, the effect would be to apply all provisions of the law of the enacting jurisdiction to the IdM system or identity credentials, including, for instance, rules on limitation of liability under statute or contract.