United Nations A/CN.9/WG.IV/WP.160

General Assembly

Distr.: Limited
16 September 2019

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Fifty-ninth session
Vienna, 25–29 November 2019

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

Note by the Secretariat

Contents

V.19-09430 (E)

I. Introduction

1. The revised draft provisions on identity management (IdM) and trust services set out in the annex to this document incorporate the deliberations of the Working Group at its fifty-eighth session (New York, 8–12 April 2019), as well as the outcome of the Secretariat's consultations with experts, as requested by the Working Group (A/CN.9/971, para. 67). To this end, the Secretariat convened an expert group meeting (Vienna, 22–23 July 2019) to discuss standards and procedures that qualify an IdM system for legal recognition, as well as other matters covered in the draft provisions, notably the reliability of IdM systems, and the obligations and liability of IdM service providers.

2. Background information on the current work of Working Group IV is available in document A/CN.9/WG.IV/WP.159, paras. 6–17.

Annex I

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

Chapter I. General provisions

Article 1. Definitions

For the purposes of this [instrument]:

(a) "Attribute" means an item of information or data associated with a subject;[1]

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

(c) "Identification" means the process of collecting, verifying, and validating sufficient attributes to define and confirm the identity of a subject within a specific context;[2]

(d) "Identity" means a set of attributes that [allows the subject to be sufficiently distinguished] [[uniquely] describes the subject] within a given context;[3]

(e) "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];[4,5]

(f) "Identity management (IdM) services" means services consisting of managing the identification of subjects in an online context;

(g) "Identity management (IdM) service provider" means a person [that provides IdM services][that provides services in relation to IdM systems][responsible for an IdM system];[6,7]

---

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

[2] See A/CN.9/WG.IV/WP.150, paragraph 29. The Working Group may wish to consider whether this definition accurately reflects the use of the term "identification" in these draft provisions (bearing in mind draft article 9 in particular), or whether the definition should be revised to include other IdM processes such as enrolment and the issuance of identity credentials.

[3] 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 taking into account 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).

[4] 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).

[5] 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".

[6] The Working Group has agreed to use the term "IdM service provider" in preference to "IdM system operator" (A/CN.9/971, para. 97).

[7] The Working Group may wish to consider whether this definition should be retained in its current form in light of the definitions of "identity provider" in paragraph 37 of document A/CN.9/WG.IV/WP.150, namely: (a) an entity responsible for the identification of persons, legal entities, devices, and/or digital objects, the issuance of corresponding identity credentials, and the maintenance and management of such identity information for subjects; and (b) an entity that creates, maintains and manages trusted identity information of other entities (e.g., users/subscribers, organizations and devices) and offers identity-based services based on trust, business and other types of relationship.

(h) “Identity management (IdM) system” means a set of processes to manage the identification of subjects in an online context;[8]

(i) “Relying party” means a person that may act on the basis of IdM services or trust services;

(j) “Subject” means the person or object that is identified within a specific context;[9]

(k) “Trust service”[10] means an electronic service that provides a certain level of reliability in the qualities of data;

(l) “Trust service provider” means a person that provides one or more trust services.

Article 2. Scope of application

This [instrument] applies to the use and cross-border recognition of IdM systems and trust services in the context of commercial activities [11] and trade-related [government][12] services.[13]

Article 3. Voluntary use of IdM and trust services[14]

1. Nothing in this [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.[15]

[8] See A/CN.9/WG.IV/WP.150, paragraph 35. At the fifty-seventh 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”.

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

[10] 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).

[11] As agreed by the Working Group at its fifty-eighth session, this provision has been redrafted to combine elements of both options that were presented in article 1, paragraph 1 in document A/CN.9/WG.IV/WP.157 (A/CN.9/971, para. 23). At its fifty-second session, the Commission noted that, at this early stage of the project, the Working Group should work towards an instrument that could apply to both domestic and cross border use of IdM and trust services (A/74/17, para. 172). This position is reflected in the reference in this provision to both the “use” and “recognition” of IdM systems and trust services.

[12] The Working Group may wish to consider whether reference to “government” is necessary, or whether a generic reference to “trade-related services” would suffice to capture those transactions that are relevant for trade but not commercial in nature, such as interaction with an electronic single window for customs operations.

[13] The Working Group has agreed that the instrument should convey the possibility of using the work product for needs outside purely commercial settings (A/CN.9/971, para. 23). At its fifty-second session, the Commission noted that the outcome of the work had implications for matters beyond commercial transactions (A/74/17, para. 172).

[14] The content of draft article 2 of document A/CN.9/WG.IV/WP.157, dealing with “matters not affected by this [draft instrument]”, is now incorporated in draft articles 5 and 13. Similarly, the Working Group may wish to consider whether content of current draft article 3 should be incorporated in draft articles 5 and 13.

[15] If the subject is a physical or digital object that is not capable of autonomous conduct, the consent will be attributable to the physical or legal person legally responsible for that subject (A/CN.9/965, para. 109).

Article 4. Interpretation[16]

1. In the interpretation of this [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 [in international trade].

2. Questions concerning matters governed by this [instrument] which are not expressly settled in it are to be settled in conformity with the general principles on which it is based, in particular non-discrimination against the use of electronic means, technology neutrality and functional equivalence [and …][17] [or, in the absence of such principles, in conformity with the law applicable by virtue of the rules of private international law].[18]

Chapter II. Identity management

Article 5. Legal recognition of IdM[19]

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:

(a) [The results of the verification[20] of identity are] [the IdM system is] in electronic form; or

(b) The IdM system is not a designated IdM system pursuant to article 11.

2. Nothing in this [instrument] requires a person to identify a subject or to use a particular IdM service.

3. Other than as provided for in this [instrument], nothing in this [instrument] affects the application to IdM services of any applicable rule of law [including any rule of law applicable to privacy and data protection].[21]

4. Nothing in this [instrument] affects a legal requirement that a subject be identified in accordance with a procedure defined or prescribed by law.[22]

---

[16] A provision on the interpretation of the instrument (draft article 5 of document A/CN.9/WG.IV/WP.157) was not considered by the Working Group at its fifty-eighth session. The provision is based on similar provisions in other UNCITRAL texts. The Working Group may wish to consider whether reference should be made to good faith and, if so, whether to specify "good faith in international trade".

[17] The Working Group may wish to consider whether additional general principles should be listed, namely the principle of transparency (see A/CN.9/936, para. 88).

[18] 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.

[19] Paragraph 1 of draft article 5 mirrors draft article 13, which in turn reflects the deliberations of the Working Group at its fifty-eighth session. This provision establishes the legal effect of identification by use of electronic means regardless of whether an offline identification procedure exists. Paragraphs 2 to 4 are modelled on draft article 2 in document A/CN.9/WG.IV/WP.157.

[20] If the first option in subparagraph (a) is retained, the Working Group may wish to consider adding a reference to the "authentication" of identity, consistent with the wording in the definition of "identity credentials" in article 1.

[21] The reference to privacy and data protection reflects the importance that the Working Group places on these topics while acknowledging that they fall outside the scope of the mandate of the Working Group (A/CN.9/965, para. 125).

[22] This new provision addresses a concern raised in the Working Group at its fifty-second session (A/CN.9/971, para. 30).

Article 6. Obligations of IdM service providers

An IdM service provider shall [at a minimum]:[23]

(a) Enrol subjects, including by:

(i) Registering and collecting attributes;

(ii) Carrying out identity proofing and verification; and

(iii) Binding the identity credentials to the subject;

(b) Update attributes;

(c) Manage identity credentials according to the rules governing the IdM system, including by:

(i) Issuing, delivering and activating credentials;

(ii) Suspending, revoking and reactivating credentials; and

(iii) Renewing and replacing credentials;

(d) Authenticate subjects, including by:

(i) Managing authentication factors; and

(ii) Managing authentication mechanisms;

(e) Ensure the online availability and correct operation of the IdM system; and

(f) Provide reasonable access to the rules governing the IdM system.[24]

Article 7. Obligations of IdM 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 IdM system, including the attributes managed therein, an IdM service provider shall:

(a) Immediately notify [the oversight authority] [affected subjects and relying parties] of the breach of security or loss of integrity;

(b) Remedy the breach of security or loss of integrity;

(c) Suspend affected [identity credentials] until the breach of security or loss of integrity is remedied;

(d) Re-establish affected [identity credentials] without delay; and

(e) Revoke affected [identity credentials] if the breach or loss cannot be remedied within [time frame].

2. If a subject notifies the IdM service provider of a breach of security or loss of integrity, the IdM service provider shall:

(a) Investigate the potential breach of security or loss of integrity; and

(b) Take any other appropriate action under paragraph 1.[25,26]

---

[23] These fundamental obligations of the IdM service provider have been identified with the assistance of experts.

[24] Letter (f) has been inserted to reflect the principle of transparency in the provision of IdM services (see also draft article 12, paragraph 2(b)). At its fifty-sixth session, the Working Group identified the principle of transparency as relevant for future discussions on IdM (A/CN.9/936, para. 88).

[25] This paragraph implements the suggestion that the draft provisions establish an obligation for IdM service providers to act upon security breach notifications (A/CN.9/971, para. 88).

[26] 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.

Article 8. Obligations of subjects and relying parties

1. The subject shall comply with the reasonable instructions communicated by the IdM service provider to avoid unauthorized use of the identity credentials or authentication processes.

2. The subject shall notify the IdM service provider if:

(a) The subject knows that the identity credentials or authentication processes of the relevant IdM system have been compromised; or

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

3. A relying party shall notify the IdM service provider if:

(a) The relying party knows that the identity credentials or authentication processes of the relevant IdM system have been compromised; or

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

Article 9. Identification using IdM systems

Where the law or a party requires the identification of a subject in accordance with a certain [method][policy], that requirement is met with respect to IdM if a reliable [method][IdM system] is used to identify the subject.[27,28,29]

Article 10. Factors relevant to determining reliability[30]

1. In determining the reliability of the [method][IdM system], all relevant circumstances shall be taken into account, which may include:

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

(b) Compliance of the rules governing the operation of the IdM system with any recognized international standards and procedures, including level of assurance framework, in particular rules on:

(i) Governance;

(ii) Published notices and user information;

(iii) Information security management;

(iv) Record-keeping;

(v) Facilities and staff;

---

[27] This provision reflects the working draft agreed on by the Working Group at its fifty-eighth session (A/CN.9/971, para. 49). The Working Group may wish to consider whether reference should be made to “reliable IdM system” instead of “reliable method”.

[28] The use of a reliable method (or IdM system) for identification is the cornerstone of the legal recognition regime for IdM in the draft instrument. The draft instrument foresees two mechanisms to determine reliability: draft article 10 provides an indicative list of factors relevant for ex post determination of reliability; draft article 11 provides for the establishment of a mechanism for ex ante designation of reliable methods (or IdM systems). Following consultations with experts, the provision dealing with a presumption of reliability (draft article 10 in document A/CN.9/WG.IV/WP.157) has been deleted to simplify the draft instrument. The content of paragraph 2 of draft article 10 in document A/CN.9/WG.IV/WP.157 has been incorporated in draft article 11, paragraph 5.

[29] The Working Group may wish to consider whether draft article 9 addresses cases in which a functional equivalence needs to be established between offline and online identification. If not, a new provision to that effect could be inserted along the following lines: “Where a rule of law requires or permits the identification of a subject, that rule is satisfied if a reliable IdM system is used”.

[30] The title of this provision reflects the agreement of the Working Group at its fifty-eighth session (A/CN.9/971, para. 59).

(vi) Technical controls; and

(vii) Oversight and audit;

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

(d) Any agreement between the parties.

2. In determining the reliability of the [method][IdM system], no regard shall be had:

(a) To the geographic location where the IdM system is operated; or

(b) To the geographic location of the place of business of the IdM service provider.[31]

Article 11. Designation of reliable IdM systems

1. [A person, organ or authority, whether public or private, specified by the enacting State as competent] may designate [methods][IdM systems] that are reliable for the purposes of article 9.[32,33]

2. Any designation made under paragraph 1 shall be consistent with recognized international standards and procedures relevant for determining the reliability of IdM systems, including level of assurance frameworks.[34,35]

3. In designating [a method][an IdM system], no regard shall be had:

(a) To the geographic location where the IdM system is operated; or

(b) To the geographic location of the place of business of the IdM service provider.[36]

4. The identification of a subject using identity credentials issued by an IdM system designated according to paragraph 1 shall be recognized as reliable proof of the subject's identity.

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

(a) To establish in any other way the reliability of [a method][an IdM system] for the purpose of article 9; or

(b) To adduce evidence of the non-reliability of [a method][an IdM system] designated pursuant to paragraph 1.

---

[31] This is a geographic non-discrimination provision based on article 12 of the UNCITRAL Model Law on Electronic Signatures (MLES) whose intended effect is to enable the cross-border recognition of IdM systems.

[32] This provision has been revised to reflect the amendments agreed by the Working Group at its fifty-eighth session (A/CN.9/971, para. 76), except for inserting a reference to article 9 due to the changes to that provision following consultations with experts. The words "that are reliable for the purposes of article 9" have been inserted instead.

[33] The Working Group may wish to consider whether the instrument should deal with liability for damages arising from the use of a system designated reliable under draft article 11.

[34] This provision has been revised to reflect the amendments agreed by the Working Group at its fifty-eighth session (A/CN.9/971, para. 76).

[35] The Working Group may wish to clarify whether and how the elements listed in draft article 10 apply to the designation of a reliable IdM system under draft article 11 (i.e., whether the designating person/organ/authority is required to take into account the circumstances listed in article 10, paragraph 1).

[36] This is a geographic non-discrimination provisions based on article 12 MLES whose intended effect is to enable the cross-border recognition of IdM systems.

Article 12. Liability of IdM service provider

1. The IdM service provider shall be liable for damage caused to any person due to intentional or negligent failure to comply with its obligations [arising from the provision of IdM services][under article 6].[37]

2. Notwithstanding paragraph 1, the IdM service provider shall not be liable for damage arising from the use of an IdM system to the extent that:

(a) That use exceeds the limitations [on the purpose or value of the transactions for which the IdM system may be used]; and

(b) The IdM service provider has provided reasonably accessible means that enable [a [user[38] or] third party][39] to ascertain those limitations.[40]

3. An IdM service provider shall not be liable for damage caused to any person arising from the use of an IdM system designated under article 11 if [the issuance of the identity credential or assignment of an attribute] is in compliance with:

(a) Its obligations arising from the provision of IdM services, including those listed in article 6;

(b) The rules governing the functioning of the IdM system, including those listed in article 10(1)(b); and

(c) Any agreement between the parties.

[4. Paragraph 3 does not apply if the damage is attributable to an act or omission of the IdM service provider that constitutes [gross negligence or wilful misconduct].][41]

Chapter III. Trust services[42]

Article 13. Legal recognition of trust services[43,44]

1. [An information] [Data][45] that is exchanged, verified or authenticated by use of, or with support of, a trust service [that meets the requirements of [this chapter]] shall

[37] This provision reflects the working draft agreed on by the Working Group at its fifty-eighth session (A/CN.9/971, para. 101). The provision has been further amended to clarify the cause of the damage for which liability is imposed.

[38] If used, the Working Group may wish to consider defining the term "user".

[39] The Working Group may wish to consider whether the parties that should be able to ascertain the limitations should be identified in the draft article and, if so, whether those parties should correspond to the parties to whom IdM system providers may be liable.

[40] This provision is based on article 9(1)(d)(ii) MLES.

[41] This paragraph reproduces paragraph 4 of draft article 13 in document A/CN.9/WG.IV/WP.157. The Working Group may wish to consider whether paragraph 4 may be deleted in light of paragraph 1.

[42] The chapter on trust services has been revised. It now features a general provision on legal recognition of trust services (draft article 13); a general reliability standard with a non-geographic discrimination clause to facilitate cross-border recognition (draft article 23); a mechanism for ex ante designation of reliable trust services (draft article 24) and a list of trust services (draft articles 16–22) to be used as "building blocks", also in combination, to provide assurance as to certain qualities of data. In particular, electronic signatures deal with the originator of the data ("who") and its intent in creating the data ("why"); electronic timestamps deal with the time when certain events concerning the data occurred ("when"); a new provision on integrity deals with the assurance that the data has not been changed since a certain point in time ("what"); and delivery services deal with the location of data messages in cyberspace ("where").

[43] This provision has been inserted to reflect the agreement of the Working Group at its fifty-eighth session (A/CN.9/971, paras. 112–115).

[44] The Working Group may wish to consider whether the focus of this non-discrimination provision should be on the information (or data) that is exchanged, verified or authenticated, or rather on the method used to verify and authenticate. A previous draft of this provision, based on the latter approach, read: "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 6, paragraph 2 in document A/CN.9/WG.IV/WP.157).

[45] The Working Group may wish to consider whether reference should be made to "data" to align the provision with the definition of "trust service".

not be denied legal effect, validity or enforceability [, or admissibility as evidence][46] on the sole ground that:

(a) It is in electronic form; or

(b) It is not supported by a reliable trust service designated pursuant to article 24.

2. Nothing in this [instrument] requires a person to use a particular trust service.[47]

3. Other than as provided for in this [instrument], nothing in this [instrument] affects the application to trust services of any rule of law applicable to trust services [including any rule of law applicable to privacy and data protection].[48]

Article 14. 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. If a breach of security or loss of integrity occurs that has a [significant] impact on trust services, the trust service provider shall:

(a) Suspend the provision of the affected services [until [the breach or loss are contained, or, alternatively, a new certification or similar process is achieved]]; and

(b) Remedy the breach of security or loss of integrity.

3. 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[49] 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.[50,51]

Article 15. Obligations of trust service users in case of data breach

A user[52] 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.

Article 16. Electronic signatures

Where a rule of law requires or permits a signature [of a person][of a subject], that rule is satisfied [in relation to a data message] if a reliable method[53] is used to:

---

[46] It is suggested to insert the words "or admissibility as evidence" to align this provision with draft article 5.

[47] Paragraphs 2 and 3 are inspired by draft article 2 in document A/CN.9/WG.IV/WP.157.

[48] The reference to privacy and data protection reflects the importance that the Working Group places on these topics while acknowledging that they fall outside the scope of the mandate of the Working Group (A/CN.9/965, para. 125).

[49] The Working Group may wish to consider defining the notion of "customer".

[50] This paragraph reproduces paragraph 2 of draft article 17 in document A/CN.9/WG.IV/WP.157. The Working Group may wish to consider whether the obligation contained therein could be listed instead as letter (c) of paragraph 2, in line with draft article 7.

[51] 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.

[52] The Working Group may wish to consider defining the term "user".

[53] Similar to the approach followed for the assessment of the reliability of IdM system, the draft provisions foresee two mechanisms to determine reliability of a trust service: draft article 23 provides an indicative list of factors relevant for ex post determination of reliability; draft article 24 provides for the establishment of a mechanism for ex ante designation of reliable trust services. Also similar to the approach followed for IdM systems, the provision dealing with a presumption of reliability (draft article 15 in document A/CN.9/WG.IV/WP.157) has been deleted

(a) Identify the person; and

(b) Indicate the person's intention in respect of the information contained in the data message.[54]

Article 17. Electronic seals[55]

Where a rule of law requires or permits a person to affix a seal, that rule is satisfied [in relation to a data message] if a reliable method is used to:

(a) Identify the person; and

(b) Detect any alteration to the data message after the time of affixation.

Article 18. Electronic timestamps

Where a rule of law requires or permits [certain documents, records, information or data[56]] to be associated with a time and date, that rule is satisfied [in relation to a data message] if a reliable method is used to:

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

(b) Associate that time and date with the data message.[57]

Article 19. Assurance of integrity[58]

Where a rule of law requires or permits the integrity of a [document, record, information or data] to be assured, [whether by retaining the document in its original form, archiving or otherwise,] that rule is satisfied in relation to a data message if a reliable method is used to detect any alteration to the data message after its creation, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display.[59]

Article 20. Electronic archiving[60]

Where a rule of law requires or permits [certain documents, records or information] to be retained, that rule is satisfied by retaining data messages, provided that:

---

to simplify the draft instrument. The content of paragraph 2 of draft article 15 in document A/CN.9/WG.IV/WP.157 has been incorporated in draft article 24, paragraph 5.

[54] It was suggested at the fifty-eighth session to include the words "in a way that a third party can later verify that intention" to address the function of "perpetuation" of electronic signatures (in a way that a third party can later verify that intention, see A/CN.9/971, para. 122). It has equally been suggested that it is unnecessary to include these words on the basis that the ability to carry out later verification is a necessary quality of signatures (ibid.).

[55] This provision reflects the agreement of the Working Group to insert a standalone provision on electronic seals (A/CN.9/971, para. 128). In keeping with the streamlined approach explained in footnote 42, the Working Group may wish to consider whether a standalone provision is necessary or whether the same function pursued with the use of electronic seals may be achieved by using electronic signatures (with respect to identification) and assurance of integrity (with respect to detection of alterations).

[56] The insertion of the word "data" reflects the agreement of the Working Group (A/CN.9/971, para. 130).

[57] The insertion of the words "and to identify a time zone" reflects the agreement of the Working Group (A/CN.9/971, para. 132).

[58] This provision is inserted to introduce a general rule for integrity of data messages. This rule offers the functional equivalent of the notion of "original" in the paper-based world. It is presented to the Working Group as an alternative to article 20 on electronic archiving. In this formulation of the rule, the trust service is clearly identified (i.e., providing the reliable method to detect alteration).

[59] The Working Group may wish to consider whether to include a requirement that the information contained in the data message is "accessible so as to be usable for subsequent reference" (see also draft article 20(a)).

[60] If draft article 19 is retained, the Working Group may wish to consider whether draft article 20 should be deleted as redundant.

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

(b) The data message is retained:

(i) In the format in which it was generated, sent or received; or

(ii) 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.[61]

Article 21. Electronic registered delivery services

Where a rule of law requires or permits proof of dispatch or receipt of [a certain document, record or information], that rule is satisfied [in relation to a data message] if a reliable method is used to provide assurance that the data message left or entered an information system.[62]

Article 22. Website authentication[63]

Where a rule of law requires or permits identification of a website owner, that rule is satisfied if a reliable method is used to identify the person that owns the website and to link that person to the website.

Article 23. Reliability standard for trust services[64]

1. For the purposes of articles [16 to 22], the method referred to shall be:

(a) As reliable as appropriate for the fulfilment of the function for which the method is being used, in the light of all relevant circumstances, which may include:

(i) Any operational rules governing the trust service;

(ii) Any applicable industry standard;

(iii) The security of hardware and software;

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

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

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

(vii) Any relevant agreement; or

(b) Proven in fact to have fulfilled the functions to which the relevant trust service relates.

2. In determining the reliability of the method for the purposes of articles [16 to 22], no regard shall be had:

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

---

[61] This condition does not extend to information the sole purpose of which is to enable the message to be sent or received: see article 10, paragraph 2 of the UNCITRAL Model Law on Electronic Commerce.

[62] The text reflects the agreement of the Working Group to incorporate in the draft provision elements of article 10 of the United Nations Convention on the Use of Electronic Communications in International Contracts (A/CN.9/971, para. 141).

[63] In keeping with the streamlined approach explained in footnote 42, the Working Group may wish to consider whether the functions pursued with website authentication may be achieved by identifying digital objects, including websites, with electronic signatures.

[64] The elements listed under paragraph 1(a) are inspired by article 10 MLES and article 12(a) of the UNCITRAL Model Law on Electronic Transferable Records, which sets out a general reliability standard for the method used.

(b) To the geographic location of the place of business of the trust service provider.[65]

Article 24. Designation of reliable trust services[66,67]

1. [A person, organ or authority, whether public or private, specified by the enacting State] may designate [methods][trust services] that are reliable for the purposes of articles [16 to 22].

2. Any designation made under paragraph 1 shall be consistent with recognized international standards and procedures relevant for determining the reliability of trust services, including level of reliability frameworks.[68]

3. In designating a [method][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.[69]

4. The use of a trust service designated according to paragraph 1 shall be recognized as reliable proof of [the quality of data to which it relates].

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

(a) To establish in any other way the reliability of [a method][a trust service] for the purpose of articles [16 to 22]; or

(b) To adduce evidence of the non-reliability of [a method][a trust service] designated pursuant to paragraph 1.

Article 25. Liability of trust service providers

1. The trust service provider shall be liable for damage caused to any person due to intentional or negligent failure to comply with its obligations [arising from the provision of trust services][under [article 14] [this instrument]].

2. Notwithstanding paragraph 1, the trust service provider shall not be liable for damage arising from the use of trust services to the extent that:

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

(b) The trust service provider has provided reasonably accessible means that enable [a [user[70] or] third party][71] to ascertain those limitations.[72]

---

[65] This is a geographic non-discrimination provisions based on article 12 MLES whose intended effect is to enable the cross-border recognition of trust services.

[66] This draft provision enables the possibility to carry out an ex ante assessment of reliability of trust services.

[67] The Working Group may wish to clarify whether and how the elements listed in draft article 23 apply to the designation of a reliable trust service under draft article 24 (i.e., whether the designating person, organ or authority is required to take into account the circumstances listed in article 23, paragraph 1(a)).

[68] This provision has been revised to reflect the amendments agreed by the Working Group at its fifty-eighth session (A/CN.9/971, para. 76).

[69] This is a geographic non-discrimination provisions based on article 12 MLES whose intended effect is to enable the cross-border recognition of trust services.

[70] If used, the Working Group may wish to consider defining the term “user”.

[71] The Working Group may wish to consider whether the parties that should be able to ascertain the limitations should be identified in the draft article and, if so, whether those parties correspond to the parties to whom trust services providers may be liable.

[72] This provision is based on article 9(1)(d)(ii) MLES.

Chapter IV. International aspects

Article 26. Cross-border recognition of IdM and trust services[73]

1. [An IdM system operated] [Identity credentials issued] or a 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 a trust service provided in [the enacting jurisdiction] if they offer [a substantially equivalent] [the same] level of reliability.[74,75]

2. 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].

Article 27. 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; and

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

---

[73] This provision reproduces paragraphs 2 and 3 of draft article 19 in document A/CN.9/WG.IV/WP.157. The Working Group may wish to consider whether this provision should be retained in light of the paragraphs on non-geographic discrimination inserted in articles 10, 11, 23 and 24.

[74] This provision is inspired by article 12, paragraph 2 MLES. Therefore, the term “level of reliability” as used in this draft provision does not necessarily have the same meaning as in other draft provisions of the instrument.

[75] The Working Group may wish to consider whether this provision implies the application to the foreign IdM or trust service of all rules of law of the enacting jurisdiction, including the provisions of this instrument as well as rules on limitation of liability under statute or contract.