United Nations A/CN.9/WG.IV/WP.170

General Assembly

Distr.: Limited
7 September 2021

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Sixty-second session
Vienna, 22–26 November 2021

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

Note by the Secretariat

Contents

		Page
I.	Introduction	2
II.	Issues for consideration	2
	A. Terminology	2
	B. Revision of draft provisions	3
	C. Liability	4
Annex		
	Draft Provisions on the Use and Cross-border Recognition of Identity Management (IdM) and Trust Services	5

V.21-06563 (E)

I. Introduction

1. The revised draft provisions on the use and cross-border recognition of identity management (IdM) and trust services set out in the annex to this document (the "present draft") incorporate the deliberations of the Working Group at its sixty-first session (6–9 April 2021), as reported in document A/CN.9/1051.[1]

2. Background information on the current work of Working Group IV is available in document A/CN.9/WG.IV/WP.169, paragraphs 4 to 20. The draft provisions considered by the Working Group at its sixty-first session, as set out in the annex to document A/CN.9/WG.IV/WP.167, are referred to as the "previous draft".

II. Issues for consideration

3. The deliberations of the Working Group at its sixty-first session focussed on the issues of terminology, trust services, liability, and cross-border recognition. Substantial progress was made in the consideration of those issues. In this section, the secretariat offers some additional comments to assist the Working Group in continuing its consideration of those issues.

A. Terminology

4. It has been acknowledged in the Working Group that IdM comprises two stages. Different terminology has been used in previous sessions of the Working Group to refer to the two stages. No decision was taken as to which terms to use. Moreover, in some instances a decision has yet to be taken on whether to refer to IdM in terms of a "system" or "services":

(a) In the present draft (like in the previous draft), the first stage is referred to as "identity proofing". However, it has been noted in the Working Group that, in technical terminology, this stage can be referred to as "identification".[2] It has also been referred to as "enrolment",[3] and indeed the present draft (as in the previous draft) acknowledges that identity proofing is part of enrolment (see art. 6(a)(i));

(b) For the second stage, the present draft (like the previous draft) uses the term "electronic identification", although the terms "authentication" and "verification" have also been used in the Working Group.[4] It has also been suggested in the Working Group that "authentication" should be used to refer to "identify proofing" (i.e., the first stage).[5] Moreover, it has been noted that "identification" is used in the second stage to refer to the assertion of an identity (which then needs to be "authenticated" or "verified").[6] Added to this difference in terminology is the use of the term "electronic authentication" in recent electronic commerce chapters of regional trade agreements;[7] while the term is not given a uniform meaning across those agreements, it generally corresponds to the second stage of identity

[1] In the footnotes accompanying the present draft, the draft provisions considered by the Working Group at its sixtieth session, as set out in document A/CN.9/WG.IV/WP.162, are referred to as the "previous draft". The draft also makes reference to other UNCITRAL texts on electronic commerce, namely the UNCITRAL Model Law on Electronic Commerce ("MLEC"), UNCITRAL Model Law on Electronic Signatures ("MLES"), the United Nations Convention on the Use of Electronic Communications in International Contracts ("ECC") and the Model Law on Electronic Transferable Records ("MLETR").

[2] A/CN.9/1005, para. 84.

[3] Ibid.

[4] Ibid.

[5] A/CN.9/1051, para. 67.

[6] Ibid.

[7] See, e.g. Comprehensive and Progressive Agreement for Trans-Pacific Partnership, article 14.1; United States-Mexico-Canada Agreement, article 19.1; Regional Comprehensive Economic Partnership, article 12.1(c).

management.[8] At the sixty-first session of the Working Group, broad support was expressed in favour of using "electronic identification" to refer to the second stage, while some support was expressed in favour of using "authentication";[9]

(c) The draft provisions refer to IdM systems and IdM services. Both terms are defined in article 1. In most instances, the present draft refers to IdM services. In some provisions, however, the present draft refers to IdM systems either (i) as distinct from IdM services (see, e.g. articles 6, 7, 12 and 25) or (ii) as an alternative to referring to IdM services (see, e.g. articles 5, 10 and 11, which refer to the reliability and designation of "IdM systems" and "IdM services"). While the interaction between IdM systems and IdM services has been discussed in previous sessions,[10] the Working Group may wish to confirm, for the latter references, whether the term "IdM system" should be used instead of "IdM services" or vice versa.

B. Revision of draft provisions

5. Articles 16 to 21 of the draft instrument have been reformulated to reflect the deliberations of the Working Group. In particular:

(a) *Where the law "permits"* – the draft provisions no longer refer to a rule of law "permitting" the corresponding paper-based practice. As such, the draft provisions have reverted to the formulation used in the UNCITRAL Model Law on Electronic Commerce ("MLEC") and the United Nations Convention on the Use of Electronic Communications in International Contracts ("ECC");[11]

(b) *Presumption of reliability* – to avoid repetition, the common rules establishing the presumption of reliability of methods used by a designated trust service, as set out in paragraphs 2 and 3 of articles 16 to 21 of the previous draft, have been consolidated in article 22;[12]

(c) *Relative standard of reliability* – the reliability requirements in article 22 have been revised by inserting paragraph 1(a) to acknowledge that the reliability of a method used by a trust service is relative and not absolute.[13] The paragraph is based on article 9(3)(b)(i) of the ECC, by which reliability is determined relative to the "purpose" of the underlying data message (i.e. the electronic communication to which the electronic signature is applied).

The corresponding provisions in chapter II on IdM (i.e. articles 9 and 10) have been revised to mirror those changes.

6. In addition, provisions of chapter III with respect to trust services have been aligned with provisions of chapter II with respect to IdM where those provisions perform the same function.[14] In particular:

(a) *Obligations of trust service providers* – a new obligation to have in place operational rules, policies and practices has been inserted in article 14(1)(a). It is based on the obligation of IdM service providers contained in article 6(a). The existing obligation in article 14(1)(b) has been revised to align with the existing obligation of IdM service providers in article 6(b). As a result, both trust service providers and IdM service providers are now obliged to act in accordance with their operational rules, policies and practices *and* with any representations made by them with respect to

[8] In some regional trade agreements, the term "authentication" extends to assuring the integrity of data messages, which is a function addressed by trust services in the present draft.
[9] A/CN.9/1051, para. 67.
[10] See A/CN.9/1045, para. 126 and A/CN.9/1051, para. 59. See also discussion in A/CN.9/WG.IV/WP.171.
[11] A/CN.9/1051, paras. 42–44.
[12] Ibid., paras. 31–34.
[13] Ibid., para. 45.
[14] Ibid., para. 52.

those rules, policies and practices. The existing obligations in articles 6(d) and (e) have also been revised to align with articles 14(1)(c) and (d);

(b) *Obligations of subscribers* – article 15 has been revised to pick up the wording of the corresponding obligation in article 8.

C. Liability

7. The liability rules in articles 12 and 24 of the draft instrument have been reformulated to reflect the deliberations of the Working Group at its sixty-first session.[15]

8. The present draft retains "option B" of the previous draft for which broad support has been expressed in preference to "option A" of that draft. The reference to the elements of fault ("negligence" and "intentional") has been removed, and the term "loss" has been used instead of "damage".[16] As such, the present draft establishes a new basis for liability that is distinct from contractual liability.[17]

9. Consensus has not yet been reached on the substance of the liability rules. Several issues were raised at the sixty-first session, which the Working Group may wish to consider further at its sixty-second session, including:

(a) *Relationship with contract*[18] – under the present draft, liability arises from a failure of the service provider to comply with the obligation under the draft instrument to act in accordance with its operational rules, policies and practices. Those rules, policies and practices would ordinarily be incorporated into a contract between the subscriber and service provider. Accordingly, breach of contract may engage liability of the service provider both under the draft instrument and under contract law. National law could in turn impact the ability of the service provider to limit or exclude its liability according to articles 12(3) and 24(3). The Working Group may therefore wish to consider the extent to which the service provider can limit by contract its liability under the draft instrument other than as provided for in articles 12(3) and 24(3);

(b) *Other legal consequences* – under the present draft, liability for loss is not the only legal consequence that flows from a failure of the service provider to comply with an obligation under the draft instrument. Such a failure may compromise not only the reliability of the method used by the service provider (see articles 10(2)(a) and 22(2)(a)), but also the designation of the service provider (see articles 11(2)(a) and 23(2)(a)).

10. A related issue raised at the sixty-first session of the Working Group in the context of liability was the relationship between the obligations under the draft instrument and contractual obligations. The prevailing view expressed in the Working Group is that, for at least some of those obligations, there is no room for contractual deviation.[19] The Working Group has also heard suggestions that, by framing the relevant provision as establishing "minimum" requirements, those obligations could be supplemented, but not derogated, by contract. In other words, the draft provisions establish a mandatory floor. The Working Group may wish to further consider this matter.

[15] Ibid., paras. 13–29.
[16] Ibid., para. 21.
[17] Ibid., para. 24.
[18] Ibid., para. 16.
[19] A/CN.9/1045, para. 19.

Annex

Draft Provisions on the Use and Cross-border Recognition of Identity Management (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 person;

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

(c) "Electronic identification" ["Authentication"], in the context of IdM services, means a process used to achieve sufficient assurance in the binding between a person and an identity;[20]

(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) "IdM services" means services consisting of managing identity proofing or electronic identification of persons in electronic form;[21]

(g) "IdM service provider" means a person that provides IdM services;[22]

(h) "IdM system" means a set of functions and capabilities to manage identity proofing and electronic identification of persons in electronic form;[23]

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

(k) "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;[24]

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

Article 2. Scope of application

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

---

[20] See paragraph 4 above.

[21] The Working Group may wish to consider whether the words "of persons in electronic form" may be deleted in light of the definitions of "identity proofing" and of "electronic identification".

[22] The Working Group may wish to consider whether the word "any" should be inserted before "IdM services" to clarify that not all the functions listed in article 6 may be relevant to all IdM systems and therefore that an IdM service provider might not perform each listed function (A/CN.9/1045, para. 88).

[23] See footnote 21.

[24] The definition of "trust service" has been revised to reflect the deliberations of the Working Group at its sixty-first session (A/CN.9/1051, paras. 35–36).

2. Nothing in this [instrument] requires:[25]

(a) The identification of a person;

(b) The use of a particular IdM service; or

(c) The use of a particular trust service.

[where the person's identification or the use of a particular IdM service or trust service is not required by applicable law or the agreement of the parties.] [26]

3. Nothing in this [instrument] 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.[27]

4. Other than as provided for in this [instrument], nothing in this [instrument] affects the application to IdM services or trust services of any law applicable to data protection and privacy.[28]

Article 3. Voluntary use of IdM and trust services[29]

1. Nothing in this [instrument] requires a person to use an IdM service or trust service [or to use a particular IdM service or trust service] [30] 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 [instrument], 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 [instrument] which are not expressly settled in it are to be settled in conformity with the general principles on which it is based.[31]

---

[25] Article 2(2) aims to preserve technology and model neutrality while article 3(1) aims to preserve party autonomy. The Working Group may wish to consider whether paragraphs 2 and 3 of article 2, which relate to the operation of the provisions, should be placed in article 3. In that case, article 2 would only delimit the subject matter scope of the instrument. Alternatively, the Working Group may wish to consider whether only paragraphs (2)(b) and (c) should be incorporated in article 3(1) (see footnote 30).

[26] The bracketed text aims to signal that paragraph 2 does not affect any law or contractual agreement imposing a duty to identify or to use specific IdM and trust services.

[27] Article 2(3) applies to limit the use of IdM. The Working Group may wish to consider whether it should be extended to limit the use of trust services and, if so, whether to insert the text in square brackets. A different approach is taken in the MLEC and in the UNCITRAL Model Law on Electronic Signatures (MLES), which limit the use of trust services within scope (e.g. electronic signatures) by prompting enacting jurisdictions to specify particular exclusions (including by reference to particular laws): see art. 7(3) MLEC and art. 1 MLES (with accompanying notes).

[28] In keeping with existing UNCITRAL model laws (as explained in footnote 10 of A/CN.9/WG.IV/WP.167), article 2(4) has been revised to remove the general preservation of "any applicable rule of law", while retaining the specific preservation of laws applicable to data protection and privacy.

[29] Article 3 is based on article 8(2) ECC, which deals with the voluntary use and acceptance of electronic communications. The Working Group has agreed that the provision should protect both the subscriber and the relying party against the imposition of any new obligation to use IdM or trust services (A/CN.9/1005, para. 116). Consistent with article 8(2) ECC, the Working Group may wish to consider adding the words "or accept" after the word "use". It may also wish to consider replacing "an IdM service or trust service" with "electronic identification or a trust service".

[30] The bracketed text aims to implement the suggestion to incorporate article 2(2)(b) and (c) in article 3 (see footnote 25).

[31] Article 4(2) has been revised to reflect the decision of the Working Group at its sixty-first session (A/CN.9/1051, para. 56).

Chapter II. Identity management

Article 5. Legal recognition of IdM

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

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

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

Article 6. Obligations of IdM service providers[32]

An IdM service provider shall[, at a minimum]:[33]

(a) Have in place operational rules, policies and practices, as appropriate to the purpose[34] and design of the IdM system, to address [at a minimum][35] 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 IdM system;

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

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

---

[32] See paragraph 6(a) above (on aligning the obligations with those of trust service providers) and paragraph 10 (on the relationship with contractual obligations).

[33] The words “at a minimum” are contained in the chapeau of article 6 and in paragraph (a). Those words were inserted in paragraph (a) following deliberations at the sixtieth session of the Working Group and are designed to address the concern that the paragraph might otherwise allow an IdM service provider to disclaim responsibility for carrying out functions related to the IdM service that were carried out by a contractor (e.g. a separate entity in a multi-party private sector IdM system) (see A/CN.9/1045, para. 90). The Working Group may wish to consider whether the words “at a minimum” in the chapeau of article 6 already address that concern, and therefore that the words in article 6(a) may be deleted.

[34] The Working Group may wish to consider whether this provision should refer to “function” rather than “purpose”, given the use of the terms “function” and “purpose” in article 10(1), which is based on established UNCITRAL terminology.

[35] See footnote 33.

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, the IdM service provider shall, [in accordance with the law]:[36]

(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 [in accordance with the law].[37]

2. If a person notifies the IdM service provider of a breach of security or loss of integrity, the IdM 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[38]

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

(a) The subscriber knows that the subscriber's identity credentials have [or may 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 IdM[39]

Subject to article 2, paragraph 3, where the law requires the identification of a person [for a particular purpose], [40] or provides consequences for the absence of identification, that requirement is met with respect to IdM services if a method is used for the electronic identification of the person [for that purpose].

Article 10. Reliability requirements for IdM [services][systems]

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

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

(b) Proven in fact to have fulfilled the function described in article 9.[41]

---

[36] At the sixtieth session of the Working Group, it was indicated that several actions listed in article 7 could fall under data protection and privacy laws, and therefore that all actions listed, not just notification, should be performed in accordance with applicable law (A/CN.9/1045, para. 99). The Working Group may wish to consider whether to delete the words "in accordance with the law" from article 7(1)(c) and to insert those words at the end of the chapeau of article 7(1) as indicated in square brackets.

[37] See footnote 36.

[38] Article 8 has been revised in view of the decisions of the Working Group at its sixtieth session (A/CN.9/1045, para. 105). The chapeau has been further revised to emphasize that the provision is primarily concerned with notification as opposed to particular means of notification. The provision was not considered further by the Working Group at its sixty-first session, and therefore the square brackets in subparagraphs (a) and (b) remain.

[39] Article 9 reflects the decisions of the Working Group at its sixtieth session (A/CN.9/1045, para. 117). It has also been further revised as explained in paragraph 5 above.

[40] See footnote 34.

[41] The Working Group may wish to consider whether paragraph 1(b) of article 10 (and the corresponding provision in article 22) should be retained or could be deleted in light of paragraph 5(a) of article 10, which may already provide this effect when the method has in fact fulfilled its function.

2. In determining the reliability of the method, 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 operational rules, policies and practices of the IdM service provider with any applicable recognized international standards and procedures relevant for the provision of IdM services, including [level of assurance framework][levels of assurance or similar frameworks providing guidelines to designate the degree of confidence in IdM systems],[42] 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 IdM system;

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

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

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

(a) To the geographic location where the [IdM system is operated][IdM service is provided]; or

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

4. A method used by an IdM system [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 a IdM system designated pursuant to article 11.

Article 11. Designation of reliable IdM systems [services]

1. [*A person, organ or authority, whether public or private, specified by the enacting jurisdiction as competent*] may designate IdM systems [services] that are presumed reliable.[43]

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

[42] The words “levels of assurance or similar frameworks providing guidelines to designate the degree of confidence in IdM systems” aim to capture the various forms in which those frameworks may be formulated. “Level of assurance” is a term defined in document A/CN.9/WG.IV/WP.150. The Working Group may wish to confirm whether the words are adequate to describe the concept of “level of assurance framework”.

[43] See paragraph 4(c) above. The Working Group may wish to consider whether article 11 should refer to designation of systems or services, noting that article 23 refers to designation of services. See A/CN.9/1045, paragraph 126, for the latest discussion of the Working Group on this point.

(a) Take into account all relevant circumstances, including the factors listed in article 10, in designating an IdM system [service]; and

(b) Publish a list of designated IdM systems [services], including details of the IdM service provider[, or otherwise inform the public].[44]

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.[45]

4. In designating an IdM system [service], no regard shall be had:

(a) To the geographic location where the IdM system is operated [service is provided]; or

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

Article 12. Liability of IdM service providers[46]

1. The IdM service provider shall be liable for loss caused [to any person] due to a failure to comply with its obligations under [this instrument].

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 under [this instrument] of a failure of the IdM service provider to comply with its obligations under [this instrument].

3. Notwithstanding paragraph 1, the IdM service provider shall not be liable to the subscriber for loss 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;

[(b) Those limitations are agreed between the IdM service provider and the subscriber;][47] and

(c) The IdM service provider has notified [informed] [48] the subscriber of those limitations in accordance with the law.

---

[44] At its sixtieth session, the Working Group agreed to place the words "otherwise inform the public" in square brackets for further consideration. The words aim to capture means of informing the public other than the publication of lists. At the sixtieth session, several delegations insisted that, while other means may be used, it was essential to retain an obligation to publish a list of designated IdM systems (A/CN.9/1045, para. 128). The words were not considered by the Working Group at its sixty-first session. If the words are retained, the Working Group may wish to consider inserting them also in article 23(2)(b).

[45] The reference to "level of assurance framework" will be revised based on the outcome of deliberations on article 10(2)(b).

[46] See paragraphs 7 to 10 above.

[47] Paragraph 3(b) of article 12 has been added to reflect the understanding of the Working Group that limitations of liability may be recognised provided these are agreed upon.

[48] Paragraph 3(c) of article 12 does not aim to introduce a new obligation but to refer to existing obligations under applicable law. To avoid doubt, the Working Group may wish to consider whether the word "informed" is more appropriate than the word "notified" to that end.

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:[49]

(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 [functions] [50] of the trust service;

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

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

(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.

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]:[51]

(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 [in accordance with the law].[52]

Article 15. Obligations of subscribers[53]

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 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 so compromised.

Article 16. Electronic signatures

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

(a) To identify the person; and

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

---

[49] See paragraph 6(a) (on aligning the obligations with those of IdM service providers) and paragraph 10 (on the relationship with contractual obligations) above.

[50] See footnote 34.

[51] See footnote 33.

[52] Ibid.

[53] See paragraph 6(b) above. The provision will be revised in light of the outcome of the discussions on article 8.

Article 17. Electronic seals

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

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

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

Article 18. Electronic timestamps

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

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

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

Article 19. Electronic archiving

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

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

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

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

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

Article 20. Electronic registered delivery services

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

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

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

(c) To identify the sender and the recipient.

Article 21. Website authentication

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

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

(b) To associate that person to the website.

Article 22. Reliability requirements for trust services

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

(a) As reliable as appropriate for the purpose[54] for which the trust service is being used; or

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

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

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

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

(c) Any applicable industry standard;

(d) The security of hardware and software;

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

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

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

(h) The function[55] for which the trust service is being used;[56] and

(i) 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

[54] See footnote 34.

[55] See footnote 34.

[56] Article 22(1)(h) reflects a decision of the Working Group at its sixtieth session (A/CN.9/1045, para. 56). The Working Group may wish to note that this factor differs from the factor included in article 10(2)(d).

(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 any person] due to a failure to comply with its obligations under [this instrument].

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 under [this instrument] of a failure of the trust service provider to comply with its obligations under [this instrument].

3. Notwithstanding paragraph 1, the trust service provider shall not be liable to the subscriber for loss 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;

[(b) Those limitations are agreed between the trust service provider and the subscriber;][57] and

(c) The trust service provider has notified[58] the subscriber of those limitations in accordance with the law.

Chapter IV. International aspects

Article 25. Cross-border recognition[59]

1. An IdM system operated, an identity credential issued, or an IdM service or trust service provided outside [*the enacting jurisdiction*] shall have the same legal effect in [*the enacting jurisdiction*] as an IdM system operated, identity credential issued or an IdM service or trust service provided in [*the enacting jurisdiction*] if it offers [a substantially equivalent][at least an equivalent] level of reliability.

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

[3. Equivalence shall be presumed if [*the person, organ or authority specified by the enacting jurisdiction*] according to article 11 and 23 has determined the equivalence for the purposes of this paragraph.][60]

---

[57] See footnote 47.

[58] See footnote 48.

[59] Paragraphs 1 and 2 of article 25 have been revised to reflect the deliberations of the Working Group at its sixty-first session (A/CN.9/1051, paras. 60 and 61).

[60] Paragraph 3 of article 25 was considered by the Working Group at its sixty-first session (A/CN.9/1051, paras. 63-66). The Working Group agreed to retain the paragraph for further

Article 26. Cooperation

[*The person, organ or authority specified by the enacting jurisdiction as competent*] [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) Recognition of the legal effects of foreign IdM systems and trust services, whether granted unilaterally or by mutual agreement;

(b) Designation of IdM systems and trust services; and

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

consideration, subject to a minor amendment to correct the reference to the designating authority (ibid., para. 66).