United Nations A/CN.9/WG.IV/WP.167

General Assembly

Distr.: Limited
26 January 2021

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Sixty-first session
New York (online), 5–9 April 2021

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

Note by the Secretariat

Contents

V.21-00518 (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 sixtieth session (Vienna, 19–23 October 2020), as reported in A/CN.9/1045.[1]

2. Background information on the current work of Working Group IV is available in document A/CN.9/WG.IV/WP.166, paragraphs 4–17.

[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").

Annex

Draft Provisions[2] 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;[3]

(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;[4]

(f) "IdM services" means services consisting of managing identity proofing or electronic identification of persons in electronic form;[5]

(g) "IdM service provider" means a person that provides IdM services;[6]

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

(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;

---

[2] *Form of instrument*: During preliminary discussions on the issue at the fifty-ninth session of the Working Group, a strong preference was expressed for the instrument to take the form of a model law as opposed to a convention (A/CN.9/1005, para. 123). In the present draft, the term "[instrument]" is used pending the decision of the Working Group on the issue when transmitting the instrument to the Commission for adoption.

[3] *Definitions – "electronic identification"*: The present draft continues to use the term "electronic identification" instead of "authentication" to address the concerns on the multiple meanings of "authentication" (A/CN.9/1005, paras. 13, 84–86, 92). At the sixtieth session of the Working Group, support was expressed for the use of the term "authentication" (A/CN.9/1045, para. 134) and the Working Group agreed to place the definitions of "authentication" and "electronic identification" in square brackets for further consideration (ibid., para. 136). As the definition of "authentication" in the previous draft was only used in the context of trust services (i.e. as "a process used to attribute an identifier to an object"), the term "authentication" (and not the definition of that term) has been placed in square brackets in the present draft.

[4] *Definitions – "identity credentials"*: The Working Group discussed this definition at its sixtieth session (A/CN.9/1045, para. 137). In the present draft, the definition has been amended by replacing the words "the electronic identification of its identity in electronic form" with the words "electronic identification" to avoid superfluity. The Working Group may wish to confirm the definition as amended.

[5] *Definitions – "IdM services"*: This definition reflects the understanding that IdM comprises two stages (or phases): "identity proofing" and "electronic identification". The Working Group may wish to consider whether the definition of "IdM services" should refer to the functions listed in article 6(a). In that case, the words ", including the services listed in article 6(a)" may be added at the end of the definition.

[6] *Definitions – "IdM service provider"*: 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 may not perform each listed function (A/CN.9/1045, para. 88).

(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;[7]

(k) "Trust service" means an electronic service that provides assurance of certain qualities of a data message and includes electronic signatures, electronic seals, electronic time stamps, website authentication, electronic archiving and electronic registered delivery services;[8]

(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 systems and trust services in the context of commercial activities and trade-related services.

2. Nothing in this [instrument] requires:

(a) The identification of a person;

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

(c) The use of a particular trust service.

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.[9]

4. Other than as provided for in this [instrument], nothing in this [instrument] affects the application to IdM services or trust services of any [applicable rule of law, including any rule of][10] law applicable to data protection and privacy.[11]

---

[7] *Definitions – "subscriber"*: At the fifty-ninth session, preference was expressed for the use of the term "subscriber" to refer to the person to whom services are provided (A/CN.9/1005, paras. 43 and 96). At its sixtieth session, the Working Group confirmed its support for the definition of "subscriber" as reflected in the present draft (A/CN.9/1045, para. 22). It was added that the signatory of an electronic signature would fall within the definition (ibid.), and suggested that relying parties would not (ibid., para. 18).

[8] *Definitions – "trust services"*: The term "trust services" was not considered by the Working Group at its sixtieth session. Based on the deliberations of the Working Group at its fifty-ninth session, the definition (which remains unchanged from the previous draft) combines a stand-alone "abstract" definition, which focuses on the veracity and genuineness of the underlying data, with a non-exhaustive list of the trust services that are covered in the draft instrument (A/CN.9/1005, para. 18).

[9] *Preserving laws requiring a particular procedure*: 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 in taken in the MLEC and 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).

[10] *Preserving other domestic laws*: Article 2(4) was drafted before the Working Group discussed the form of the instrument. The Working Group may wish to consider whether, if the draft provisions take the form of a model law (see footnote 2), the words in square brackets can be deleted. UNCITRAL texts assume that the provisions of a model law will be enacted as part of the domestic legislation of the enacting jurisdiction, to which existing rules of that jurisdiction dealing with conflicting legislation will apply. While UNCITRAL model laws may expressly preserve specific laws (e.g., art. 1(2) MLETR), they do not preserve the application of "any" other laws outside the model law. Moreover, the reference to "applicable" law may be misunderstood as a reference to the law applicable by virtue of the relevant rules of private international law. See also footnote 19 for considerations on the relationship between article 2(4) and article 7.

[11] *Preserving data protection and privacy laws*: At the sixtieth session of the Working Group, it was suggested that article 2(4) should refer to "data protection and privacy" (rather than "privacy and data protection") to acknowledge that the provision was concerned with "data privacy" and not with privacy in other contexts. The Working Group may wish to confirm that reference, as reflected in the present draft.

Article 3. Voluntary use of IdM and trust services[12]

1. Nothing in this [instrument] requires a person to use an IdM service or trust service without the person's consent.

2. For the purposes of paragraph 1, consent may be inferred from the person's conduct.

Article 4. Interpretation

1. In the interpretation of this [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[or, in the absence of such principles, in conformity with the law applicable by virtue of the rules of private international law].[13]

Chapter II. Identity management

Article 5. Legal recognition of IdM[14]

Subject to article 2, paragraph 3, the electronic identification of a person 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 a designated IdM system pursuant to article 11.

Article 6. Obligations of IdM service providers[15]

An IdM service provider shall [at a minimum]:[16]

---

[12] *Voluntary use of IdM and trust services*: Article 3 remains unchanged from the previous draft (see A/CN.9/1045, para. 80). It 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".

[13] *General principles*: Article 4(2) mirrors article 5(2) ECC. The Working Group may wish to consider whether the text in square brackets can be deleted. At the fifty-ninth session, it was explained that a reference to interpretation in accordance with applicable law was useful in case the instrument took the form of a convention (A/CN.9/1005, para. 117; see further explanation in A/CN.9/527, para. 124). None of the UNCITRAL model laws on electronic commerce contains this additional reference. As noted above (footnote 10), UNCITRAL texts assume that the provisions of a model law will be enacted as part of the domestic legislation of the enacting jurisdiction, to which the general rules of interpretation of that jurisdiction will apply.

[14] *Legal recognition of IdM – general*: Article 5 has been revised to reflect the decisions of the Working Group at its sixtieth session (A/CN.9/1045, para. 84).

[15] *Obligations of IdM service providers*: Article 6 has been revised to reflect the decisions of the Working Group at its sixtieth session (A/CN.9/1045, para. 95). At that session, it was explained that, in the case of private sector IdM systems, the functions listed would ordinarily be governed by contractual rules. It was noted that not all functions listed in article 6 would be relevant for all IdM services providers (e.g. multi-party IdM systems). It was also observed that article 6 should ensure that the IdM service provider remains responsible for the full suite of IdM services provided to the subscriber (i.e. all the functions listed in article 6), and that article 6 did not prevent the service provider from outsourcing any function or from allocating risk among its contractors (ibid, paras. 90–91).

[16] The words "at a minimum" were inserted to indicate that the functions listed represent the "fundamental obligations" of the IdM service provider, which may be supplemented by

(a) Have in place operational rules, procedures and practices, as appropriate to the purpose and design [17] of the IdM system, to address [at a minimum] [18] 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 according to the operational rules, procedures and practices;

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

(d) Provide reasonable access to the operational rules, procedures and practices; and

(e) Make available reasonable means for the subscriber to give notice pursuant to article 8.

Article 7. Obligations of IdM service providers in case of data breach[19]

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) 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;

---

contractual obligations under operational rules (see A/CN.9/WG.IV/WP.160). The Working Group may wish to confirm that their effect is also to leave no room for contractual deviation.

[17] At the sixtieth session of the Working Group, it was explained that the purpose of the words "as appropriate to the purpose and design" was to give flexibility in the design of IdM systems (A/CN.9/1045, para. 90). The Working Group may wish to consider whether it is more appropriate to refer to the "structure" of an IdM system (rather than to its "design").

[18] The words "at a minimum" were inserted in article 6(a) following deliberations at the sixtieth session of the Working Group and are designed to address the concern, already identified in footnote 15, that the wording of new paragraph (a) might 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.

[19] *Obligations of IdM service providers in case of data breach*: The Working Group may wish to confirm that article 7 establishes a minimum standard from which the operational rules of the IdM system or other contractual arrangement cannot deviate, bearing in mind the Working Group's prevailing view that article 14(2) establishes such a minimum standard (A/CN.9/1045, para. 19). The Working Group may also wish to clarify, in light of the proviso in article 2(4) that data protection and privacy laws are not affected by the instrument "other than as provided in this instrument", the relationship between article 7 and those laws (for the view indicating that article 7 would effectively find application only in jurisdictions that do not have any data protection and privacy laws, see A/CN.9/1045, paras. 97–98).

(c) Notify the breach or loss in accordance with the law.[20,21]

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[22]

The subscriber shall notify the IdM service provider, by utilizing the 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.]"[23]

Article 9. Identification of a person using IdM[24]

1. Subject to article 2, paragraph 3, where a rule of law requires or permits the identification of a person [for a particular purpose], that rule is satisfied with respect to IdM services if a reliable method is used for the electronic identification of the person [for that purpose].[25]

---

[20] *References to "applicable law"*: In keeping with other UNCITRAL model laws on electronic commerce, the present draft refers to "the law" rather than "applicable law".

[21] *Role of other laws governing the handling of data security breaches*: 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, consistent with the approach outlined in footnote 20, insert the words ", in accordance with the law" at the end of the chapeau of article 7(1).

[22] *Obligations of subscribers*: 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 words "utilize means made available by the IdM service provider pursuant to article 6, or otherwise use reasonable means, to notify the IdM service provider" have been reformulated accordingly.

[23] *Obligations of subscribers – knowledge of compromised credentials*: Paragraph (b) aims at addressing cases in which the subscriber is presumed to know of compromised credentials.

[24] *Legal recognition of IdM – general*: Article 9 has been revised to reflect the decisions of the Working Group at its sixtieth session (A/CN.9/1045, para. 117). At that session, it was explained that article 9 aimed at providing a functional equivalence rule for identification in those cases where the law required identification but did not specify a procedure to identify, or where the parties agreed to identify. It was also explained that the functional equivalence rule would, in line with established principles in UNCITRAL texts, complement the rule on legal recognition set out in article 5. It was added that the instrument did not affect requirements to identify according to a specific procedure, as set out in article 2(3). Finally, it was said that the rule operated only when an offline equivalent existed, since the goal of the rule was to establish requirements for equivalence between offline and online identification (ibid., para. 106). If no offline equivalent exists, article 5 remains relevant in ensuring that the use of electronic identification is not denied legal recognition on grounds alone that it is carried out by electronic means (e.g. by exchange of data messages).

[25] *Legal recognition of IdM – offline equivalent*: The inclusion of the words in square brackets referring to purpose aims to address a concern raised at the sixtieth session regarding verification of sufficient attributes (A/CN.9/1045, paras. 110–111). It was explained that, without correlating the attributes required to satisfy an offline identification requirement with the attributes contained in the identity credentials used for electronic identification, article 9 would be inadequate as a functional equivalence rule. It was added that the issue was not addressed by the reliability test as that was concerned with the processes in managing identity credentials rather than with the attributes contained in identity credentials (ibid., para. 113). The need to include

2. A method is presumed to be reliable for the purposes of paragraph 1 if an IdM system designated pursuant to article 11 is used.

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

(a) To establish in any other way, for the purpose of paragraph 1, the reliability of a method pursuant to article 10; or

(b) To adduce evidence of the non-reliability of a designated IdM system.

Article 10. Requirements for determining reliability of IdM [services][systems][26]

1. In determining the reliability of the method for the purposes of article 9, all relevant circumstances shall be taken into account, which may include:[27]

(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 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 the methods and processes used by IdM systems],[28] 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.

2. In determining the reliability of the method, 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.

---

the text in square brackets was questioned at the sixtieth session (ibid., para. 116). The reasoning for that view was that, if electronic identification involves linking a person to an "identity", and if "identity" is defined as a set of attributes that allows the person to be "uniquely distinguished within a particular context", the context in which the offline identification requirement applies, including its purpose, would already determine the attributes required for electronic identification.

[26] *Requirements for determining reliability – title*: The title of article 10 has been changed to reflect the deliberations at the sixtieth session of the Working Group (A/CN.9/1045, para. 124).

[27] *Factors relevant to determining reliability*: Article 10 has been revised to reflect the decisions of the Working Group at its sixtieth session (A/CN.9/1045, paras. 118 and 120).

[28] *Levels of assurance*: The words "levels of assurance or similar frameworks providing guidelines to designate the degree of confidence in the methods and processes used by 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 these words are adequate to describe the concept of "level of assurance framework".

Article 11. Designation of reliable IdM systems[29]

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

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

(a) Take into account all relevant circumstances, including the factors listed in article 10, in designating an IdM system [service];[30] and

(b) Publish a list of designated IdM systems [services], including details of the IdM service provider[, or otherwise inform the public].[31]

3. Any designation made under paragraph 1 shall be consistent with recognized international standards and procedures relevant for performing the designation process, including level of assurance frameworks.

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

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

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

Article 12. Liability of IdM service provider[32]

Option A for article 12[33]

The liability of IdM service providers shall be determined according to the law.

Option B for article 12[34]

1. Without prejudice to its liability arising from a failure to comply with other obligations under the law, the IdM service provider shall be liable for damage caused to any person due to intentional or negligent failure to comply with its obligations under [this instrument].

2. Paragraph 1 shall be applied in accordance with rules on liability under the law.

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

---

[29] *Designation of reliable IdM systems*: Article 11 establishes a mechanism for the ex ante determination of reliable IdM systems. It has been revised to reflect the decisions of the Working Group at its sixtieth session (A/CN.9/1045, paras. 125–126 and 129).

[30] *"Systems" versus "services"*: As agreed by the Working Group at its sixtieth session, reference to "service" (in the singular) has been inserted beside the word "system" since IdM service providers offer IdM services, and not IdM systems, to their subscribers. However, it was noted that the notion of IdM system encompassed that of IdM service, and that designation should involve the broader notion (A/CN.9/1045, para. 126). The Working Group may wish to clarify whether reference should be made to "IdM services" (in the plural), noting that that is the defined term in article 1(f).

[31] *Notification of designated IdM systems*: At its sixtieth session, the Working Group agreed to place the words "otherwise inform the public" in square brackets for further consideration. They aim to capture means of informing the public other than the publication of lists. At the sixtieth session of the Working Group, 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). If the words are retained, the Working Group may wish to consider inserting them in article 23(2)(b).

[32] *Liability of IdM service providers*: Article 12 has been revised to mirror the options presented in article 24 (A/CN.9/1045, para. 131).

[33] See footnote 53.

[34] See footnote 54.

(b) The IdM service provider has notified the subscriber of those limitations in accordance with the law.

Chapter III. Trust services

Article 13. Legal recognition of trust services[35]

The result deriving from the use of a trust service shall not be denied legal effect, validity or enforceability, or admissibility as evidence on the sole ground that:

(a) It is in electronic form; or

(b) It is not supported by a trust service designated pursuant to article 23.

Article 14. Obligations of trust service providers

1. A trust service provider shall:[36]

(a) Act in accordance with representations made by it with respect to its policies and practices;

(b) Make those policies and practice easily accessible to subscribers and third parties; and

(c) Provide and make publicly available the means that the subscriber should use to satisfy the obligation to notify security breaches under article 15.[37]

2. If a breach of security or loss of integrity occurs that has a significant impact[38] on a trust service, the trust service provider shall:[39]

(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.

---

[35] *Legal recognition of trust services – general*: Article 13 has been revised to reflect the decisions of the Working Group at its sixtieth session (A/CN.9/1045, para. 16).

[36] *Obligations of trust service providers – compliance with policies and practices*: Article 14(1) has been revised to reflect the decisions of the Working Group at its sixtieth session (A/CN.9/1045, paras. 18 and 21).

[37] *Obligations of trust service providers – obligation to make available means to give notice*: The Working Group may wish to consider whether the nature of the obligation in article 14(1)(c) should be the same as the obligation in article 6(d) and, if so, whether the wording of the two obligations should be aligned.

[38] At its sixtieth session, the Working Group was invited to provide guidance on the meaning of "significant impact". In that regard, the Working Group may wish to note that article 19(2) of the eIDAS Regulation (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) requires trust service providers to notify "any breach of security or loss of integrity that has a significant impact on the trust service provided". Several factors may contribute to the assessment of the impact. Dedicated eIDAS Regulation breach notification forms assist in assessing the impact by clarifying its duration, the type of data and the percentage of subscribers affected, and other relevant information. Technical guidelines for incident reporting under article 19 of eIDAS, as well as an annual report on such security incidents, are available from the European Union Agency for Cybersecurity.

[39] The prevailing view at the sixtieth session of the Working Group was that article 14(2) established a minimum standard of mandatory application and therefore that there was no room left for contractual deviation (A/CN.9/1045, para. 19). See also footnote 19.

Article 15. Obligations of subscribers[40]

A subscriber[41] shall notify the trust service provider if:

(a) The subscriber knows that the trust service has been compromised in a manner that affects the reliability of the trust service; 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[42]

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

(a) Identify the person; and

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

2. A method is presumed to be reliable for the purposes of paragraph 1 if an electronic signature designated pursuant to article 23 is used.

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

(a) To establish in any other way, for the purpose of paragraph 1, the reliability of a method pursuant to article 22; or

(b) To adduce evidence of the non-reliability of a designated electronic signature.

Article 17. Electronic seals

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

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

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

2. A method is presumed to be reliable for the purposes of paragraph 1 if an electronic seal designated pursuant to article 23 is used.

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

(a) To establish in any other way, for the purpose of paragraph 1, the reliability of a method pursuant to article 22; or

(b) To adduce evidence of the non-reliability of a designated electronic seal.

Article 18. Electronic timestamps

1. Where a rule of law requires or permits certain documents, records, information or data 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

---

[40] *Obligations of subscribers – general*: The Working Group may wish to consider revising article 15 to align with article 8, noting the proposal in footnote 37.

[41] *Obligations of subscribers – definition of "subscriber"*: At its fifty-ninth session, the Working Group agreed that the instrument should not impose obligations on relying parties (A/CN.9/1005, paras. 38 to 40 and 95 to 96). As noted in footnote 7, it was explained at the sixtieth session that the signatory of an electronic signature would fall within the definition of "subscriber" (A/CN/9/1045, para. 22).

[42] *Electronic signatures*: At its sixtieth session, the Working Group agreed to retain the text of article 16 as contained in the previous draft for further consideration (A/CN.9/1045, para. 34).

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

2. A method is presumed to be reliable for the purposes of paragraph 1 if an electronic timestamp designated pursuant to article 23 is used.

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

(a) To establish in any other way, for the purpose of paragraph 1, the reliability of a method pursuant to article 22; or

(b) To adduce evidence of the non-reliability of a designated electronic timestamp.

Article 19. Electronic archiving[43]

1. Where a rule of law requires or permits certain documents, records or information to be retained, that rule is satisfied in relation to the archiving of a data message if:

(a) The information contained in the data message is accessible so as to be usable for subsequent reference; and

(b) A reliable method is used to:

(i) Indicate the time and date of archiving and associate that time and date with the data message; and

(ii) 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;

(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.

2. A method is presumed to be reliable for the purposes of paragraph 1(b) if an electronic archiving [service] designated pursuant to article 23 is used.

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

(a) To establish in any other way, for the purpose of paragraph 1, the reliability of a method pursuant to article 22; or

(b) To adduce evidence of the non-reliability of a designated electronic archiving service.

Article 20. Electronic registered delivery [services][44]

1. Where a rule of law requires or permits certain documents, records or information to be delivered by registered mail or similar service, that rule is satisfied in relation to a data message if a reliable method is used:

(a) To indicate the time and date at which the data message was received for delivery;

(b) To indicate the time and date at which the data message was delivered;

(c) To assure the integrity of the data message; and

[43] *Electronic archiving*: Article 19 has been revised to reflect the decisions of the Working Group at its sixtieth session (A/CN.9/1045, para. 39). Among other things, the Working Group agreed that the term "data message" included data that was not sent or received (A/CN.9/1045, para. 41).

[44] *Electronic delivery - functions*: Article 20 has been revised to reflect the decisions of the Working Group at its sixtieth session to expressly require the electronic delivery service to assure the integrity of the data message and identify the sender and the recipient (A/CN.9/1045, para. 44).

(d) To identify the sender and the recipient.

2. A method is presumed to be reliable for the purposes of paragraph 1 if an electronic registered delivery [service] designated pursuant to article 23 is used.

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

(a) To establish in any other way, for the purpose of paragraph 1, the reliability of a method pursuant to article 22; or

(b) To adduce evidence of the non-reliability of a designated electronic registered delivery service.

Article 21. Website authentication[45]

1. Where a rule of law requires or permits the authentication of a website, that rule is satisfied if a reliable method is used to identify the person who holds the domain name[46] for the website and to link that person to the website.[47]

2. A method is presumed to be reliable for the purposes of paragraph 1 if a website authentication designated pursuant to article 23 is used.

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

(a) To establish in any other way, for the purposes of paragraph 1, the reliability of a method pursuant to article 22; or

(b) To adduce evidence of the non-reliability of a designated website authentication.

Article 22. Requirements for determining reliability for trust services[48]

1. In determining the reliability of the method for the purposes of articles 16 to 21, all relevant circumstances shall be taken into account, which may include:

(a) Any operational rules, policies and practices of the trust service provider, including any plan for the termination of activity in order to ensure continuity;

(b) 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;

---

[45] *Website authentication – general*: Article 21 has been revised to reflect the decisions of the Working Group at its sixtieth session (A/CN.9/1045, para. 48).

[46] *Website authentication – person who holds the domain name*: The term "person who holds the domain name" is used to cover persons who have been assigned or licensed to use the domain name by a domain name registrar. In its discussions so far, the Working Group has focused on circumstances where a party (e.g., the website owner) agrees to authenticate a website, rather than where it does so to satisfy a rule of law that "requires" such authentication. In these circumstances, the party would be acting pursuant to a rule of law that "permits" such authentication.

[47] *Website authentication – functions*: At its fifty-ninth session, the Working Group agreed that the essential function of website authentication is to link the website to the person to whom the domain name has been assigned or licensed (A/CN.9/1005, para. 66). At the Working Group's sixtieth session, it was indicated that website authentication comprised two elements: identification of the domain name holder and linking that person with the website. Hence, the object of the trust service was the trustworthiness of the website and not the identity of the owner. It was emphasized that website authentication aimed to identify persons, not objects (A/CN.9/1045, para. 47). At that session, it was also indicated that any discussion on objects in the framework of the draft instrument should be limited to their traceability to a person (ibid., para. 49). Article 21 is the only provision dealing with objects.

[48] *Requirements for determining reliability*: Article 22 (article 23 of the previous draft) has been revised to reflect the decisions of the Working Group at its sixtieth session (A/CN.9/1045, paras. 56–57 and 61). The reliability level of the method used may vary in light of the function pursued with that method.

(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 for which the trust service is being used;[49] 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.

2. A method is deemed reliable if it is proven in fact to have fulfilled the functions to which the relevant trust service relates.

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

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

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

Article 23. Designation of reliable trust services[50]

1. [*A person, organ or authority, whether public or private, specified by the enacting jurisdiction as competent*] may designate trust services that are reliable for the purposes of articles 16 to 21.

[1 *bis*. A method is presumed to be reliable for the purposes of articles 16 to 21, if a trust service designated pursuant to paragraph 1 is used.

1 *ter*. Paragraph 2 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 designated trust service.][51]

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

(a) Take into account all relevant circumstances, including the factors listed in article 22, in designating a trust service; and

(b) Publish a list of designated trust services, including details of the trust service provider.

3. Any designation made under 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

---

[49] 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(1)(d).

[50] *Designation of reliable trust services – general*: Article 23 (article 24 of the previous draft) has been revised to reflect the decisions of the Working Group at its sixtieth session (A/CN.9/1045, para. 61). It establishes a mechanism for the ex ante determination of reliable trust services. It was explained during discussions at the Working Group's fifty-ninth session that the designation did not pertain to generic types of trust service or to all the trust services offered by a specific trust service provider, but rather to a specific trust service provided by an identified service provider (A/CN.9/1005, para. 69).

[51] *Designation of reliable trust services – effects*: The Working Group may wish to consider whether paragraphs 1 *bis* and 1 *ter* should be inserted in article 23 and therefore that the corresponding paragraphs 2 and 3 of articles 16, 17, 18, 19, 20 and 21 should be deleted. Similarly, the Working Group may wish to consider whether paragraphs 2 and 3 of article 9 should be moved to article 11.

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

Article 24. Liability of trust service providers[52]

Option A[53]

[The liability of trust service providers shall be determined according to the law.]

Option B[54]

1. Without prejudice to its liability arising from a failure to comply with other obligations under the law, the trust service provider shall be liable for damage caused to any person due to intentional or negligent failure to comply with its obligations under [this instrument].

2. Paragraph 1 shall be applied in accordance with rules on liability under the law.

3. Notwithstanding paragraph 1, the trust service provider shall not be liable to the subscriber 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 notified the subscriber of those limitations in accordance with the law.

Chapter IV. International aspects

Article 25. Cross-border recognition of IdM [systems][services] and trust services

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

2. In determining whether [identity credentials] [an IdM system] [IdM services] or a trust service offers [a substantially equivalent] [the same] level of reliability, regard shall be had to [recognized international standards].[55]

---

[52] *Liability of trust service providers*: At the fifty-ninth session of the Working Group, general support was expressed for retaining a provision on liability so as to provide legal certainty. At its sixtieth session, the Working Group considered several options put forward by the Secretariat. Article 24 has been revised to reflect the decisions of the Working Group at that session (A/CN.9/1045, para. 66).

[53] Option A adopts a minimalist approach by acknowledging that the liability of the trust service provider, including any limitation thereof, is to be determined according to applicable law outside the instrument. The Working Group may wish to consider whether this provision should be retained if the draft instrument takes the form of a model law or whether it would be superfluous given that its legal effect would occur on the basis of general legal principles.

[54] Option B adopts an approach similar to that used in article 13 of the eIDAS Regulation. Paragraph 1 sets forth a general principle of liability for wilful or negligent failure to comply with any of the obligations arising under the instrument. The envisaged standard of negligence is ordinary, i.e. neither slight nor gross. Slight and gross negligence are legal notions whose content may differ in the various legal systems and that may not exist in all legal systems. Paragraph 2 refers to domestic law for related matters such as the elements constituting negligence, burden of proof and other evidentiary issues, and matters such as contributory negligence and vicarious liability. Paragraph 3 establishes the conditions for limiting liability.

[55] *Cross-border recognition – level of equivalence*: At the fifty-ninth session of the Working Group, different views were expressed on the level of equivalence required for cross-border legal effect (A/CN.9/1005, para. 120). The present draft mirrors article 12(2) MLES, which requires "substantial" equivalence. An alternative presented in the previous draft was for exact equivalence (i.e., the foreign service must offer the "same" level of reliability). Those deliberations were continued at the sixtieth session (A/CN.9/1045, para. 69).

[3. Equivalence shall be presumed if a person, organ or authority designated by [*the enacting jurisdiction*] according to article 11 and 23 has determined the equivalence for the purposes of this paragraph.][56]

Article 26. Cooperation

[*A person, organ or authority, whether public or private, specified by the enacting State 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.

[56] *Cross-border recognition – presumption of equivalence*: Paragraph 3 aims to link article 25 with articles 11 and 23 (see A/CN.9/1045, para. 71), in particular with respect to ex ante designation. The Working Group may wish to discuss the instances in which a designating authority would avail itself of paragraph 3 instead of designating the foreign IdM system or trust service, particularly in view of articles 11(4) and 23(4). In addition, the Working Group may wish to consider whether a new provision should be added to article 25 to empower the designating authority to determine that an IdM system or trust service designated by a foreign authority will be treated in the enacting jurisdiction as an IdM system or trust service designated under articles 11(1) and 23(1), respectively.