United Nations A/CN.9/WG.IV/WP.162

General Assembly

Distr.: Limited
28 January 2020

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Sixtieth session
New York, 6–9 April 2020

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

Note by the Secretariat

Contents

V.20-00755 (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 fifty-ninth session (Vienna, 25–29 November 2019), as reported in A/CN.9/1005. In the footnotes accompanying the present draft, the draft provisions considered by the Working Group at its fifty-ninth session, as set out in document A/CN.9/WG.IV/WP.160, are referred to as the "previous draft".

2. The Working Group may wish to note that the current draft contains changes in terminology to address concerns regarding potential different understandings. In particular, the term "authentication" has been replaced with "electronic identification" and the process previously referred to as "identification" is now referred to as "identity proofing" (art. 1). Accordingly, the IdM process is now made of two stages (or phases), "identity proofing" and "electronic identification". The term "authentication" is now used exclusively in the context of trust services (arts. 21 and 22).

3. Background information on the current work of Working Group IV is available in document A/CN.9/WG.IV/WP.161, paragraphs 6–18.

Annex

Draft Provisions[1] on the Use and Cross-border Recognition of IdM and Trust Services

Chapter I. General provisions

Article 1. Definitions

For the purposes of this [instrument]:

(a) "Attribute" means an item of information or data associated with a [subject][person];[2]

(b) "Authentication", in the context of trust services, means a process used to attribute an identifier to an object;[3]

(c) "Data message" means information generated, sent, received or stored by electronic, magnetic, optical or similar means;[4]

[1] *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 taking 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.

[2] *Definitions – "attribute"*: This definition is drawn from document A/CN.9/WG.IV/WP.150, paragraph 13. The term is used in the definitions of "identity proofing" and "identity" as well as in articles 6 and 7.
For the use of "subject" and "person", depending on the outcome of the Working Group's consideration of the definition of "subject", see footnote 14.

[3] *Definition – "authentication"*: A new definition of "authentication" has been inserted to refer to the process of using trust services to confirm the identity of objects. The Working Group may wish to consider the definition jointly with the proposals to introduce a general provision on authentication of objects (art. 22) and to exclude objects from the scope of IdM provisions (art. 1(k), definition of "subjects").

[4] *Definitions – "data message"*: This definition is drawn from existing UNCITRAL texts on electronic commerce, notably the UNCITRAL Model Law on Electronic Commerce (MLEC) (United Nations publication, Sales No. E.99.V.4) and the United Nations Convention of the Use of Electronic Communications in International Contracts (ECC) (United Nations, *Treaty Series*, vol. 2898, No. 50525, p. 3). The term is used to define the requirements of the various trust services set out in chapter III. As clarified in the definition of "trust services", it is the particular qualities of a data message that are the focus of each trust service.

(d) "Electronic identification", in the context of IdM services, means a process used to achieve sufficient assurance in the binding between a [subject][person] and an identity;[5,6,7]

(e) "Identity" means a set of attributes that allows a [subject][person] to be uniquely distinguished within a particular context;[8]

(f) "Identity credentials" means the data, or the physical object upon which the data may reside, that a [subject][person] may present for the electronic identification of its identity in electronic form;[9]

[5] *Definitions – "electronic identification"*: As noted in paragraph 2 above, the present draft uses the term "electronic identification" instead of "authentication" to address the concerns on the multiple meanings of "authentication". At the fifty-ninth session of the Working Group, several questions were raised about the meaning of the term "authentication", and whether it had the same meaning in the various contexts it was used (A/CN.9/1005, paras. 13, 84–85, 92). The Working Group asked the Secretariat to ensure the consistent use of terminology throughout the document, as well as with terminology adopted by the International Telecommunications Union (ITU) (see A/CN.9/1005, para. 86).
The definition of "electronic identification" is drawn from the definition of "authentication" in document A/CN.9/WG.IV/WP.150, paragraph 15, which in turn is taken from Recommendation ITU-T X.1252 of ITU. The term "assurance" is used in the definition instead of "confidence" on the basis that: (a) the term "assurance" is used in the present draft; and (b) Recommendation ITU-T X.1252 equates "assurance" and "confidence" in the context of authentication, as demonstrated in the definition of "assurance level" as the "level of confidence in the binding between an entity and the presented identity information".
In the present draft, the notion of "electronic identification" so defined is used in the context of IdM in the definitions of "identity credentials", "IdM services", "IdM system", as well as in articles 5, 6, 8 and 9.
In the draft instrument, the term "authentication" refers to the use of trust services to identify objects, in line with the title of the trust service "website authentication".

[6] *Definitions – "electronic identification factors"*: The Working Group may wish to consider whether the following definition should be inserted in the draft instrument: "'Electronic identification factors', in the context of IdM services, means the items of information or processes used to electronically identify the identity of a subject". In doing so, the Working Group may wish to bear in mind the definitions of "electronic identification" and of "identity credentials". The definition is based on that contained in document A/CN.9/WG.IV/WP.150, para. 17. The term "electronic identification factors" is used only in article 6.

[7] *Definitions – "electronic identification mechanisms"*: The Working Group may wish to consider whether the following definition should be inserted in the draft instrument: "'Electronic identifications mechanisms', in the context of IdM services, means the mechanisms by which subjects use identity credentials to identify themselves". The definition is drawn from article 8(3)(c) of the Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ("eIDAS Regulation"). In doing so, the Working Group may wish to bear in mind the definitions of "electronic identification" and of "identity credentials". The term "electronic identification mechanisms" is used only in article 6.

[8] *Definitions – "identity"*: This definition is drawn from document A/CN.9/WG.IV/WP.150, paragraph 31. At the fifty-ninth session of the Working Group, there was general agreement that a requirement of "uniqueness" should be included in the definition (see A/CN.9/1005, para. 108).

[9] *Definitions – "identity credentials"*: This definition is drawn from document A/CN.9/WG.IV/WP.150, paragraph 21. The term is broadly synonymous with "electronic identification means" as defined in article 3(2) of the eIDAS Regulation. The definition includes elements from the definition in § 59.1-550 of the Electronic Identity Management Act of Virginia (Title 59.1 Chapter 50 of the Virginia Code). At the fifty-ninth session of the Working Group, it was noted that electronic identity credentials could be used offline, and it was thus suggested that the definition refer instead to identity credentials "in electronic form" (rather than "in an online context"). The Working Group agreed to amend the definition accordingly (A/CN.9/1005, para. 110).

(g) "Identity management (IdM) services" means services consisting of managing identity proofing or electronic identification of [subjects][persons] in electronic form;[10]

(h) "Identity management (IdM) service provider" means a person that provides IdM services;[11]

(i) "Identity management (IdM) system" means a set of functions and capabilities to manage the identity proofing and electronic identification of [subjects][persons] in electronic form;[12]

(j) "Identity proofing" means the process of collecting, verifying, and validating sufficient attributes to define and confirm the identity of a [subject][person] within a particular context;[13]

(k) "Subject" means a person [or an object];[14]

[10] *Definitions – "IdM services"*: This definition is drawn from document A/CN.9/WG.IV/WP.150, paragraph 35, option (a). The definition reflects the understanding that IdM comprises two stages (or phases): "identity proofing" and "electronic identification" (previously referred to as "identification" and "authentication": A/CN.9/1005, para. 84). Some concern has previously been expressed about defining IdM by referring to these stages cumulatively (A/CN.9/965, para. 91). Bearing this concern in mind, the definition refers to "identity proofing *or* electronic identification", noting that the term "or" is not disjunctive (A/CN.9/1005, para. 109). The reference to "electronic form" follows the agreement of the Working Group regarding the definition of "identity credentials" (see footnote 9). The term "identification" has been replaced with the term "identity proofing" to reflect the terminological change (see footnote 13).

[11] *Definitions – "IdM service provider"*: This definition reflects the agreement of the Working Group at its fifty-ninth session (A/CN.9/1005, para. 111).

[12] *Definitions – "IdM system"*: At the fifty-ninth session of the Working Group, it was suggested that, as the draft referred to "IdM services", it was not necessary to refer to "IdM systems". However, it was pointed out that, in several provisions of the draft instrument, it was more appropriate to refer to "IdM systems", including article 5 on non-discrimination (A/CN.9/1005, paras. 86 and 112) and article 11 on the ex ante determination of reliability (A/CN.9/1005, para. 102). Accordingly, the Working Group decided to retain a definition of IdM system (A/CN.9/1005, para. 112). The current definition of the term reflects the agreement of the Working Group to refer to "functions and capabilities", consistent with ITU terminology. In this regard, Recommendation ITU-T X.1252 defines identity management as a "set of functions and capabilities" that is used for (i) assurance of identity information; (ii) assurance of the identity of an entity; and (iii) supporting business and security applications.

[13] *Definitions – "identity proofing"*: As noted in paragraph 2 above, the present draft uses the term "identity proofing" instead of "identification" to address the concerns on the multiple meanings of "identification" (cf. A/CN.9/WG.IV/WP.150, para. 29).
At the fifty-ninth session of the Working Group, it was pointed out that the definition of "identification" included the enrolment stage (or phase) of IdM but excluded the authentication stage (or phase), which is referred to electronic identification stage (or phase) in the present draft (A/CN.9/1005, para. 84). "Enrolment" may be defined as "the process by which IdM service providers verify the identity claims of a subject before issuing a credential to such subject" (A/CN.9/WG.IV/WP.150, para. 26).
The term "identification" is used in a non-technical sense in article 9.

[14] *Definitions – "subject"*: The use of the terms "subject" and "person" has been revised for consistency throughout the draft provisions. The term "subject" is only used in the context of IdM. The words "or an object" may be deleted if the Working Group agrees to limit IdM provisions to physical and legal persons. In that case, the Working Group may wish to consider deleting the definition of "subject" and replacing the term "subject" with "person" throughout the draft instrument.

(l) "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;[15]

(m) "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;[16]

(n) "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.[17,18]

2. Nothing in this [instrument] requires:

(a) The identification of a person;[19]

(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 [subject][person] be identified in accordance with a procedure defined or prescribed by law.

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 law applicable to privacy and data protection.[20]

---

[15] *Definitions – "subscriber"*: The term "subscriber" is used in articles 8 and 15, which impose obligations on subscribers in the event of a security breach or compromise of services. At the fifty-ninth session of the Working Group, it was noted that the term "user" was unclear as it could refer to both: (a) the person to whom services are provided (e.g., the person being identified), and with whom the service provider was in a contractual relationship, and (b) the relying party, with whom the service provider was not in a contractual relationship (see A/CN.9/1005, paras. 28, 39 and 95). 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).

[16] *Definitions – "trust services"*: The term "trust services" is drawn from the eIDAS Regulation, where it is defined as "an electronic service normally provided for remuneration" consisting of one of the various services described in chapter III of the regulation. As such, the eIDAS Regulation does not set out a stand-alone definition of "trust services". The previous draft attempted to establish such a definition in terms of "an electronic service that provides a certain level of reliability in the qualities of data". At the fifty-ninth session of the Working Group, it was indicated that such a definition did not provide adequate guidance and that the approach in the eIDAS Regulation should be adopted. At the same time, it was noted that a more "abstract" definition could better accommodate future developments. It was also noted that trust services were more concerned with the veracity and genuineness of data rather than its reliability. The current definition reflects the decision of the Working Group to include a non-exhaustive list of trust services (A/CN.9/1005, para. 18).

[17] *Scope of application – domestic and cross-border use of IdM and trust services*: At its fifty-second session, the Commission noted that the Working Group should work towards an instrument that could apply to both domestic and cross-border use of IdM and trust services (A/74/17, para. 172).

[18] *Scope of application – trade-related services*: At its fifty-ninth session, the Working Group agreed that the term "trade-related services" was sufficient to capture transactions with certain public authorities involved in trade, such as customs operating a single window, and therefore that it was not necessary to qualify the term with the word "government" (A/CN.9/1005, para. 115).

[19] The Working Group may wish to consider the relationship between this provision and article 3(1).

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

Article 3. Voluntary use of IdM and trust services[21]

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.[22]

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.[23]

Chapter II. Identity management

Article 5. Legal recognition of IdM[24]

The electronic identification of a [subject][person][25] 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;[26] or

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

---

[21] *Voluntary use of IdM and trust services*: Article 3 is based on article 8(2) ECC. The drafting has been revised to reflect the decisions of the Working Group at its fifty-ninth session (see A/CN.9/1005, para. 116). In its present form, the provision prevents the imposition of any new obligation not only on the subscriber, but also on the service provider and the relying party. The principle of voluntary use was previously considered by the Working Group at its fifty-seventh session (A/CN.9/965, para. 110), where a link was drawn with the principle of party autonomy.

[22] *Uniform interpretation*: UNCITRAL texts commonly contain a provision establishing an obligation of uniform interpretation. At its fifty-ninth session, the Working Group agreed to specify that the reference to good faith is to good faith "in international trade" (A/CN.9/1005, para. 118). In its present form, article 4(1) mirrors article 5(1) ECC.

[23] *General principles*: At its fifty-ninth session, the Working Group agreed not to list some of the general principles on which the instrument is based, namely the principles of non-discrimination against the use of electronic means, technology neutrality, and functional equivalence (A/CN.9/1005, para. 118). In its present form, article 4(2) mirrors article 5(2) ECC.

[24] *Legal recognition of IdM – general*: Article 5(1) is based on similar provisions in existing UNCITRAL texts on electronic commerce, such as article 5 MLEC, article 8(1) ECC and article 7(1) of the UNCITRAL Model Law on Electronic Transferable Records (MLETR) (United Nations publication, Sales No. E.17.V.5). It legally enables the use of IdM and applies regardless of whether an offline equivalent exists (cf. article 9). The reference to "admissibility as evidence" is drawn from article 9 MLEC. Paragraph 1(b) extends the non-discrimination provision to discrimination between ex ante and ex post determinations of reliability. Paragraph 1(b) only deals with the *denial* of legal effect for the use of a non-designated IdM system, and thus does not affect article 9(2), which provides *greater* legal effect to the ex ante determination of reliability in the form of a rebuttable presumption of reliability.

[25] *Legal recognition of IdM – non-discrimination*: At its fifty-ninth session, the Working Group agreed that the goal of non-discrimination as identified in the chapeau of article 5(1) (i.e., the thing being protected by the non-discrimination provision) should be "the verification of identity" (A/CN.9/1005, para. 86) and that, in this context, "verification" was synonymous with "authentication" (A/CN.9/1005, para. 85). In light of the approach described in paragraph 2, the term "electronic identification" is now used.

[26] *Legal recognition of IdM – prohibited grounds*: At its fifty-ninth session, the Working Group agreed that the prohibited grounds for discrimination as set out in paragraph 1(a) should be that the "identification and verification" are in electronic form (see A/CN.9/1005, para. 86). In light of the approach described in paragraph 2, and consistent with the definition of "IdM services" in article 1, the terms "identity proofing" and "electronic identification" are now used.

Article 6. Obligations of IdM service providers[27]

An IdM service provider shall [at a minimum]:

(a) Enrol [subjects][persons], including by:

(i) Registering and collecting attributes, as appropriate for the IdM service;

(ii) Carrying out identity proofing and verification; and

(iii) Binding the identity credentials to the [subject][person];

(b) Update attributes;

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

(i) Issuing, delivering and activating credentials;

(ii) Suspending, revoking and reactivating credentials; and

(iii) Renewing and replacing credentials;

(d) Manage the electronic identification of [subjects][persons], including by:

(i) Managing electronic identification factors; and

(ii) Managing electronic identification mechanisms;

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

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

Article 7. Obligations of IdM service providers in case of data breach[28]

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;

(c) Notify the breach or loss in accordance with applicable law.

2. If a [subject][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.

[27] *Obligations of IdM service providers*: The obligations in article 6 were developed in consultation with experts following a request by the Working Group at its fifty-eighth session (A/CN.9/971, para. 67). The provision has been revised to reflect the decision of the Working Group at its fifty-ninth session to amend subparagraph (a)(i) to give effect to the principle of data minimization (A/CN.9/1005, para. 93).

[28] *Obligations of IdM service providers in case of data breach*: Article 7 has been revised to reflect the decisions of the Working Group at its fifty-ninth session (A/CN.9/1005, para. 94 and paras. 32 to 36). In particular, the Working Group has agreed that the obligations of IdM service providers in the case of a data breach should be formulated along the lines of the obligations of trust service providers in the case of a data breach, which are set out in article 14(2). For further discussion on the scope of those obligations, see footnotes 43 and 44.

Article 8. Obligations of subscribers[29]

The subscriber shall notify the IdM service provider if:

(a) The subscriber knows that the identity credentials or electronic identification mechanisms of the relevant IdM system have been compromised; or

(b) The circumstances known to the subscriber give rise to a substantial risk that the identity credentials or electronic identification mechanisms may have been compromised.

Article 9. Identification of a [subject][person] using IdM[30]

Option A

1. Where a rule of law requires or permits the identification of a [subject][person], that rule is satisfied with respect to IdM if a reliable method is used for the electronic identification of the [subject][person].[31]

Option B

1. A subject may be identified by using IdM services if a reliable method is used for the electronic identification of the [subject][person].[32]

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.[33]

[29] *Obligations of subscribers*: Article 8 has been revised to reflect the decisions of the Working Group at its fifty-ninth session (A/CN.9/1005, para. 96 and paras. 37 to 43). In particular, the Working Group has agreed that the obligations of IdM service subscribers should align with the obligations of trust service subscribers, which are set out in article 14. For further discussion on the scope of those obligations, see footnotes 45 and 46.

[30] *Legal recognition of IdM – general*: This provision aims to provide legal recognition with respect to the use of IdM for identification purposes. Two options are submitted to the Working Group for consideration.
Option A of article 9 has been revised to reflect the decisions of the Working Group at its fifty-ninth session (A/CN.9/1005, paras. 98, 99 and 101). At that session, it was noted that article 9 would ordinarily find application where the parties had agreed to use an IdM service to identify one another (A/CN.9/1005, para. 97). By virtue of article 2(2)(b), article 9 does not supersede any legal requirement under applicable law that a subject be identified in accordance with a defined or prescribed procedure.

[31] *Legal recognition of IdM – offline equivalent*: Option A of article 9 retains the functional equivalence approach of earlier drafts. It has previously been noted that a provision based on functional equivalence requires an offline equivalent to be identified (A/CN.9/965, para. 66). At its fifty-ninth session, the Working Group agreed that the offline equivalent was the "identification of a subject", which is reflected in the title of the article.

[32] *Legal recognition of IdM*: Option B of article 9 aims to assert the legality of using electronic identification without applying a functional equivalence approach. The Working Group may wish to bear in mind article 5 when considering this option.

[33] *Presumption of reliability*: At its fifty-ninth session, the Working Group agreed that article 9 should be recast along the lines of the equivalent provisions setting out the requirements of trust services (i.e., arts. 16 to 22) (A/CN.9/1005, para. 99). Accordingly, paragraphs 2 and 3 have been inserted, which are based on paragraphs 2 and 3 of article 16 and effectively replace paragraphs 4 and 5 of article 11 of the previous draft.

Article 10. Factors relevant to determining reliability

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:

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

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

(i) Governance;

(ii) Published notices and user information;

(iii) Information security management;

(iv) Record-keeping;

(v) Facilities and staff;

(vi) Technical controls; and

(vii) Oversight and audit;

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

(d) Any agreement between the parties.

2. In determining the reliability of the method, 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.

Article 11. Designation of reliable IdM systems[34]

1. [*A person, organ or authority, whether public or private, specified by the enacting State as competent*] may designate IdM systems 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; and

(b) Publish a list of designated IdM systems, including details of the IdM service provider.

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

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

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

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

[34] *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 fifty-ninth session (A/CN.9/1005, para. 102) and has therefore been reformulated along the lines of the corresponding provision of chapter II that deals with the ex ante determination of reliable trust services (article 24). For further discussion of the various elements of this provision, see footnotes 63 and 64.

Article 12. Liability of IdM service provider[35]

Option A

[The liability of IdM service providers shall be determined according to applicable law.][36]

Option B

An IdM service provider shall bear the legal consequences for its failure to comply with its obligations under [this instrument].

Option C

1. The IdM service provider shall be liable for damage caused to any person due to intentional or negligent failure to comply with its obligations under [this instrument].[37]

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

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

Chapter III. Trust services[38]

Article 13. Legal recognition of trust services[39]

[The qualities of a data message assured][40] [Data that is exchanged, verified or authenticated] by use of, or with support of, a trust service shall not be denied legal effect, validity or enforceability, or admissibility as evidence[41] 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 24.

---

[35] *Liability of IdM service providers*: At its fifty-ninth session, the Working Group decided not to include a safe harbour provision that excluded the liability of IdM service providers under certain conditions (A/CN.9/1005, para. 104). For the rest, the Working Group agreed to reconsider the liability of IdM service providers in conjunction with the liability of trust service providers (A/CN.9/1005, para. 106). Accordingly, article 12 has been revised to mirror the options presented in article 25. Three options are submitted to the Working Group for consideration.

[36] The Working Group may wish to consider whether this provision should be retained in case the draft instrument had 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.

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

[38] The chapter on trust services features a general provision on legal recognition of trust services (art. 13); a general reliability standard with a non-geographic discrimination clause to facilitate cross-border recognition (art. 23); a mechanism for ex ante designation of reliable trust services (art. 24), a provision on liability (art. 25) and a list of trust services (arts. 16–22).

[39] *Legal recognition of trust services – general*: Article 13 has been revised to reflect the decisions of the Working Group at its fifty-ninth session (A/CN.9/1005, para. 26).

[40] The alternative wording “The qualities of a data message assured” is suggested to closer align article 13 with the definition of “trust services”.

[41] It is suggested to insert the words “or admissibility as evidence” to align this provision with article 5.

Article 14. Obligations of trust service providers

1. A trust service provider shall:[42]

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

(b) Make those policies and practice easily accessible to subscribers.

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:

(a) Take all reasonable steps to contain the breach or loss, including, where appropriate, suspending or revoking the affected service;[43]

(b) Remedy the breach or loss; and

(c) Notify the breach or loss in accordance with applicable law.[44]

Article 15. Obligations of subscribers

A subscriber[45] 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;[46] or

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

---

[42] *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 fifty-ninth session (A/CN.9/1005, paras. 31 and 73). With regard to paragraph 1(b), the Working Group agreed on the following text: "[t]hese policies and practices shall be made easily accessible to subscribers", which has been recast in the present draft to clarify that this is an obligation imposed on the service provider. The Working Group may wish to consider whether the obligation should be aligned with the obligation on IdM service providers in article 6(f) to "[p]rovide reasonable access to the rules governing the IdM system".

[43] *Obligations of trust service providers – containment of security breach*: Article 14(2)(a) of the previous draft imposed an obligation to suspend trust services affected by a security breach, with an optional endpoint measured by reference either to the breach being "contained" or to new certificate or equivalent being issued (see also A/CN.9/WG.IV/WP.154, para. 47). Acknowledging that measures other than full suspension might be appropriate, the Working Group agreed at its fifty-ninth session that the trust service provider should instead be obliged to "take all reasonable steps" (A/CN.9/1005, para. 33). Article 14(2)(a) of the present draft reflects this agreement and specifies that the steps must be directed to containing the breach. The Working Group may wish to consider whether reference to "containing" the breach reflects the desired objective of the steps taken by the trust service provider to respond to a security breach.

[44] *Obligations of trust service providers – notification of security breach*: Article 14(3) of the previous draft imposed a notification obligation on the trust service provider, which specified (a) who was to be notified and (b) the timing for such notification. At its fifty-ninth session, the Working Group agreed that the instrument should defer to applicable law on these matters (A/CN.9/1005, para. 36).

[45] *Obligations of subscribers – general*: 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).

[46] *Obligations of subscribers – trigger*: While the obligation imposed on trust service providers in article 14(2) is triggered by a "breach of security or loss of integrity", the obligation imposed on subscribers in article 15 is triggered by the trust service being "compromised". At the fifty-ninth session of the Working Group, it was suggested that article 15 was concerned with the reliability of trust services (A/CN.9/1005, para. 37). The addition of the words "in a manner that affects the reliability of the trust service" in the present draft reflect that suggestion. A similar formulation is found in article 10(1) of the eIDAS Regulation.

Article 16. Electronic signatures

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 24 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 23; or

(b) To adduce evidence of the non-reliability of a designated electronic signature.[47]

Article 17. Electronic seals

1. Where a rule of law requires or permits a legal person[48] 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.[49]

2. A method is presumed to be reliable for the purposes of paragraph 1 if an electronic seal designated pursuant to article 24 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 23; or

(b) To adduce evidence of the non-reliability of a designated electronic seal.[50]

---

[47] *Electronic signatures – presumption of reliability*: At its fifty-ninth session, the Working Group agreed that trust services that are determined to be reliable based on an ex ante approach (i.e., pursuant to art. 24) should enjoy greater legal effect in the form of a rebuttable presumption of reliability (A/CN.9/1005, para. 12). The Working Group also agreed that this presumption should be contained in each provision setting out the requirements of a trust service (i.e., arts. 16 to 22) (A/CN.9/1005, para. 51). Article 16(2) and (3) reflects this agreement and replace articles 24(4) and (5) of the previous draft, respectively. Article 16(3) mirrors article 6(4) of the Model Law on Electronic Signatures (MLES) (United Nations publication, Sales No. E.02.V.8).

[48] *Electronic seals – restriction to legal persons*: At its fifty-ninth session, the Working Group agreed that electronic seals were only created by legal persons, and therefore that article 17 of the previous draft (article 18 of the present draft) should be limited to subscribers that are legal persons (A/CN.9/1005, paras. 52 and 54).

[49] *Electronic seals – function*: At its fifty-ninth session, the Working Group agreed that the function of an electronic seal was to assure the origin and integrity of the data to which it is associated (A/CN.9/1005, paras. 52 and 54). Assurance of origin is provided for in paragraph (a) while assurance of integrity is provided for in paragraph (b). It has been suggested that assurance of origin is functionally the same as identifying the legal person creating the seal (A/CN.9/1005, para. 52), in which case it is conceivable that the origin of the data may be assured through the use of an electronic signature. Allowance in paragraph (b) for "the addition of any endorsement and any change that arises in the normal course of communication, storage and display" reflects the agreement of the Working Group (A/CN.9/1005, paras. 56 to 58).

[50] *Electronic seals – presumption of reliability*: See footnote 47.

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

(b) Associate that time and date with the data message.[51]

2. A method is presumed to be reliable for the purposes of paragraph 1 if an electronic timestamp designated pursuant to article 24 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 23; or

(b) To adduce evidence of the non-reliability of a designated electronic timestamp.[52]

Article 19. Electronic archiving

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[53] 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) 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.[54]

(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.[55]

2. A method is presumed to be reliable for the purposes of paragraph 1(b) if an electronic archiving service designated pursuant to article 24 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 23; or

(b) To adduce evidence of the non-reliability of a designated electronic archiving service.[56]

---

[51] *Electronic timestamps – general*: Article 18 has been revised to reflect the decisions of the Working Group at its fifty-ninth session (A/CN.9/1005, para. 55).

[52] *Electronic timestamps – presumption of reliability*: See footnote 47.

[53] *Electronic archiving services – general*: The previous draft referred to electronic archiving in terms of "retaining data messages". To align with the wording in other trust service provisions and in the balance of paragraph (1), as well as the wording used by the Working Group at its fifty-ninth session (A/CN.9/1005, para. 59), the present draft refers to "the archiving of a data message".

[54] *Electronic archiving services – function*: At its fifty-ninth session, the Working Group agreed that an essential function of electronic archiving was an assurance of data integrity (A/CN.9/1005, para. 59). Consistent with the decision taken by the Working Group, paragraph (b)(ii) has been reformulated to reflect the criteria for assessing integrity as set out in article 17(1)(b).

[55] This condition does not extend to information the sole purpose of which is to enable the message to be sent or received: see article 10(2) MLEC.

[56] *Electronic archiving services – presumption of reliability*: See footnote 47.

Article 20. Electronic registered delivery services

1. Where a rule of law requires or permits certain documents, records or information to be delivered by registered mail or similar service,[57] 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; and

(b) To indicate the time and date at which the data message was delivered.[58]

2. A method is presumed to be reliable for the purposes of paragraph 1 if an electronic registered delivery service designated pursuant to article 24 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 23; or

(b) To adduce evidence of the non-reliability of a designated electronic registered delivery service.[59]

Article 21. Website authentication

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 for the website and to link that person to the website.[60]

Article 22. Object authentication

Where a rule of law requires or permits the authentication of an object, that rule is satisfied if a reliable method is used to authenticate that object.[61]

---

[57] *Electronic registered delivery services – offline equivalent*: The previous draft referred to a rule of law requiring or permitting "proof of dispatch or receipt" of a document etc. At the fifty-ninth session of the Working Group, it was suggested that more appropriate language could be formulated by focusing on the functional equivalence between registered mail services and electronic registered delivery services. Accordingly, the chapeau of article 20(1) has been revised to refer to a rule of law requiring the document etc. "to be delivered by registered mail or similar service".

[58] *Electronic delivery service – function*: At its fifty-ninth session, the Working Group agreed that the essential function of an electronic delivery service was to provide assurance "of the time at which the data message was received for delivery by the electronic registered delivery service and the time at which the data message was delivered by that system to the addressee" (A/CN.9/1005, para. 64). Article 20(1) of the present draft has been reformulated accordingly, although the provision refers to an "indication" of time, consistent with terminology used in article 18(1). The Working Group may wish to consider whether this provision should expressly require the electronic delivery service to assure the integrity of the data message, confirm receipt and delivery, and identify the sender and/or the recipient. Arguably, these functions are already covered in paragraphs (a) and (b).

[59] *Electronic delivery service – presumption of reliability*: See footnote 47.

[60] *Website authentication – function*: 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). In the present draft, the term "domain name holder" 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.

[61] *Object authentication – function*: The Working Group may wish to consider whether article 23 should be inserted to refer to all instances of identification of physical and digital objects. In doing so, the Working Group may wish to consider the suggested definition of "authentication" and the suggested revision of the definition of "subject" so as to exclude objects from the scope of the provisions on IdM.

Article 23. Reliability standard for trust services[62]

1. In determining the reliability of the method for the purposes of articles 16 to 22, all relevant circumstances shall be taken into account, which may include:

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

(b) Any applicable recognized international standards and procedures;

(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; and

(h) Any relevant agreement.

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 24. Designation of reliable trust services[63]

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

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 23, in designating a trust service; and

(b) Publish a list of designated trust services, including details of the trust service provider.[64]

---

[62] *Reliability standard*: Article 23 has been revised to reflect the decisions of the Working Group at its fifty-ninth session (A/CN.9/1005, paras. 67 and 68).

[63] *Designation of reliable trust services – general*: Article 24 establishes a mechanism for the ex ante determination of reliable trust services. Paragraphs 1 and 4 (para. 3 of the previous draft) have been revised to reflect the decision of the Working Group at its fifty-ninth session that the focus of designation is the trust service and not the method used by the trust service (A/CN.9/1005, para. 73). It was explained during discussions at the 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.

[64] *Designation of reliable trust services – obligations of designating authority*: A new paragraph 2 has been inserted to reflect the decision of the Working Group at its fifty-ninth session to impose two new obligations on the designating authority (A/CN.9/1005, para. 73). The purpose of paragraph 2(a) is to ensure some degree of consistency between trust services that are designated as reliable applying an ex ante approach and those that satisfy the reliability standard in article 23 applying an ex post approach. The purposes of paragraph 2(b) is to promote transparency and inform potential subscribers of the relevant trust service (A/CN.9/1005, para. 70).

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

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 25. Liability of trust service providers[65]

Option A

[The liability of trust service providers shall be determined according to applicable law.][66]

Option B

A trust service provider shall bear the legal consequences for its failure to comply with its obligations under [this instrument].

Option C

1. The trust service provider shall be liable for damage caused to any person due to intentional or negligent failure to comply with its obligations under [this instrument].

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

[65] *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. Several proposals were put forward. The Working Group requested the Secretariat to redraft article 25 to reflect those proposals for future consideration. Article 25 of the present draft has been recast accordingly. Option A adopts the minimalist approach by reminding that the liability of the trust service provider, including any limitation thereof, is to be determined according to applicable law. Option B adopts the approach taken in article 9(2) MLES. While it preserves any limitations on liability under applicable law, it specifies that some legal consequences will flow from a failure of the trust service provider to comply with the obligations set out in the draft instrument. Option C provides the most guidance building upon article 25 of the previous draft. It includes a new paragraph 2, which is based on article 11(4) of the eIDAS Regulation. Paragraph 3 has been revised to reflect the decisions of the Working Group (A/CN.9/1005, para. 76).

[66] The Working Group may wish to consider whether this provision should be retained in case the draft instrument had 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.

Chapter IV. International aspects

Article 26. Cross-border recognition of IdM and trust services[67]

1. An IdM system operated or a trust service provided outside [*the enacting State*] shall have the same legal effect in [*the enacting State*] as an IdM system operated or a trust service provided in [*the enacting State*] if it offers a substantially equivalent[68] level of reliability.

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

Article 27. Cooperation[69]

[*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.

---

[67] *Cross-border recognition – general*: Article 26 is inspired by article 12(2) MLES. The purpose of that provision is "to provide the general criterion for the cross-border recognition of certificates without which suppliers of certification services might face the unreasonable burden of having to obtain licences in multiple jurisdictions" (see *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001*, United Nations publication, Sales No. E.02.V.8, Part Two, para. 153). Article 26 aims at providing guidance in the implementation of other provisions of the draft instrument addressing cross-border recognition, namely: article 10(2) (geographic origin not relevant in determining the reliability of IdM methods); article 11(4) (geographic origin not relevant in designating reliable IdM methods); article 23(3) (geographic origin not relevant in determining the reliability of trust services) and article 24(4) (geographic origin not relevant in designating reliable trust services). Articles 10(2), 11(4), 23(3) and 24(4) are based on article 12(1) MLES, which establishes a general rule of non-discrimination in determining the legal effectiveness of a certificate or electronic signature (see *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001*, Part Two, para. 152). To assist these deliberations, the Working Group may wish to review its discussion of the interaction between articles 12(1) and 12(2) MLES, as recorded in document A/CN.9/483, paras. 28–36.

[68] *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. 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).

[69] *International cooperation*: Article 27 has been revised to reflect the decisions of the Working Group at its fifty-ninth session (A/CN.9/1005, para. 122).