United Nations A/CN.9/WG.IV/WP.164

General Assembly

Distr.: Limited
25 August 2020

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Sixtieth session
Vienna, 19–23 October 2020

Draft Provisions on the Use and Cross-border Recognition of Identity Management and Trust Services – synthesis of comments submitted by States and international organizations

Note by the Secretariat

Contents

V.20-04519 (E)

I. Introduction

1. Prior to the postponement of the sixtieth session of the Working Group due to the COVID-19 pandemic, the Secretariat distributed a note (A/CN.9/WG.IV/WP.162) containing revised draft provisions on the use and cross-border recognition of identity management (IdM) and trust services (the "draft provisions").

2. To facilitate the progress of work, the Secretariat invited States, international governmental organizations and those international non-governmental organizations invited to the Working Group to submit comments on the draft provisions ahead of the rescheduled sixtieth session. The Secretariat prepared a template for submitting comments, which comprised a table containing a non-exhaustive list of questions for the various draft provisions drawn from A/CN.9/WG.IV/WP.162 and a table for general comments on the draft provisions.

3. At the submission date of this document, the Secretariat has received submissions from 24 States and the European Union, as well as from two international organizations.

4. This document – which is comprised of A/CN.9/WG.IV/WP.164 and A/CN.9/WG.IV/WP.164/Add.1 – does not reproduce the comments submitted. Rather, it synthesizes those comments to present various positions on the draft provisions and links each position to the relevant States and international organizations by way of the footnotes. Each position is presented in terms expressed by the Secretariat and does not necessarily reflect the terms of the comments submitted by the relevant States and international organizations. In the footnotes:

(a) The term "EU" refers to the comments jointly submitted by the European Commission and seven EU member States (Austria, Belgium, Czechia, France, Germany, Italy and Poland);

(b) The term "UINL" refers to the International Union of Notaries; and

(c) The term "CIETAC" refers to the China International Economic and Trade Arbitration Commission.

5. Moreover, this document does not synthesize the comments submitted by the World Bank on the draft provisions (A/CN.9/WG.IV/WP.163) but rather links the various positions presented to those comments by way of the footnotes.

II. Key issues raised

6. A number of key issues emerge from the comments submitted, namely:

(a) The object and purpose of the draft provisions;

(b) The need to "map" the existing applicable legal landscape;

(c) The concepts of "electronic identification", "identity proofing" and "trust service";

(d) The accommodation of multiparty contract-based IdM systems;

(e) The interaction with government-operated IdM systems; and

(f) The treatment of objects.

A. The object and purpose of the draft provisions

7. The comments submitted indicate a difference of view among members of the Working Group on what the draft provisions are designed to do. On one view, the draft provisions are designed to give legal recognition to the use of IdM and trust services. On another view, the draft provisions are designed to regulate the provision of IdM and trust services. This difference of view is anticipated by the comments

submitted by the World Bank, which notes that the draft provisions on IdM currently address the use and cross-border recognition of IdM systems and invites the Working Group to consider whether the provisions should address "IdM transactions", as well as the "functioning of an IdM system" and the "provision of IdM services".[1]

8. The Working Group agreed early on that the goals of its work on IdM and trust service should be "legal recognition and mutual recognition".[2] While initial discussions focussed on achieving these goals in a cross-border context,[3] the Commission noted at its fifty-second session in 2019 that the Working Group should "work towards an instrument that could apply to both domestic and cross-border use" of IdM and trust services.[4] The Commission has also noted that the instrument should be guided by the core principles of UNCITRAL's work in the area of electronic commerce, notably technology neutrality, non-discrimination against the use of electronic means, functional equivalence and party autonomy.[5]

9. The operation of the draft provisions may be summarized as follows:

(a) They give "legal recognition" to electronic identification and the provision of trust services by prohibiting discrimination against the use of electronic means in verifying a person's identity (i.e., electronic identification) or in verifying particular qualities of data (i.e., the provision of a trust service) (articles 5 and 13);

(b) They give "legal effect" to electronic identification and the provision of trust services by declaring that they satisfy legal requirements for (i) in-person identification, or (ii) using a particular procedure for the execution, delivery and retention of paper-based documents or records, if a "reliable" method is used (articles 9 and 16-22);

(c) They provide for – but do not mandate – the designation of IdM systems and trust services that are "reliable" ("ex ante" determination of reliability) (articles 11 and 24);

(d) They impose certain standalone obligations on (i) the IdM service provider and trust service provider relating to the provision of services and interaction with the subscriber (articles 6, 7 and 14), and (ii) the subscriber in the event of a data breach (articles 8 and 15); and

(e) They give "cross-border recognition" to IdM systems operated, and trust services provided, outside the State (article 26).

10. Based on this summary, the draft provisions do regulate the provision IdM and trust services, but only to a limited extent:

(a) On the one hand, the draft provisions regulate the provision of IdM and trust services indirectly through the condition of reliability that is prescribed in articles 9 and 16-22 (by which legal effect is given to electronic identification and trust services that use a "reliable method"). Specifically, by providing that the rules governing the relevant IdM system or trust service are relevant factors in determining reliability, articles 10 and 23 have an indirect effect on the design of IdM systems and trust services that a service provider may wish to use to generate the legal effects provided in articles 9 and 16-22. The extent to which the draft provisions confer a right on the parties to agree on the reliability of the method remains an open issue (see paras. 23–24 below).

(b) On the other hand, the draft provisions regulate the provision of IdM and trust services directly by imposing certain obligations on the service provider and subscriber (as noted in para. 9(d) above).

[1] A/CN.9/WG.IV/WP.163, pp. 5–6.
[2] A/CN.9/902, para. 45.
[3] A/CN.9/936, para. 61.
[4] A/74/17, para. 172.
[5] A/73/17, para. 159.

11. The draft provisions do not, however, establish a comprehensive regime for regulating IdM or trust services (such as the regime for IdM established in Switzerland under the recently enacted Federal Law on Electronic Identification Services and the regime for trust services established in the EU under the eIDAS Regulation[6]). At most, what could be said is that the draft provisions are designed to regulate the provision of IdM and trust services to the extent necessary to give legal recognition and effect to those services.

B. The need to "map" the existing applicable legal landscape

12. Option A of article 9(1) applies a functional equivalence approach to giving legal effect to the use of IdM.[7] It focuses on the identification of a person rather than on the production of credentials for the purpose of identification.[8] However, the role of functional equivalence in the draft provisions has been questioned in some of the comments submitted (see synthesis of comments on question 3 for article 9 below).[9]

13. Provisions giving legal effect to IdM and trust services on a functional equivalence approach assume the existence of certain laws that are designed for paper-based or in-person transactions. In the context of IdM, these are laws which require or permit the identification of a person. In the context of trust services, these are laws which require or imply a particular procedure for executing, delivering and retaining documents or records (e.g., articles 16-20). The draft provisions also assume the existence of laws that require the identification of a person in accordance with a procedure defined or prescribed by law (e.g., on the basis of particular identity documents or the in-person presence of the person being identified) (article 2(3)).

14. Related issues as to how the draft provisions "plug in" to contract-based IdM systems and legislated government-operated IdM systems are addressed separately below (see paras. 22–28).

C. The concepts of "electronic identification", "identity proofing" and "trust service"

15. The definition for each of these terms in article 1 of the draft provisions seeks to reflect decisions taken by the Working Group, including its decision to ask the Secretariat "to ensure that the notions of authentication, identification and verification [are] used consistently through the instrument, as well as consistently with terminology adopted by the International Telecommunication Union (ITU)".[10] Nevertheless, the comments submitted indicate some concern among members of the Working Group that these terms may be misinterpreted or that their definitions may be misdirected.

1. Electronic identification

16. The concept of "electronic identification" raises two issues. The first issue is that the term "electronic identification" could be mistaken for referring to the entire

[6] 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.

[7] As noted in footnote 32 of the draft provisions, option B of article 9(1) does not apply a functional equivalence approach.

[8] The Working Group has considered whether the object of legal recognition should be electronic identity credentials that are functionally equivalent to paper-based identity credentials used for identification purposes (e.g., e-passports). It has also considered giving legal effect to electronic identity credentials that have no paper-based equivalence. See generally A/CN.9/965, paras. 62–85.

[9] The Working Group has also considered the role of functional equivalence in its previous sessions: ibid.

[10] A/CN.9/1005, para. 86.

IdM process, rather than the discrete process constituted by the verification or confirmation of the binding between the person being identified based on presented identity credentials, as per the definition in article 1(d). The second issue is that the definition of "electronic identification" in article 1(d) accords with the concept of "authentication" as understood in some IdM systems and legal systems. For instance, the eIDAS Regulation in the EU defines "authentication" in the context of IdM to mean "an electronic process that enables the electronic identification of a natural or legal person… to be confirmed".[11]

17. Replacing "electronic identification" with "authentication" would result in the same term being used for both IdM and trust services, which in turn engages the point made at the last session of the Working Group that "care should be exercised to ensure that the term [is] used consistently in all instances in the instrument".[12] It would seem that, at least based on the synopsis below (see letter (c) of question 1 for article 1), the use of authentication in both contexts does not pose any problems, noting in particular that the term is used in the eIDAS Regulation in both contexts. Indeed, the point has been made that electronic identification is essentially a trust service (in the sense that it verifies or confirms that data comprising an "identity" is linked to a particular person).

2. Identity proofing

18. The concept of "identity proofing" raises the issue that the term could be mistaken for referring to the verification or confirmation of the binding between the person being identified and an identity (i.e., "electronic identification"), rather than the process during the earlier enrolment phase of the IdM process in which the IdM service provider (or other participant in the IdM system) collects attributes for the subscriber (e.g., personal data) and checks them against trusted sources such as civil registration and vital statistics (CRVS) systems before issuing identity credentials for the subscriber to use for electronic identification. "Identity proofing" is a term adopted by the ITU.[13]

19. To overcome the risk of misinterpretation, the Working Group may wish to consider the need to single out identity proofing in the draft provisions and, if so, whether a different term should be used (e.g., "enrolment").[14]

3. Trust services

20. The concept of "trust service" raises the issue of whether the draft provisions giving legal recognition and legal effect to "trust services" (article 13, 16-22) should instead be concerned with the product of the trust service. In essence, the product of a trust service is the data message provided by the trust service provider which verifies or confirms a particular quality of other data, such as (i) that the other data identifies a specified person, (ii) that the other data indicates a specified time, or (iii) that the other data identifies any specified alteration.

21. The Working Group may wish to consider whether the definition of "trust services" in article 1(m) and the draft provision giving legal recognition to trust

---

[11] 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. Note that, unlike the current draft provisions, the eIDAS Regulation employs the term "electronic identification" not to refer to the process of confirmation but rather to the use of "person identification data" (i.e., an "identity" in the terms of the draft provisions) contained in "electronic identification means" (i.e., "identity credentials" in the terms of the draft provisions) for such confirmation.

[12] A/CN.9/1005, para. 85.

[13] See Recommendation ITU-T X.1252.

[14] For example, (i) definitions referring to "identity proofing" could instead refer to "enrolment", (ii) article 5(a) could omit reference to "identity proofing" (which is not carried out in electronic form), and (iii) article 6(a)(iii) could describe in general terms what "identity proofing" entails instead of referring to that term.

services in article 13 should be reformulated to focus on the product of trust services (i.e., the data message generated in provision of the trust service).

D. The accommodation of multiparty contract-based IdM systems

22. The comments submitted indicate some uncertainty as to how the draft provisions accommodate multiparty contract-based IdM systems, such as trust frameworks. These systems involve different participants, such as enrolment agents, attribute providers and authentication providers, performing different functions under a matrix of contracts. Accommodating multiparty contract-based IdM systems raises two distinct yet connected issues. The first issue is concerned with the contractual basis for these systems and the principle of party autonomy. The second issue is concerned with the participation of multiple parties in these systems and pinpointing the appropriate IdM service provider for the purposes of the draft provisions.

1. Party autonomy

23. The draft provisions establish a range of rights and obligations that may be inconsistent with the rights and obligations of the various participants in an IdM system according to the rules governing the IdM system, which are given legal standing in the contracts between the participants. The draft provisions also establish a liability regime that may be inconsistent with the liability regime established under the rules governing the IdM system (by way of indemnities, disclaimers and liability caps). On their face, the draft provisions prevail to the extent of that inconsistency. Unlike the MLES, the draft provisions do not confer a right on the parties (e.g., participants in an IdM system) to vary the effect of the provisions as between themselves by contract.[15] This is consistent with a regulatory approach to IdM.

24. The Working Group may wish to clarify whether the draft provisions should have mandatory application, or whether they should confer a right on the parties to contract out of the provisions in favour of the rules of the relevant IdM system on the basis of party autonomy.

2. Pinpointing the appropriate IdM service provider

25. The draft provisions refer to the “IdM service provider” in the singular. While the reference in some of the draft provisions to the “IdM service provider” could be interpreted severally, other provisions, notably article 6, contemplate a single IdM service provider that performs a range of functions, including identity proofing, identity credentials management and electronic identification.

26. The Working Group may wish to consider whether the draft provisions need to be adapted to recognize that multiple parties may be responsible for performing functions within an IdM system. One option suggested in the comments submitted[16] is to pinpoint the IdM service provider as the person which performs the electronic identification (i.e., which verifies or confirms the binding between the person being identified and an identity) and to modify article 6 so as to oblige that person to “ensure” that the functions listed therein are performed (thus allowing for these functions to be performed by a person other than the IdM service provider). If the Working Group wished to consider this option, it may also wish to consider how, under option C of article 12, the IdM service provider would be liable for the failure of another participant to perform its functions, and whether it can offset its liability against that other participant under the rules governing the IdM system.

[15] Compare article 5 MLES, which provides that its provisions “may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law”.

[16] See letter (b) of issue 1 for article 6.

E. Interaction with government-operated IdM systems

27. States around the world have established IdM systems to assist individuals (and corporations) interact with government services (and also with the private sector). These government-operated IdM systems are sometimes – but not always – established by legislation.[17] Some of the comments submitted have indicated interest in addressing how the draft provisions interact with government-operated IdM systems and the Working Group may wish to consider this issue further.

28. In this regard, the application of the draft provisions may be summarized as follows:

(a) The draft provisions apply to the use of IdM systems and trust services in the context of commercial activities and trade-related services (article 2(1)), including when involving government agencies (either as a commercial party or as the provider of trade-related services);

(b) At the same time, the draft provisions do not require a government agency to use an IdM or trust service (article 3(1)), and the legislation establishing government-operated IdM systems would prevail to the extent of any inconsistency with the draft provisions (article 2(4));

(c) The draft provisions do not address issues of interoperability of IdM systems or portability of credentials, including with respect to government-operated IdM systems. Specifically, they do not confer any right on a participant in the other IdM system to use identity credentials issued by a government-operated IdM system (which may be restricted under existing law, including laws relating to privacy and data protection)[18] or to access the government-operated IdM system to perform electronic identification using those identity credentials;

(d) Moreover, the draft provisions give no special legal treatment to "attributes" or "identities" that are sourced from a government-operated database such as a civil registration and vital statistics (CRVS) system (see synthesis of comments on question 6 for article 1 below), or to electronic identification using identity credentials issued by a government-operated IdM system (except to the extent that such an IdM system is designated under article 11).

III. Synthesis of comments on chapter I (general provisions)

A. Article 1 – definitions

1. Synthesis of comments in response to specific questions

Question	*Synthesis of comments*
1. According to the terminology used in WP.162, the IdM process is made up of two stages (or phases), "identity proofing" and "electronic identification" (see para. 2 of WP.162). Are these terms adequate to describe the stages of the	(a) The terms are acceptable.[19] (b) The term "authentication" should be used instead of "electronic identification".[20] The term "electronic identification" may be misinterpreted to cover the entire IdM process.[21]

[17] See, e.g., the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 in India, the Electronic Identity Verification Act 2012 in New Zealand, the National Identity Management Commission Act, 2007 in Nigeria, the Philippine Identification System Act in Philippines.

[18] See, e.g., restrictions on the use of "government related identifiers" under clause 9.1 and 9.2 of Schedule 1 to the Privacy Act 1988 (Australia).

[19] Lebanon, Senegal (with reference to "electronic identification"), Singapore, Switzerland, Ukraine, CIETAC, UINL.

[20] EU, United Kingdom, United States.

[21] United Kingdom, United States.

Question	*Synthesis of comments*
IdM process? Are the definitions of these terms accurate?	(c) It is appropriate for the term "authentication" to be used in both the IdM and trust services[22] contexts. (d) The term "enrolment" should be used instead of "identity proofing".[23] (e) The binding between the subject and an identity (as referred to in the definition of "electronic identification") occurs at the identity proofing phase and not at the electronic identification phase.[24] (f) The concept of "electronic identification" should be understood as referring to the *confirmation* of identity.[25] (g) It is erroneous for the draft provisions to assume that the IdM process comprises only two phases – identity proofing and electronic identification (see, e.g., in the definitions of "identity management (IdM) services" and "identity management (IdM) system").[26] (h) The draft provisions should expressly refer to *authentication and exchange of identity information or to verification and validation* as an additional phase in the IdM process.[27]
2. Is the new definition of "authentication" in the context of trust services (articles 21 and 22) acceptable (see footnote 3 of WP.162)?	(a) The definition is acceptable.[28] (b) The definition is not acceptable.[29] (c) In the chapter on trust services, the term "authentication" should be defined in terms of *confirmation* (of identity, integrity etc.).[30]
3. Is it necessary to include a definition of "electronic identification factors" (as used in article 6)? If so, is the definition in footnote 6 of WP.162 acceptable?	(a) A definition of this term is necessary.[31] The definition in footnote 6 is acceptable.[32] (b) Using the term emphasizes that the governance of such factors is separate to the governance of identity credentials.[33] (c) A definition of this term is not necessary.[34] (d) The term "electronic identification factors" should not be used.[35] Article 6(d)(i) should be omitted.[36] The term "electronic identification means", as used in the eIDAS Regulation, should replace "identity credentials".[37]

[22] EU and United States.
[23] Denmark.
[24] Denmark, United Kingdom.
[25] United Kingdom.
[26] Denmark.
[27] Denmark, Switzerland.
[28] Singapore, Switzerland, UINL.
[29] Denmark, EU.
[30] Dominican Republic, EU, Ukraine, United Kingdom, CIETAC.
[31] EU, Lebanon, Singapore, CIETAC, UINL.
[32] EU, Lebanon, Singapore, CIETAC, UINL.
[33] Singapore.
[34] Switzerland, Ukraine, United States.
[35] Denmark, United Kingdom.
[36] United Kingdom.
[37] Denmark.

Question	*Synthesis of comments*
4. Is it necessary to include a definition of "electronic identification mechanisms" (as used in article 6)? If so, is the definition in footnote 7 of WP.162 acceptable?	(a) A definition of this term is necessary.[38] The definition in footnote 6 is acceptable.[39] (b) A definition of this term is necessary, but the term should be defined to mean the mechanisms by which a subject uses identity credentials to "confirm its identity to a third party".[40] (c) The concept needs to be discussed further. The definition is problematic as it focuses on the conduct of the subject and not that of the IdM service provider.[41] (d) A definition of this term is not necessary.[42] (e) The term "electronic identification factors" should not be used. The relationship between this concept and "identity credentials" should be clarified.[43]
5. Should the definition of "identity management (IdM) services" refer to "services consisting of managing identity proofing or electronic identification of [subjects][persons] in part or in full in electronic form" to include in that definition any step (e.g. identity proofing) that may be carried out offline? *Note by Secretariat: A similar specification could be included in the definition of "identity management (IdM) system".*	(a) This specification is unnecessary.[44] It is implicit in the definition.[45] (b) The definition of "identity management (IdM) services should specify that services may be "in part of in full" in electronic form.[46] (c) The definition is too imprecise and should include an indicative list of services.[47]
6. Is it necessary to add a clarification (either in a definition – for instance, of "identity" or of "identity proofing" – or in an explanatory document) to indicate that records from civil registration and vital statistics (CRVS) systems may be a reliable source of attributes of physical persons and, similarly, a dedicated registry may be a reliable source of attributes of legal persons?	(a) A reference to CRVS systems as a reliable source of attributes is not necessary.[48] (b) The draft provisions should not recognise CRVS systems as a reliable source of attributes.[49] (c) A reference to CRVS systems as a reliable source of attributes could be useful.[50] (d) The draft provisions could recognise CRVS systems as a reliable source of attributes if the concept of "reliable source" is defined.[51] (e) Examples of reliable sources of attributes, including CRVS, could be included in an explanatory document.[52]

[38] Dominican Republic, EU, Lebanon, CIETAC.
[39] EU, Lebanon, CIETAC.
[40] China.
[41] United States.
[42] Switzerland, Ukraine, United Kingdom, UINL.
[43] Denmark.
[44] Ukraine, UINL.
[45] UINL.
[46] Denmark, EU, Lebanon, Singapore, Switzerland, United Kingdom, United States, CIETAC.
[47] Argentina.
[48] CIETAC, UINL.
[49] EU, Switzerland, Ukraine, United States.
[50] Denmark, United States.
[51] Denmark.
[52] United Kingdom.

Question	*Synthesis of comments*
7. Is it necessary to insert a definition of the term "level of assurance", as used in articles 10(1)(b), 11(3) and 27(c)?	(a) A definition of this term is not necessary.[53] (b) A definition of this term is useful.[54] (c) A definition of this term is necessary.[55]

2. Synthesis of other comments on article 1

Issue	*Synthesis of comments*
1. "Identity credentials"	(a) The definition of the term should be amended to refer to the verification or authentication of identity (rather than electronic identification).[56] (b) The term "authenticator" should be used instead, and the definition should refer to behavioural characteristics to capture biometrics.[57]
2. "Identity proofing"	*See letter (d) of question 1 for article 1*
3. "Subscriber"	(a) The term "subscriber" as defined could be understood to refer to the relying party rather than the subject (i.e., the person being identified).[58] (b) The definition of "subscriber" could be understood to include not only to the subject, but also attribute providers and other persons who enter into a contractual arrangement with an IdM service provider.[59]
4. "Subject"	*See letter (a) of issue 1 for article 22*
5. "Trust services"	(a) The definition is imprecise and should include an indicative list of services.[60]
6. Terms not defined	(a) The term "identifier" (in the definition of "authentication") should be defined.[61] (b) The term "identity management" should be defined.[62] (c) The term "rules governing the IdM system" (as used in articles 6(c), 6(f) and 10(1)(b)) should be defined.[63] See also "rules governing the trust service" (as used in article 23(1)(a)). (d) The term "verification" (as used in articles 6(a)) should be defined.[64]

[53] United States, CIETAC, UINL.
[54] Lebanon, Switzerland, Ukraine, United Kingdom.
[55] Argentina, Denmark.
[56] China.
[57] United Kingdom.
[58] Denmark, United Kingdom.
[59] United States. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, pp. 5 and 8).
[60] Denmark, United Kingdom.
[61] Dominican Republic. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, p. 4).
[62] Dominican Republic, United States. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, p. 4).
[63] Argentina, Dominican Republic. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, p. 4).
[64] Argentina, Dominican Republic. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, p. 4).

Issue	*Synthesis of comments*
7. Terminology in general	(a) The draft provisions should include reference to the following concepts: “electronic commerce”, “digital document”, “electronic data interchange” and “electronic signature”.[65] (b) The definition of “identity management (IdM) services” and “identity management (IdM) system” should be revised to avoid the redundant reference to “electronic identification” as being in “electronic form”.[66] (c) The terminology of the draft provisions should be more closely aligned with terminology used internationally in matters of privacy and data protection.[67] (d) Some of the terminology is outdated and should be revised to reflect current usage, while also accommodating future developments in IdM and trust services.[68]

B. Article 2 – scope of application

1. Synthesis of comments in response to specific questions

The template contained no specific questions on article 2.

2. Synthesis of other comments on article 2

Issue	*Synthesis of comments*
1. Inclusions within scope	(a) The current scope is sufficient.[69] (b) The Working Group should consider whether the draft provisions apply to government agencies engaged in commercial activities.[70] (c) The Working Group should address IdM and trust services separately.[71] The most important work to be done at this point is to identify and define the issues appropriate to (i) identity transactions and IdM systems, and (ii) existing law imposing identification requirements on the private sector.[72]
2. Exclusions from scope	(a) The draft provisions should contain a provision stating that it is not concerned with surveillance or tracking of persons, or with the processing of personal data for any other purposes.[73]

[65] Dominican Republic.
[66] El Salvador.
[67] Argentina.
[68] Canada.
[69] United Kingdom. Compare comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, pp. 5-6).
[70] Argentina.
[71] Canada, United States.
[72] United States.
[73] Niger.

Issue	*Synthesis of comments*
	(b) The draft provisions should not require the use of a particular IdM system.[74] (c) The draft provisions should only apply to multiparty IdM systems. Two-party IdM systems should be excluded from scope.[75]
3. Interaction with government-operated IdM systems	(a) It is unclear how the draft provisions interact with government-operated IdM systems (e.g., whether a commercial party can use such systems for the identification of another party).[76] (b) The Working Group could consider additional provisions addressing interaction, including on access to government-operated IdM systems and additional conditions.[77]

C. Article 3 – voluntary use of IdM and trust services

1. Synthesis of comments in response to specific questions

Question	*Synthesis of comments*
1. There have been questions about the relationship between articles 2 and 3. Would their relationship be clearer by recasting article 3 to state: "Nothing in this [instrument] requires a [person][relying party] to accept the electronic identification of a subject or to rely on a trust service without the [person's][relying party's] consent."?	(a) It is unnecessary to recast article 3 in this way.[78] (b) Article 3 should be recast in this way.[79] (c) Article 3 should also contain a provision for subscribers to the effect that the instrument does not require the subscriber to present its identity for electronic identification without its consent.[80] (d) It is important for the draft articles to confirm voluntary use for all parties.[81] (e) There is a partial overlap between article 2(2) and 2(3) and article 3(1).[82] (f) Article 2 and 3 can be combined.[83]

2. Synthesis of other comments on article 3

Issue	*Synthesis of comments*
1. Consent to use an IdM or trust service	(a) Article 3 should specify that consent must be informed, freely given, explicit and unambiguous, and that consent may be withdrawn.[84]

[74] United Kingdom, United States. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, p. 6).
[75] United States.
[76] United States. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, pp. 2 and 6).
[77] Russian Federation. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, pp. 2-3).
[78] EU, Switzerland, CIETAC.
[79] Lebanon, Ukraine, United Kingdom, UINL.
[80] United Kingdom.
[81] EU, Russian Federation.
[82] Russian Federation.
[83] Senegal.
[84] Senegal.

Issue	*Synthesis of comments*
	(b) It is not enough for consent to be inferred by conduct (as specified in article 3(2)).[85] (c) Article 3 should specify the purpose for which consent is given.[86]
2. Party autonomy	(a) The draft provisions should clarify the interaction between the instrument and the rights and obligations of the parties under contract, including under the contracts that form the basis of multiparty IdM systems (e.g., trust frameworks).[87] Specifically, the Working Group should consider identifying the provisions that are mandatory and those whose effect may be varied by the parties under contract.[88] (b) The draft provisions should state that matters not governed by the instrument are determined by any contract between the parties. Failing that, the law of the subscriber's domicile should be applied.[89] (c) Mandatory rules are often redundant and may result in increased costs for IdM services, with particularly impact on small and medium-sized enterprises. Moreover, it is difficult to reach consensus on mandatory rules and the discussion of mandatory rules may jeopardise the principle of technology neutrality.[90]

D. Article 4 – interpretation

1. Synthesis of comments in response to specific questions

The template contained no specific questions on article 4.

2. Synthesis of other comments on article 4

Issue	*Synthesis of comments*
1. Terminology	(a) The concept of "international character" of the instrument is not clear and may not be appropriate for a model law.[91] (b) It is not clear how "uniformity" of application should apply for a model law.[92] (c) It is not clear whose "good faith" is relevant in the context of a model law.[93] (d) It is questionable whether the instrument, in the form of a model law, needs to refer to the rules of private international law for the purposes of interpretation.[94]

[85] Dominican Republic, Senegal. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, p. 6).
[86] United Kingdom.
[87] United Kingdom, United States. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, pp. 3, 6-7).
[88] Canada. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, pp. 3, 6-7).
[89] Argentina.
[90] Russian Federation.
[91] United States.
[92] United States.
[93] United States.
[94] United States.

IV. Synthesis of comments on chapter II (identity management)

A. Article 5 – legal recognition of IdM

1. Synthesis of comments in response to specific questions

The template contained no specific questions on article 5.

2. Synthesis of other comments on article 5

Issue	*Synthesis of comments*
1. Application of article 5	(a) The scope and purpose of this provision is not clear.[95] (b) It is not clear how article 5 interacts with paper-based identification requirements under existing law, particularly in view of article 2(3).[96]

B. Article 6 – obligations of IdM service providers

1. Synthesis of comments in response to specific questions

Question	*Synthesis of comments*
1. Is it desirable to retain the words "at a minimum" in the chapeau?	(a) These words should be retained.[97] They make it clear that the list is not exhaustive of the functions performed by IdM service providers.[98] (b) It is not clear what these words are meant to convey without knowing what functions of the IdM service provider are covered.[99]

2. Synthesis of other comments on article 6

Issue	*Synthesis of comments*
1. Accommodating multiparty IdM systems	(a) The draft provisions need to accommodate multiparty IdM systems, in which the functions listed in article 6 may be performed by a variety of different participants in the system, and participants may perform a variety of functions.[100] (b) In a multiparty IdM system, the party which performs the electronic identification should be responsible for the other functions listed in article 6 (relating to identity proofing and identity credentials management) even it that party does not actually carry out that function itself. Accordingly, while the list of functions in article 6 is appropriate, the text of article 6 should be revised to acknowledge that persons other than the "IdM service provider" may actually carry out some of the functions listed.[101]

[95] Denmark.
[96] United States.
[97] EU (if the instrument is a model law), Lebanon, Senegal, Switzerland, Ukraine, CIETAC, UINL.
[98] Ukraine.
[99] Denmark.
[100] United Kingdom, United States. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, p. 6).
[101] United Kingdom.

Issue	*Synthesis of comments*
2. Listed functions	(a) The manner of enrolling subjects should be clarified.[102] (b) It is not ordinarily the IdM service provider which updates attributes (as listed in article 6(b)).[103] (c) Article 6 should also include obligations of confidentiality, security, retention, and continuity of service.[104]

C. Article 7 – obligations of IdM service providers in case of data breach

1. Synthesis of comments in response to specific questions

Question	*Synthesis of comments*
1. Is "containing" a security breach the desired objective of the steps taken by the IdM service provider to respond to the breach, as required by article 7(1)(a)?	(a) The desired objective is to "contain" the security breach.[105] (b) The desired objective is to put an end to the security breach.[106] (c) Containment is not the only desired objective. (d) Containment is not enough. The desired objective is to remedy or mitigate the security breach.[107]

2. Synthesis of other comments on article 7

Issue	*Synthesis of comments*
1. Terminology	(a) The concept of "significant impact" needs to be clarified.[108] (b) The obligation to "remedy" in article 7(1)(b) should be clarified.[109] (c) It is not clear that to which "applicable law" refers.[110] *Note by Secretariat: The Working Group decided to include this reference at its fifty-ninth session: A/CN.9/1005, paras. 34-36.*
2. Preconditions	(a) The obligations in article 7 should be engaged in the event of any security breach (not just those with a "significant impact").[111] (b) The obligations in article 7 should be engaged only if the IdM service provider is aware of the security breach.[112]

[102] El Salvador.
[103] Denmark.
[104] Senegal.
[105] EU, Lebanon, Switzerland, Ukraine, United Kingdom, CIETAC, UINL.
[106] Senegal.
[107] Denmark.
[108] United States.
[109] United States. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, p. 7).
[110] United States.
[111] United States.
[112] Singapore.

Issue	*Synthesis of comments*
3. Accommodating multiparty IdM systems	(a) The obligations in article 7 should be distributed among the various participants in a multiparty IdM system and imposed on the participant with responsibility for the component of the IdM system that is breached or compromised.[113]

D. Article 8 – obligations of subscribers

1. Synthesis of comments in response to specific questions

Question	*Synthesis of comments*
1. Are there any circumstances in which rights and obligations of relying third parties should be addressed in the draft provisions (e.g., to notify breaches of which they are aware)?	(a) The draft provisions should not address the rights and obligations of relying third parties.[114] The obligations of relying parties are ordinarily addressed in the rules governing the IdM system.[115] (b) The draft provisions should not address the rights and obligations of relying parties if there is no contractual relationship between the relying party and the IdM service provider.[116] If the relying party is a participant in the IdM system, it should be subject to the obligations in articles 6 and 7.[117] (c) The draft provisions should impose an obligation (i) to use the electronic identification mechanism only in accordance with the conditions of the IdM service provider, and (ii) not to use the identification mechanism for purposes and activities that are prohibited by law or in a manner that is discriminatory.[118]

2. Synthesis of other comments on article 8

Issue	*Synthesis of comments*
1. "Subscriber"	*See issue 3 for article 1.*
2. Scope of obligations	(a) It may not be reasonable to impose the obligations in article 8 on subscribers. For instance, a subscriber may be aware of circumstances indicating that the identity credentials or electronic identification mechanisms have been compromised, but not understand the significance of those circumstances. Moreover, the subscriber might not be in a position to determine the existence of a "substantial risk".[119]

[113] Dominican Republic, United States. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, p. 7).
[114] Denmark (also for article 16), EU (also for article 16), Lebanon (also for article 16), Singapore, Switzerland (also for article 16), Ukraine (also for article 16), United States.
[115] Denmark, EU.
[116] Switzerland, United States.
[117] Dominican Republic.
[118] United Kingdom. The Working Group may wish to consider whether such additional obligations should be imposed on the subscriber or on a relying party.
[119] United States. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, pp. 8-9).

Issue	*Synthesis of comments*
	(b) The draft provisions should impose an obligation on a subscriber to notify the IdM service provider of fraud or the usurpation of its identity.[120]

E. Article 9 – identification using IdM

1. Synthesis of comments in response to specific questions

Question	*Synthesis of comments*
1. Which option for article 9(1) is preferable?	(a) Option A.[121] (b) Option B.[122]
2. What is the relationship between article 2(3) and article 9?	(a) Articles 2(3) and 9 contradict one another.[123] (b) Article 2(3) makes it clear that article 9 does not alter any specific procedure required by domestic law.[124] If domestic law requires identification, article 9 applies, whereas if the law requires identification using a specific procedure, article 9 does not apply.[125] (c) Article 2(3) is the principle and article 9 explains the methods involved.[126]
3. Is it necessary to retain a functional equivalence provision for identification, or are the identification components of electronic signatures and electronic seals sufficient to achieve the desired goal of establishing functional equivalence standards for identification?	(a) A provision on functional equivalence for identification should be retained.[127] (b) A provision on functional equivalence for identification should not be retained.[128] (c) Functional equivalence may not be the proper question.[129]
4. If article 9 is retained, should the reliability standard of the method referred to in article 9 be qualified as "reliable as appropriate" to better reflect the varying standards for offline identification?	(a) The standard for the method used should be "as reliable as appropriate".[130] (b) The standard "as reliable as appropriate" would need to be defined.[131] (c) The standard "as reliable as appropriate" should not be used.[132] (d) It is not necessary to qualify the reliability standard because appropriateness is addressed in article 11.[133]

[120] Niger.
[121] EU, Russian Federation, Singapore, Switzerland, UINL.
[122] China, Ukraine, CIETAC.
[123] United States.
[124] United Kingdom.
[125] Singapore.
[126] Lebanon.
[127] Lebanon, Senegal, Singapore, Switzerland, United Kingdom.
[128] China, UINL.
[129] United States.
[130] Lebanon, Singapore, Switzerland, United Kingdom, United States. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, p. 10).
[131] Senegal, UINL.
[132] Denmark.
[133] EU.

Question	*Synthesis of comments*
5. Is it desirable to insert a provision to acknowledge that the IdM service provider might be the person seeking to rely on the electronic identification?	(a) Such a provision is desirable.[134] Only in the case of a multiparty IdM system in which the relying party is a participant.[135] *See also letter (c) of issue 2 for article 2.* (b) Such a provision is unnecessary.[136] It is clear from the draft provisions that article 9 applies where the IdM service provider is the relying party.[137] Such an acknowledgment can be included in an explanatory document.[138]

2. Synthesis of other comments on article 9

Issue	*Synthesis of comments*
1. Survey of domestic law requiring identification	(a) The Working Group should identify existing law imposing identification requirements on the private sector.[139]
2. Object of reliability assessment ("method" of electronic identification versus "IdM system"/"trust services")	(a) It is not just the "method" of the electronic identification but the IdM system as a whole that must be reliable.[140] *See also question 2 for article 26*
3. Using the UNCITRAL Model Law on Electronic Signatures (MLES) as a model.	(a) It is questionable whether the MLES should serve as a model for draft provisions on IdM given additional complexities of IdM and additional parties involved.[141]

F. Article 10 – factors relevant to determining reliability

1. Synthesis of comments in response to specific questions

Question	*Synthesis of comments*
1. Article 10(1)(d) aims at accommodating IdM systems governed by contractual rules such as trust frameworks. Its operation is limited to the parties to those contractual agreements. Is the provision sufficient for its intended purpose? Or does it require further	(a) Article 10(1)(d) is sufficient in its current wording.[142] (b) It is not clear (i) how the standards in articles 10 and 23 interact with contractual agreements and (ii) how contractual agreements should be balanced against the other factors listed in articles 10 and 23 (including where that balancing exercise is carried out by the designating person, organ or authority under articles 11(2)(a) and 24(2)(a)).[143] (c) Article 10(1)(d) should specify the types of agreement to which it applies.[144]

[134] Lebanon. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, p. 3).
[135] United States.
[136] EU, Switzerland, United Kingdom.
[137] EU.
[138] Switzerland.
[139] United States. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, p. 6).
[140] Dominican Republic. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, pp. 10-11).
[141] United Kingdom, United States. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, p. 6).
[142] Lebanon, United Kingdom.
[143] United States (also for article 23(1)(h)).
[144] Switzerland (also for article 23(1)(h)).

Question	*Synthesis of comments*
specification (either in the provision itself or in an explanatory document)?	(d) Article 10(1) should specify how an agreement between the parties should be taken into account where the IdM system does not provide "strong" authentication.[145] (e) The purpose of article 10(1)(d) should be elaborated in an explanatory document.[146] (f) An agreement between the parties should not be a factor in determining reliability. The reliability of IdM systems and trust services should be determined according to common standards.[147]
2. Does the title of article 10 adequately reflect its content? If not, should it be replaced by "requirements for determining reliability"? Should the titles of articles 10 and 23 be aligned?	(a) The title of article 10 is appropriate.[148] The title of article 23 should be revised accordingly.[149] (b) The title of article 10 should be replaced by "requirements for determining reliability".[150] The title of article 23 should be revised accordingly.[151]

2. Synthesis of other comments on article 10

Issue	*Synthesis of comments*
1. Content of article 10	(a) The factors listed in article 10 should be recast as requirements, and an IdM system must satisfy each requirement in order to be considered reliable.[152] (b) Article 10 should specify how each factor is to be assessed and how compliance should be documented.[153] (c) There are numerous factors that are relevant to reliability, and it is not appropriate for the draft provisions to attempt to list them.[154]
2. "Recognized international standards and procedures" for reliability (Article 10(1)(b))	(a) Such standards and procedures do not exist[155] or need clarification.[156] (b) There is no body which sets such standards and procedures.[157]
3. Rules on governance (Article 10(1)(b)(i))	(a) The text should specify that these rules include (i) verification of the applicant's means of identification, (ii) in-person presence of the applicant, and (iii) face-to-face verification.[158] (b) The concept of "governance" should be clarified.[159]

[145] UINL.
[146] Singapore.
[147] EU (also for article 23(1)(h)).
[148] Lebanon, Singapore, UINL.
[149] Singapore.
[150] Denmark, EU, Switzerland, United Kingdom.
[151] Denmark, EU, United Kingdom.
[152] EU.
[153] Denmark.
[154] United States.
[155] United States (also for article 23(1)(b)).
[156] Denmark.
[157] Denmark, United States (also for article 23(1)(b)).
[158] China.
[159] CIETAC.

G. Article 11 – designation of reliable IdM systems

1. Synthesis of comments in response to specific questions

The template contained no specific questions on article 11.

2. Synthesis of other comments on article 11

Issue	*Synthesis of comments*
1. Process for designating reliable IdM systems	(a) Further guidance and clarification is needed on the designation process.[160]
2. "Recognized international standards and procedures" for determining reliability (Article 11(3))	*See issue 2 for article 10.*

H. Article 12 – liability of IdM service provider

1. Synthesis of comments in response to specific questions

Question	*Synthesis of comments*
1. Which option for article 12 is preferable?	(a) Option A.[161] (b) Option B.[162] (c) Option C.[163] (d) None is preferable.[164]
2. If option A is preferred, is it necessary to include such provision on liability at all?	(a) A provision on liability would still be necessary or desirable.[165] (b) A provision on liability would not be necessary.[166]
3. If option B or option C is preferred, is it necessary to include a provision waiving liability for public IdM service providers?	(a) A waiver of liability for public IdM and trust service providers would not be necessary.[167] Articles 12(2) and 25(2) (option C) leave this issue to the applicable law.[168] In any case, it should not be possible to limit liability in case of death or injury to person.[169] (b) A waiver of liability for public IdM and trust service providers would be necessary.[170] (c) Such a waiver would probably be too broad and should only be decided once the liability regime under existing law is known.[171]

[160] Denmark.
[161] Lebanon (also for article 25), Switzerland (also for article 25).
[162] UINL (but option A for article 25).
[163] Argentina (only for article 25), Denmark (also for article 25), EU (also for article 25), Russian Federation (also for article 25), Senegal (also for article 25), Singapore (also for article 25), Ukraine (also for article 25), United Kingdom (also for article 25).
[164] United States.
[165] Lebanon (also for article 25, prefers option A), Switzerland (also for article 25, prefers option A).
[166] Argentina (only for article 25), Ukraine (also for article 25, prefers option C), United States (prefers none), UINL (prefers option B but option A for article 25).
[167] UINL, Denmark (also for article 25), EU (also for article 25), Senegal (also for article 25), Ukraine (also for article 25), United Kingdom (also for article 25).
[168] EU (also for article 25), United Kingdom (also for article 25).
[169] United Kingdom (also for article 25).
[170] CIETAC (also for article 25).
[171] United States.

Question	*Synthesis of comments*
4. If option B or option C is preferred, is it desirable to treat differently the liability of an IdM service provider arising from the use of an IdM system that is designated pursuant to article 11? If so, how?	(a) The draft provisions could limit the liability of IdM and trust service providers operating a designated IdM system.[172] (b) The draft provisions could establish a presumption of fault on the part of IdM and trust service providers operating a designated IdM system or offering a designated trust service.[173] (c) The draft provisions could establish a presumption of no fault on the part of IdM service providers operating a designated IdM system.[174] (d) Article 12 should only apply to IdM and trust service providers operating a designated IdM system or offering a designated trust service.[175] (e) This should be treated as bracketed language.[176]

2. Synthesis of other comments on article 12

Issue	*Synthesis of comments*
1. Accommodating multiparty IdM systems	(a) The draft provisions should also deal with the liability of other participants in a multiparty IdM system (e.g., enrolment agents, attribute providers, authentication providers).[177]
2. Options for limiting the liability of IdM service providers	(a) The IdM service provider should not be liable to a relying party if the damage was caused by reliance of the relying party on a compromised credential, and the relying party should have known that the credential was compromised.[178] (b) An IdM or trust service provider should not be liable to a subscriber for damage resulting from an insufficient level of assurance if (i) the subscriber knew that the level of assurance was insufficient, or (ii) the subscriber did not perform a sufficient risk assessment to determine the required level of assurance.[179]
3. Desirability of addressing liability	(a) Liability will ordinarily be addressed in the rules governing the IdM system and will therefore vary depending on the type of IdM system.[180] (b) Further discussion on the liability regime under existing law (including the extent to which the parties are able to apportion liability among themselves under contract) is needed.[181] *See also issue 2 for article 3.*

[172] Singapore (also for article 25).
[173] EU (also for article 25).
[174] United Kingdom.
[175] Denmark (also for article 25).
[176] United States.
[177] Argentina, United States. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, p. 12).
[178] United States.
[179] United Kingdom (also for article 25).
[180] United States. See also comments submitted by the World Bank (A/CN.9/WG.IV/WP.163, pp. 12-13).
[181] United States (also for article 25).

Issue	*Synthesis of comments*
	(c) Liability issues are very complicated and it may be difficult to reach consensus.[182]
4. Terminology	(a) Option C for articles 12 and 25 should refer not only to the IdM or trust service provider being "liable for damage" but also to it bearing the "legal consequences" for failing to comply with its obligations.[183] (b) The concept of "legal consequences" in option B for articles 12 and 25 should be clarified.[184] (c) The term "damage" in option C (article 12(1)) is assumed to mean "harm".[185]
5. Nature of liability	(a) The draft provisions should specify that the liability of IdM and trust service providers may be civil or criminal in nature. Wilful negligence of an IdM or trust service provider in complying with its obligations may engage criminal liability.[186]

[182] CIETAC.
[183] Russian Federation (also for article 25).
[184] United States (also for article 25).
[185] United States.
[186] Madagascar (also for article 25).