United Nations A/CN.9/1113

General Assembly

Distr.: General
30 May 2022

Original: English/French

United Nations Commission on International Trade Law
Fifty-fifth session
New York, 27 June–15 July 2022

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

Compilation of comments by Governments and international organizations

Contents

V.22-03487 (E) 030622 060622

I. Introduction

1. At its forty-ninth session, in 2016, the Commission had before it a note by the secretariat on legal issues related to identity management (IdM) and trust services (A/CN.9/891) that summarized the discussions during the UNCITRAL Colloquium on Legal Issues Related to Identity Management and Trust Services, held in Vienna on 21–22 April 2016. The Commission agreed that the topic of IdM and trust services should be retained on the work agenda of Working Group IV (Electronic Commerce) (A/71/17, para. 228). Accordingly, Working Group IV started consideration of that topic at its fifty-fourth session (Vienna, 31 October–4 November 2016).

2. At its fifty-fourth session, in 2021, the Commission expressed its satisfaction for the progress made by Working Group IV towards completion of its work on legal issues related to IdM and trust services and encouraged the Working Group to finalize its work and to submit it for its consideration at its fifty-fifth session, in 2022.

3. At its sixty-second session (Vienna, 22–26 November 2021), Working Group IV concluded its third reading of the draft provisions on the use and cross-border recognition of IdM and trust services and their explanatory note. At that session, the Working Group requested the secretariat to revise the draft provisions and the explanatory note to reflect its deliberations and decisions and to transmit the revised text to the Commission, in the form of a model law, for consideration at its fifty-fifth session, in 2022. The secretariat was also asked to circulate the revised text to all Governments and relevant international organizations for comment, and to compile the comments received for the consideration of the Commission (A/CN.9/1087, para. 11).

4. The revised text of the draft Model Law with explanatory note has been compiled and transmitted to the Commission (A/CN.9/1112). By a note verbale dated 21 April 2022, the Secretariat transmitted that revised text to States and to invited international organizations for comments.

5. The present document reproduces the comments received by the Secretariat on the draft Model Law and the explanatory note. Comments are reproduced as received by the Secretariat with some formatting changes. Comments received by the Secretariat after the issuance of the present document will be published as addenda thereto in the order in which they are received.

II. Compilation of comments

A. World Bank

[Original: English]
[21 April 2022]

1. As requested by the Working Group, the World Bank is pleased to submit the following comments on the Draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (A/CN.9/1112), specifically on the Draft Explanatory Note (annex II), on the occasion of the 63rd session of the meeting of Working Group IV in New York (hybrid in-person and online session) from 4–8 March 2022. References in these comments are to paragraphs in the Explanatory Note.

2. The World Bank believes that these additions are both aligned with and support the Working Group discussions and decisions. These clarifications are not intended to reopen any discussions on decided issues, but rather will contribute to a more coherent reading of the Model Law, and thereby enhance its adoption.

3. These comments are divided into two parts: first, **(1)**, presenting the relevant portion of the Explanatory Note text as is, with the proposed additions in brackets and underlined (i.e., the proposed text would be indicated as follows: "[for example]") as well as with the reinsertion of removed text in brackets and italicized (i.e., the

proposed text would be indicated as follows: "[*for example*]"); and second, **(2)**, the motivations for each of the propositions, in order of their appearance in the Note:

1. Existing Explanatory Note text with the proposed additions:

47. Identification is the process of [uniquely] distinguishing a person by reference to information relating to that person [within a particular context] (i.e., attributes). That information may be collected or observed. Identification involves verifying that collected or observed attributes match an "identity" previously established for the person being identified. Identification in this sense is often carried out in response to a person claiming a particular identity and presenting attributes for its verification. [*Identification is particularly important to build trust in online transactions.*[1] *At its core, identification involves verifying that collected or observed attributes match an "identity" previously established for the person being identified*] [("identity proofing" when referring to establishing the unique identity of a person; and "electronic identification", or what in some jurisdictions has been referred to as "authentication", when referring to the subsequent verification of credentials attesting to that identity in a particular transaction).]

48. Accordingly, under the Model Law IdM involves two distinct stages (or phases) – first, issuance of identity credentials to prove uniqueness [(i.e., data that may be presented for electronic identification)]; second, the presentation and verification of those credentials by electronic means [in connection with a particular transaction (i.e., electronic identification)]:

(a) The first stage of IdM involves the collection of attributes that may comprise the person's "foundational identity" (i.e., [basic] attributes that are usually recorded by government agencies in civil registration and vital statistics systems [or foundational identification systems] for natural persons and company and business registries for legal persons). These attributes may be presented in the form of government-issued [or government-recognized] credentials (e.g., a certificate of registration) verified with the issuing agency. [The extent to which the credential might be recognized is dependent upon a consideration of the purpose for which that credential was issued.] This process, which may be carried out [either via electronic means or] "offline"[,] based on physical credentials presented in-person, results in the issuance of credentials to the person;

2. Motivations for each of the proposed additions to the Explanatory Note:

2.1 First, the proposed addition (in para. 47) of "uniquely" and "within a particular context" reflects the notion, already agreed to by the Working Group, that the nature of the identity credential is a reflection of the individual's uniqueness within a given context. While some identity credentials might be used and accepted on a relatively general basis, any given identity credential might not necessarily either effectively or validly identify an individual in another context – indeed, many credentials are not ever intended to be used widely. This logic is reflected and highlighted in the work of the Working Group and secretariat and was agreed to by the Working Group, having been precisely incorporated into the text of the Model Law, which states in the definitions of article 1(d) as follows: "*'Identity' means a set of attributes that allows a person to be uniquely distinguished within a particular context*" (*emphasis added*). Therefore, the proposed language – "uniquely" and "within a particular context" – should equally be included in the Explanatory Note, thereby assuring coherence between the Model Law and the Note.

2.2 Second, in paragraph 47, the World Bank requests that language referring to building trust be restored. The language in question – "*Identification is particularly important to build trust in online transactions*" – is important to developing a complete and larger understanding of the motivations underlying the Model Law and

[1] World Bank. 2021. *World Development Report 2021: Data for Better Lives*. Washington, D.C.: World Bank. https://www.worldbank.org/en/publication/wdr2021.

specifically needed to highlight the purposes which electronic identification (as opposed to trust services) is intended to serve. As the title of the Model Law implies, trust in online transactions is at the heart of the matter, and trust-building is a key element and objective of the entire work. However, due to the bifurcated (if parallel) structure of the Model Law, the importance of trust-building deserves reiterating specifically with regard to IdM (as opposed to with regard to that part speaking to trust services). This language mirrors the conversations that the Working Group has had throughout its sessions with regard to "reliability". The World Bank, among others, has raised this very matter in several Working Group sessions, and has referred the Working Group to its flagship report on the matter, the *World Development Report 2021: Data for Better Lives*.[2] The World Bank would equally request a footnote referencing this report at the end of this sentence: as the World Bank is a United Nations specialized agency, inclusion of an institutional output would not be inappropriate, and would match the Note's use elsewhere of outputs by United Nations bodies – in footnote 1 of the Note refers to a report by UNCTAD.

2.3 Third, in paragraph 47, the World Bank would like to see language, immediately following that discussed in paragraph 2.2, above, first, restored, and, second, complemented, to read: "*At its core, identification involves verifying that collected or observed attributes match an 'identity' previously established for the person being identified* ('identity proofing' when referring to establishing the unique identity of a person; and 'electronic identification', or what in some jurisdictions has been referred to as 'authentication', when referring to the subsequent verification of credentials attesting to that identity in a particular transaction)". The World Bank believes that it is important to include the removed language and supplemented because it would, first, help to avoid possible confusion, and, second, to gap-fill between different notions of what constitutes "identity". On this point, and before explaining the logic underlying this proposal, the World Bank would like to reiterate its support for the Working Group's decision to use the term "electronic identification" as opposed to "authentication" in the Model Law to describe the second phase of the identity management process, and to stress that the Model Law represents an important step towards the achievement of the Sustainable Development Goals.[3] It was, however, the understanding of the delegation of the World Bank that, after extensive discussion on the issue in previous sessions, the Working Group had agreed to make reference to the use of the term "authentication" in the Explanatory Note in order to ensure clarity of the use of the term "electronic identification".

The World Bank is making this proposal based on its extensive in-country experiences in financing digital ID projects, in which use of the term "identification", regardless of the qualifier, can be understood to indicate something other, or at least more limited, than what is meant here in the text of the Model Law. As noted in the deliberations of the Working Group, everything has a cultural meaning, and, regardless of how a term is defined, that underlying cultural meaning ought to be respected. For instance, understandings in the French language and in the administrative systems following this tradition create a robust, legal understanding of what constitutes "identity" and, by extension, the process of "identification". That understanding is multidimensional and multilayered, and fundamentally of relational nature, with mandatory attributes used to define identity including date- and place- of birth, parentage, filiation, profession, among others. This conception goes to the understanding that a person is not identified in a vacuum but, in order to be "identified" and to have an "identity", must be correlated and linked to certain attributes of the individual. The Model Law, however, countenances a great diversity of instances where many of these associated attributes are neither necessary nor even necessarily warranted. Indeed, in many of the contexts of electronic, commercial exchange, often only the most minimal and basic of attributes are required to identify an individual. Accordingly, it is precisely for reasons of ease of comprehension in such contexts – that is, where the term "identification" has a certain, more robust and

[2] Ibid.

[3] Sustainable Development Goal target 16.9. https://sdgs.un.org/goals/goal16.

established cultural and legal understanding and might implicitly lead readers coming from such contexts towards a meaning other than that intended by the Model Law – that the World Bank is proposing this additional language.

The World Bank believes that it is essential to make these clarifications about "authentication" in the Explanatory Note in order to avoid confusion. That risk is one that the World Bank has observed in connection with its in-county operations.

2.4 Fourth, and as with the point described in paragraph 2.1, above, the proposed insertion (in para. 48) of "in connection with a particular transaction (i.e., electronic identification)" is meant to reaffirm that the presentation and verification of identity credentials by electronic means is context-specific, and that the application is for the purposes of electronic identification (i.e., the second stage of the identification process).

2.5 Fifth, the proposed addition (in para. 48(a)) of the word "basic" as a qualifier for attributes, and "foundational identification systems" as a complement to "civil registration and vital statistics systems" – is an extension of the logic made in paragraph 2.3, above. These insertions are consistent with the language and approach of the Working Group, including the language used by the Secretariat in its documents, and the language that has been internationally agreed to and duly adhered to by the agencies in the United Nations family. Addressing each in turn:

2.5.1 First, insertion of the term "basic" is important, as the word is an essential qualifier that makes clear what the Explanatory Note already says, but which could easily be misinterpreted. The Explanatory Note already speaks of "the collection of attributes that may comprise the person's 'foundational identity'". A foundational identity does not require more than basic attributes in order to be foundational.

2.5.2 Second, insertion of "or foundational identification systems" is imperative for the successful and widespread adoption of the Model Law. As observed in paragraph 2.5.1, above, the Explanatory Note already speaks of "foundational identity", and the Working Group and the Secretariat have made repeated use of this term in their deliberations and discussions, contrasting it against "transactional" or "functional" identity credentials.[4] Although the matter of foundational identification might itself be considered beyond the scope of work, that does not mean that the use of, or recourse to, well-accepted industry terminology might not be had, when such terminology is appropriate.[5] The Note's present construction gives rise to the erroneous interpretation that civil registration and vital statistics systems are the only source of the creation of foundational identity. As the descriptor of "foundational identity" is already used in the text, as well as in the reports prepared by the Secretariat and accepted by the Working Group, this proposed addition language of "or foundational identification systems" both clarifies an existing ambiguity and is consistent with understandings of the Working Group.

2.6 Sixth – and, again, based on the World Bank's in-county operational experience – the proposed addition (in para. 48(a)) of "or government-recognized" to the existing reference to "government-issued credentials" is important as a

[4] See especially A/CN.9/WG.IV/WP.153 (noting that "Primary determination of identity, or foundational identity, relates to attribution of identity in the context in which the entity originates and at the time of its origin" (para. 8), and continuing that, "In some cases, reliable identification of the signatory may be based on the use of an identity credential and authentication process that establishes identity on the basis of foundational identity credentials. Hence, legal recognition of foundational identity across borders and across identity management systems may be useful or even necessary"). See also A/CN.9/WG.IV/WP.158 and A/CN.9/WG.IV/WP.163.

[5] See, e.g., A/CN.9/WG.IV/WP.153, at FN.7 (noting "In discussing the definition of 'identity', the Working Group may wish to consider whether the requirement of uniqueness is needed for the purposes of the Working Group's work taking into account that (a) uniqueness is a quality of foundational identity, and (b) foundational identity is currently excluded from the scope of work").

government may not issue the identity credential. Indeed, quite frequently, governments delegate the task of elaborating and issuing identity credentials to the private sector. As such, the proposed language is deemed essential to the overall coherence and applicability of the Model Law and is considered an important addition to the Explanatory Note.

2.7 Seventh, the proposed addition (in para. 48(a)) of "The extent to which the credential might be recognized is dependent upon a consideration of the purpose for which that credential was issued" is intended to connect with the logic of the point made in paragraph 2.4, above, where the presentation and verification of identity credentials by electronic means is construed as context specific.

2.8 Eighth, the proposed addition (in para. 48(a)) of "'either via electronic means' or" is also intended as a complement to the existing language in the Explanatory Note of "offline". This addition is important on the basis of physical identity credentials presented in-person, where there may be some form of offline verification – such as by means of visual inspection – but where there may equally be some form of electronic verification, such as through the connecting back to a backend system, or merely a scanning of an element of the physical credential, such as a QR code, which might not necessarily link back to a backend system but which might read the (secured) QR code to look for a digital signature. As such, there may be contexts where an electronic means of verification of physical identity credential occurs, which are not entirely or appropriately captured under the descriptor of "offline" processes. The addition of the proposed language is considered important to a coherent and complete reading of the Model Law.

2.9 Finally, and on an editorial side, the World Bank proposes that any remaining references to "privacy and data protection" be inverted to read "data protection and privacy", as doing so would more appropriately situate "privacy" within the context of "data protection", as opposed to implicating the larger, fundamental right to privacy. This formulation was already agreed in the text of Model Law, as was confirmed by the Secretariat in this last session.

The delegation of the World Bank believes that these insertions improve the coherence and clarity of the Explanatory Note, and naturally flow from the language and logic of the Working Group, including the language used by the Secretariat in its documents. Without a complete, clear and coherent reading of the Model Law, as supported through the Explanatory Note, the extent to which the Model Law would be applied and adopted risks being significantly limited.

B. Austria, Belgium, Czechia, France, Germany, Poland, European Union, Union Internationale du Notariat Latin and Conseil des Notariats de l'Union Européenne

[Original: English]
[25 May 2022]

I. Context and issue

1. During its sixty-third session, the Working Group deliberated on last pending issues concerning the draft model law on the use and cross-border recognition of identity management (IdM) and trust services. We believe that we found a consensus on most of the pending issues during this session.

2. Nevertheless, our delegations would like to draw the attention of all UNCITRAL delegations on articles 9 and 10 on Identity management as well as on articles 16–21 and 22 on Trust services, concerning which **no consensus was reached during the working group**. It currently remains two divergent positions on these articles.

3. In this context, the **document** A/CN.9/1112 transmitted by the secretariat to the Commission for consideration at its fifty-fifth session **does not reflect the**

deliberations and decisions of the working group during the last sessions. Especially, this document only includes one position, on which we have expressed our difficulties several times during the last sessions of the working group. We also regret that this position is not put into square brackets – at the minimum and which is usual in international negotiations – despite the fact that the working group does not take decision on these articles.

4. By these comments, we wish to recall the background of this file (point II) and explain our position on the principle of reliability of the method (III) as well as changes requested in the draft Model Law and the Explanatory Note (point IV).

II. Background

5. As we can read in the report of the sixty-first session (document A/CN.9/1051), there were discussions (paras. 45–51) on articles 16–21 and 22 (articles on Trust services, mirrors of articles 9 and 10 for Identity Management). We can especially read that **there is two different positions and that the working group does not take a decision on these articles, as no consensus was reached**.

6. Our delegations were therefore really surprised to see in the document prepared by the secretariat for the sixty-second session in November 2021 (document A/CN.9/WG.IV/WP.170) that articles 9, 10, 16–21 and 22 were modified by the secretariat in order to only insert the alternative proposal, without brackets, which had been suggested by a few other delegations (despite the fact that no consensus was reached), as if the working group had an agreement, and without taking into account the position of our delegations notably. As we can see in the report of this sixty-second session (document A/CN.9/1087), our delegations contested this wording in articles 9 and 10 (paras. 38–46, especially paras. 39–40 of the report) and there was no consensus/decision reached by the Working Group during this sixty-second session. In this regard, we were stupefied by a declaration of one delegation during the last sixty-third session, who said: "*It was added that the balance of article 10 had not been identified as a pending issue at the sixty-second session, and that the Working Group should exercise caution in reopening issues at such an advanced stage of deliberations.*" (document A/CN.9/1093). We were also **surprised that the document** A/CN.9/1112 **prepared by the secretariat does not reflect the two divergent views**, in conformity with the discussions held during the sixty-second session of the Working Group.

7. Our delegations have repeated with insistence our position during the last sixty-third session of the Working Group. We also made a joint declaration during this session to regret this situation and to ask the secretariat to reflect the two positions in the text to transmit to the Commission in July. Unfortunately, this was without effect.

8. In this context, we have also proposed to amend some part of the draft summary of the sixty-third session of the Working Group for the sake of transparency and in order to reflect more exactly the interventions made by our delegations. Our changes have been objected by the delegation of the United States of America, without justifications received. Again, we regret the objections raised by this last delegation and also contest this manoeuvre, reason why the document A/CN.9/1093 is not the Report of the Working Group but only the Summary of the Chair and the Rapporteur on the work of Working Group IV (Electronic Commerce) at its sixty-third session.

III. The principle of reliability of the method

9. The fact that identification (or functions related to trust services) is only useful if it is reliable, is a corner stone of the project and is in principle shared by all delegations (see current version of the Explanatory Note, para. 143).

10. However, the current text (document A/CN.9/1112) does not safeguard this principle anymore.

11. First of all, article 9 no longer contains the information, that a requirement for identification is met if a **reliable** method is used. This deprives article 9 of its core content and makes it redundant. We can make the same remarks for articles 16 to 21.

12. Secondly, article 10(1)(b) in the current version of the text undermines the principle of reliability.

13. Article 10(1)(b) allows an identification with a method which has "*Proven in fact to have fulfilled the function described in article 9*". In contrast to article 10(1)(a), a method which has only "*Proven in fact to have fulfilled the function described in article 9*" is not necessarily reliable (see para. 143 in the current Explanatory Note). Article 10(1)(b) is therefore in strong contradiction to the consensus within the Working Group, that all methods under article 9 should be reliable. By introducing an identification in fact (art. 10(1)(b)) as an alternative to an identification via a reliable method (art. 10(1)(a)), the fundamental principle of reliability is circumvented.

14. It was claimed by other delegations that introducing article 10(1)(b) would prevent unnecessary court proceedings. However, in case of doubt, the only way to determine whether a method has "*Proven in fact to have fulfilled the function described in article 9*" is by letting a court decide on this issue. The so-called "safety clause" of article 10(1)(b) is thus not apt to prevent court proceedings.

15. Nevertheless, we do acknowledge that the fact, that a method fulfilled its purpose, can be important. As a compromise, we do therefore suggest to move article 10(1)(b) to article 10(2)(f). This way, it can be taken into account together with all the other relevant circumstances.

16. This proposition is also system neutral:

- Article 10(2) describes which circumstances can be taken into account to determine reliability, if reliability is determined *ex post*;
- Article 10(4) on the other side regulates that an *ex ante* designated method is always presumed to be reliable;
- Article 10(1) is system neutral and simply states that there is no abstract level or reliability, but that an identification only has to be "*as reliable as appropriate*", a concept the working group has always agreed on.

17. We can make the same remarks *mutatis mutandis* for article 22.

IV. Changes requested in the document A/CN.9/1112

18. To sum up our position, it should be ensured that the text of the Model Law and the Explanatory Note, reflects two main principles:

1. The method used to fulfil the function shall always be "reliable";
2. The model law should not suggest that the method could be assessed otherwise than either:
   a. By the authorities designated in the enacting jurisdiction (*ex ante* approach) or
   b. By a court as part of the review of the various factors listed in article 10(2) in the event of a dispute (*ex post* approach).

Furthermore, the particular legal consequences (presumption and reverse of burden of proof) should only benefit the method designated in the *ex ante* approach. These consequences should not benefit any method used in an *ex post* approach, and *a fortiori* not any method which has only "proven in fact to have fulfilled the function", when this method does not have to be reliable and when it is unclear who evaluates what is considered "proven in fact".

19. The following proposed changes aim at addressing these two principles (the changes are underlined: additions are marked with **bold text**, deletions with ~~strikethrough~~).

Annex I – Draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services

Article 9. Identification of a person using identity management

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

Article 10. Reliability requirements for identity management services

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

~~(a) A~~ **a**s reliable as appropriate for the purpose for which the identity management service is being used~~; or~~

~~(b) Proven in fact to have fulfilled the function described in article 9~~.

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

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

(b) Compliance of the operational rules, policies and practices of the identity management service provider with any applicable recognized international standards and procedures relevant for the provision of identity management services, including level of assurance frameworks, 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 identity management service;

(d) Any relevant level of reliability of the method used;

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

(f) Have proven in fact to have fulfilled the function described in article 9; and

(~~f~~**g**) Any relevant agreement between the parties, including any limitation on the purpose or value of the transactions for which the identity management service might be used.

3. (…).

Article 16. Electronic signatures

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

(a) To identify the person; and

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

Article 17. Electronic seals

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

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

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

Article 18. Electronic timestamps

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

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

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

Article 19. Electronic archiving

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

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

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

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

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

Article 20. Electronic registered delivery services

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

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

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

(c) To identify the sender and the recipient.

Article 21. Website authentication

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

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

(b) To associate that person to the website.

Article 22. Reliability requirements for trust services

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

~~(a) A~~ **a**s reliable as appropriate for the purpose for which the trust service is being used~~; or~~

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

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

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

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

(c) Any relevant level of reliability of the method used;

(d) Any applicable industry standard;

(e) The security of hardware and software;

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

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

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

(i) The purpose for which the trust service is being used; ~~and~~

(j) Have proven in fact to have fulfilled the function described in the respective articles 16 to 21; and

(~~j~~**k**) Any relevant agreement between the parties, including any limitation on the purpose or value of the transactions for which the trust service might be used.

3. (…).

Annex II – Explanatory Note to the Draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services

57. The ex ante approach ~~may~~ provide**s** a higher level of clarity and predictability on the legal effect of IdM and trust services **thanks to presumptions and reversal of the burden of proof**, including when used across borders. However, its governance presupposes the existence of an institutional mechanism, i.e., an entity competent for administering the designation process.

73. The Model Law, in line with the approach adopted in pre-existing UNCITRAL texts, goes beyond the mere reference to place of origin as a relevant factor for granting legal recognition to foreign IdM and trust services. More precisely, it requires ex post determination of reliability of foreign IdM and trust services on the basis of the same circumstances to be used for similar domestic IdM and trust services. It also provides mechanisms for ***ex ante*** designation of reliability of foreign IdM and trust services on the basis of the same circumstances to be used for similar domestic

IdM and trust services. In short, technical reliability, rather than place of origin, should determine whether legal recognition is to be granted.

111. Subparagraph (b) specifies that the fact that the IdM service is not a designated service does not prevent its legal recognition. In other words, subparagraph (b) gives equal legal recognition to IdM services that are ***ex ante*** designated and to those that are not designated **(subject to evaluation *ex post* by the judge)**, thus ensuring neutrality with respect to the approach chosen to assess reliability. However, subparagraph (b) does not imply that any IdM service uses reliable methods and therefore provides a sufficient level of assurance for electronic identification: in order to achieve that outcome, the reliability of the method used needs to be assessed according to articles 10 and 11, as the case may be.

134. The method used to fulfil the rule in article 9 must **be reliable and** comply with article 10, paragraph 1, i.e., be as reliable as appropriate for the purpose for which the IdM service is being used ~~or proven in fact to have fulfilled the function pursued with the use of the method~~.

138. Electronic identification may be used to satisfy a requirement to verify particular attributes of one person's identity, such as age or residence, as required by physical-based identification. In that regard, since the notion of "identity" is defined with reference to "context", which in turn determines the attributes required for identification, the successful identification of a person based on article 9 includes verification of the required attributes. The need to verify the relevant attributes is reflected also in the words "for that purpose". ~~Verification of particular attributes is not addressed by the provisions on reliability contained in article 10 as those provisions are concerned with the processes in managing identity credentials rather than with the attributes contained in the identity credentials.~~ **The provisions on the determination of the reliability of an identity management service laid down in Article 10 concern also the method applied for the verification of particular attributes if their verification is part of the electronic identification in scope.**

~~142. Paragraph 1(b) contains a clause aimed at preventing repudiation of the IdM service when it has in fact fulfilled its function. Repudiation occurs when a subject declares not having performed an action. For the mechanism contained in paragraph 1(b) to operate, the method, whether reliable or not, must have in fact fulfilled the identification function, i.e., associate the person seeking identification with the identity credentials. This provision is based on article 9(3)(b)(ii) ECC.~~

143. The Model Law ~~generally~~ requires the use of reliable methods, and paragraph 2(f) does not aim to promote the use of unreliable methods, or to validate the use of those methods. **Rather, it acknowledges the role that proven identifications tools can play when assessing by the judge the reliability of an identity management service.** ~~Rather, it acknowledges that, from a technical perspective, function (in the case of article 9, identification) and reliability are two independent attributes, and clarifies that under the Model Law identification may be achieved in fact or by using a reliable method. In other words, achievement of identification in fact pre-empts the need to ascertain the reliability of the method used.~~

148. Article 10 and article 11 refer to the notion of "level of assurance frameworks" or similar frameworks otherwise named. The level of assurance framework provides guidance to relying parties on the degree of confidence that they may place in the identity proofing and electronic identification processes and whether they are adequate for specific purposes. The Model Law neither defines levels of assurance nor requires them to be defined or used. **Nevertheless, such definition of levels of assurance could facilitate international recognition.**

187. The requirement for a paper-based signature is satisfied if a **reliable** method is used to identify the signatory of the data message and to indicate the signatory's intention in respect of the signed data message. The reference to the use of the **reliable** method "in respect of information contained in the data message" applies to both identification of the person and indication of the person's intention.

198. Article 19 deals with electronic archiving services, which provide legal certainty on the validity of retained electronic records. The **reliable** method used for electronic archiving shall provide guarantee as to the integrity of the archived electronic records as well as to the date and time of the archiving. Moreover, the information archived should be accessible according to the requirement for functional equivalence with the paper-based notion of "writing" (article 6(1) MLEC).

212. The MLES and several regional and national laws on electronic signatures distinguish between trust services based on **the evaluation *ex ante* or *ex post* of** the level of reliability that they offer. Specifically, these laws attach greater legal effect **(notably presumptions and reversal of the burden of proof)** to electronic signatures that **have proven in advance to** satisfy certain requirements **(*ex ante* approach)** and therefore are deemed to offer a higher level of reliability **(see para. 216 below)**. Moreover, certain laws may require that only electronic signatures offering a higher level of reliability may be designated. ~~This~~ **The same** approach has ~~not~~ been followed in the Model Law ~~and~~ **for** trust services ~~may be designated regardless of the level of reliability they offer~~.

213. Since identity credentials offering a high level of assurance may be used for trust services with different levels of reliability, there is no **necessarily** direct correlation between level of assurance of an IdM service and level of reliability of a trust service.

224. **For the moment, l**~~L~~evels of reliability defined in different jurisdictions may not match exactly. Such mismatch is a likely situation given the absence **at this stage** of universally agreed definitions of specific levels of reliability **(while waiting for emergence of international standards in this field)**. To overcome challenges to cross-border recognition arising from that **temporary** mismatch **but also for the future, when international standards will have emerged**, article 25 refers to the notion of "at least equivalent level of reliability", which includes levels of reliability that are the same or higher than the one required. That notion should not be interpreted as demanding compliance with strict technical requirements, which may result in obstacles to mutual recognition and, ultimately, to trade **but also failure to respect technology neutrality principle**.

225. The reference to "IdM system, IdM service or identity credential, as appropriate," aims to capture all possible aspects relevant for cross-border recognition of electronic identification. In practice, it may be preferable to focus on a specific IdM service to avoid recognizing all IdM services supported by an IdM system as equally reliable even though one or more of them may offer a lower level of reliability. Moreover, **we should not permit** recognition of identity credentials ~~should avoid not permit those credentials that have remained unchanged despite~~ **when** the IdM service used to issue them having been compromised.

C. International and Comparative Law Research Center

[Original: English]
[25 May 2022]

1. The International and Comparative Law Research Center (hereinafter, "**the ICLRC**") based these comments on the provisions of the following documents:

- A/CN.9/1093 – Report of Working Group IV (Electronic Commerce) on the work of its sixty-third session (New York, 4–8 April 2022);
- A/CN.9/1112 – Draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (hereinafter, "**Model Law**"), including the Explanatory Note (hereinafter, "**Explanatory Note**").

2. The comments contained herein reflect exclusively the expert point of view of the ICLRC as an observer in the UNCITRAL Working Group IV.

I. Regional context

3. For several years, the ICLRC has been following expert discussions in the Eurasian Economic Union (hereinafter, "**the EAEU**") about electronic commerce and electronic data interchange issues. Economies of the EAEU members have been growing rapidly due to the emergence of digital technologies and their introduction to the markets. The member States and the EAEU are currently working to identify efficient and commonly recognized approach to remove barriers to electronic data flows between the member States and to establish a comprehensive legal regime for digital transactions and cross-border recognition of electronic data records and documents in the EAEU.

4. We believe, the expert work of the UNCITRAL Working Group IV could offer useful guidance on cross-border identity management (IdM) and trust services, and working solutions much needed for the development of relevant legal framework in the Eurasian region.

5. In this regard, in order to serve as genuinely comprehensive guidance, we believe, the draft Model Law would benefit from further work and additional provisions regarding equivalence, reliability, and functionality of IdM and trust services. The comments below reflect the opinion of the ICLRC on possible approaches and point out several factors that could be taken into account to develop a vital international framework for IdM and trust services.

II. Minimum requirements

6. In our view, the European Union and the Council of Europe's approaches to data protection and IdM services could be used as best practices due to their efficiency and international recognition. These approaches set forth a certain minimum level of protection assuring users from different countries that their data is protected regardless of where exactly – within the digital single market – it is being processed. This "minimum requirements" approach does not levy an unnecessary burden on market players.

7. According to paragraph 114 of the Explanatory Note, the obligations contained in the Model Law are described in a technology-neutral manner as the implementation of the principle of technology neutrality in the context of IdM calls for minimum IdM system requirements that refer to system properties rather than to specific technologies. Yet for some reason, this "minimum requirements" approach apparently was not followed in article 10 of the Model Law, which forms the core mechanism for cross-border recognition of IdM services.

8. In our opinion, the requirements contained in article 10, paragraph 2 (a) and (b) of the Model Law can hardly be considered to be minimal, and may increase uncertainty for market players. It is almost inconceivable that it would be possible to "take into account all relevant circumstances and comply 'with any applicable recognized international standards and procedures relevant for the provision of IdM services, including the level of assurance frameworks"'.

9. Turning to what we consider best practices, it could be recommended to use a set of specific principles and (or) metrics that could serve as a test for the reliability of the method of identification (authentication). Such a test, in line with the principle of technology neutrality and "minimum requirements" approach, would increase certainty for the market players introducing this method of identification or this kind of IdM service to a market, and will make the level of protection transparent for users of such services.

III. Presumption of reliability

10. The current approach to the reliability of the method contains the presumption only about designated methods (art. 11), not about methods assessed ex-post (art. 10). This approach may cause uncertainty in the market and restrict market players from using methods that were not designated by competent authorities. Notably, no such

requirement exists in the area of electronic trade with regard to “traditional” proof of identity that is used in concluding contracts in paper form.

11. In order to avoid such uncertainty and promote openness and competitiveness on the IdM market, the ICLRC would like to propose to reconsider the current approach in article 10 of the Model Law and base it on the general presumption of reliability for any methods that are actually used for identification. This presumption could be turned down due to violations of principles set forth by the Model Law. These principles include lawfulness (the method is not prohibited by applicable law), transparency (the level of protection, process, and results of identification shall be visible to users), accountability (the service provider shall demonstrate the functionality and sustainability of its service), and security (the services provider has a set of information security measures in force preventing unauthorized access to the identity management system).

12. Accordingly, the ICLRC’s proposal for amendment of article 10 reads as follows:

“Article 10. Presumption of reliability for identity management services

1. For the purposes of article 9, the method used by an identity management service provider is presumed to be reliable, unless it is proven by [a person, organ or authority, whether public or private, specified by the enacting jurisdiction as competent] to be unreliable due to its unlawfulness, lack of transparency, or inability of identity management service provider to demonstrate the functionality, sustainability and security of the method.

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

(a) To the geographic location where the identity management service is provided; or

(b) To the geographic location of the place of business of the identity management service provider.”

IV. Guide to the enactment

13. The Model Law now does not come with a guide on the legislative reform that would be required to implement it. The process of implementation, especially on the international (though regional) level may be challenging, while uniformity should preferably be achieved not only in the legal texts but also in their application. We believe it would be important to continue experts’ work in this direction and provide the Model Law with the implementation guide.

D. Ordre des Avocats de Paris

[Original: French]
[25 May 2022]

1. At the outset, we wish to welcome this initiative to strengthen the security of international transactions concluded by means of electronic signatures, mutual recognition of which will be made possible by the legal basis that the draft text establishes. As is known, in Europe the adoption of such a regulation proved difficult from the time of the first digital package, in 1999 and 2000, until the adoption, in 2014, of the eIDAS Regulation (No. 910/2014), which entered into force only in 2016. The draft is ambitious but essential at the international level.

2. Concerned about individual freedoms, the Paris Bar Association welcomes the fact that articles 2 and 3 of the draft model law make it clear that the mechanism for the mutual recognition of digital identity cannot be implemented to the detriment of regulations governing the protection of personal data, nor can it be implemented without the individual’s consent to the use of an identity management mechanism.

3. Each year, in an increasing number of jurisdictions, the production of evidence in legal proceedings involves the use of "eDiscovery"-type tools. Lawyers have the benefit of professional confidentiality (or "legal privilege") in their communications with clients and are thus able to withhold such communications from proceedings. We suggest that, in the draft text, the identity management system should encompass lawyers in order to facilitate and strengthen the protection afforded by professional confidentiality in the digital environment.

4. Lastly, the technology covered by the draft model law is essentially based on the conventional electronic signature involving a trusted third party. Future work could also focus on the mutual recognition of blockchain (essential in smart contracts), which operates on the basis of a community in horizontal mode, without a trusted third party in the strict sense of the term.

E. Asian Development Bank

[Original: English]
[26 May 2022]

1. The Asian Development Bank (ADB) conveys its sincere gratitude to the Secretariat and UNCITRAL Working Group IV for inviting ADB to review and comment on the Draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services and the Explanatory Note (A/CN.9/1112).

2. ADB does not have any additional comments on the draft model law.

3. With regard to the explanatory note (annex II), ADB noted the following points for consideration by the Secretariat, Working Group IV and the Commission:

(i) Paragraph 48(a) discusses attributes which comprise the "foundational identity" of a natural person and legal person. To promote awareness of the attributes of an international organization amongst IdM service providers, Trust service providers and enacting jurisdictions, it may be beneficial to include the attributes of an international organization (i.e., an international treaty for an international organization) in paragraph 48(a);

(ii) The obligations of a Relying party are typically encompassed in contractual arrangements with an IdM service provider and Trust service provider and/or may be established under other laws/regulations and are not covered in the draft model law and explanatory note. It may be beneficial to include commentary on general obligations of a Relying party (i.e., safeguarding the private key, checking the status of certificates etc.) in the explanatory note.

4. ADB commends the Secretariat and UNCITRAL Working Group IV for its efforts in preparing the draft model law and explanatory note which addresses central components (use of IdM and trust services) necessary to facilitate and promote e-commerce activity.