United Nations A/CN.9/1113/Add.1

General Assembly

Distr.: General
14 June 2022

Original: English/Spanish

**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.22-03956 (E) 220622 230622

# II. Compilation of comments

## F. Bankers Association for Finance and Trade

[Original: English]
[27 May 2022]

1. BAFT (The Bankers Association for Finance and Trade) appreciates the opportunity to comment on the "Draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services".

2. BAFT is an international financial services industry association whose membership includes a broad range of financial institutions and FinTechs throughout the global community. As a worldwide forum for analysis, discussion, and advocacy in international financial services, BAFT's nearly 300 members provide leadership to build consensus in preserving the safe and efficient conduct of the financial system worldwide. BAFT member institutions see the digitization of international trade finance as a key industry priority, and Identity Management (IdM) is critical component for digitization to progress.

3. The need for the establishment of the IdM cuts across numerous facets of international transaction banking including trade finance, supply chain finance, payments, and areas of compliance such as Know Your Customer (KYC) and Anti-Money Laundering (AML). As such BAFT fully endorses UNCITRAL's efforts in formulation of the Draft Model Law.

4. In Global Transaction Banking, there are several lines of action whose objective is to provide this business with a fully digital ecosystem. Digitization holds great promise; however, it cannot be said that the rate of achievement and adoption has been satisfactory to date. It's clear that digitization will not suddenly occur in a "big bang" manner, but through complementary initiatives that allow solid progress.

5. The market needs clear rules to be able to advance digitization in day-to-day operations. In this regard, The Digital Standards Initiative (DSI)[1] was founded by the International Chamber of Commerce, the Asian Development Bank and the Government of Singapore to deal with issues related to standards and interoperability of platforms and relationships with FinTechs. In terms of legal support, it has established a road map to encourage governments to adopt specific legislation for digital business as promoted by the UNCITRAL Model Law on Electronic Transferable Records[2] (MLETR). BAFT is a participant in efforts to drive global adoption of MLETR. In addition to legal framework, the industry is working towards standards for interoperability In August of 2020 BAFT published the "Distributed Ledger Payment Commitment – Industry Best Practices"[3] to establish industry guidance on interoperable payment commitments executed on a distributed ledger.

6. The existing Draft Model Law provides the general framework for identity management and trust services; but avoids following an even minimum prescriptive approach. It clearly states that "Like earlier UNCITRAL texts, the Draft Model Law is based on principals of party autonomy, technology neutrality, functional equivalence and non-discrimination against the use of electronic means, subject to adjustments. The principal of party autonomy allows parties to a contract to choose the applicable rules with the limits of mandatory law. It is based on the acknowledgement that those parties may be in the best position to determine the most appropriate rules for a given transaction."

7. The Draft Model Law expects the identity management services will have reliable requirements as is required under article 10 but does not provide how the level of assurance framework should be developed. The Draft Model Law confirms

[1] ICC Digital Standards Initiative, March 2020.
[2] UNCITRAL Model Law on Electronic Transferable Records (MLETR) July 2017.
[3] BAFT: DLPC May 2020.

that the international dimension is essential to the use of identity management and trust services and more generally, of electronic services. However, the text confirms that there are two obstacles: (i) technical incompatibility leading to a lack of interoperability, and (ii) legal obstacles to cross-border recognition.

8. To provide direction in overcoming these two obstacles in particular, BAFT would support the direct reference by the Draft Model Law to the substantial amount of work and progress that has been made by the Global Legal Identifier Foundation (GLEIF)[4] in the implementation of the Legal Electronic Identifier (LEI). The Global Legal Identifier System is a regulatory endorsed system that provides a globally recognized and trusted electronic identification mechanism for legal entities. The Legal Entity Identifier (LEI) is a global standard (ISO 17442) that connects key reference information that enables clear and unique identification of legal entities. At the recommendation of the G20 in 2011, GLEIF, a not-for-profit Swiss Foundation was founded by the Financial Stability Board. Its activities are overseen by 65 regulators and 19 observers in the Regulatory Oversight Committee from more than 50 countries.

9. The publicly available LEI data pool can be regarded as a global directory which greatly enhances transparently in the global marketplace. The LEI is a broad public good that should be leveraged to ensure technical compatibility at the national and international level.

10. The Draft Model Law aims for the harmonization of rules through legislation. This approach will result in a plethora of national technical standards meaning no interoperability and a drain on resources trying to parse and make sense of heterogenous data. The use of a multitude of identifiers and underlying national technical standards can hinder the ability to identify each party in electronic transactions in a reliable, homogenous, and comparable manner. Therefore, while UNCITRAL might want to avoid any technological preference and keep its technology neutral stance, it should consider including the LEI in the draft text as the underlying identifier to facilitate legal entity identification and verification across borders. The Global LEI System is not a technology choice. It is a public good envisioned by the Group of 20 (G20) and realized by the Financial Stability Board (FSB).

11. Given the LEI reference data already includes the local registration number of the entity, address information, timestamp on when the data was last updated, information on which data fields were updated, it has the potential to promote uniformity of entity data on a global basis.

12. The Draft Model Law already recognizes that uniform rules may improve efficiency by promoting acceptance of the result of the application of IdM and trust services across systems; lower transactions costs by facilitating compliance with regulatory requirements; increase legal predictability and certainty of electronic transactions on the basis of a common treatment of issues, including through cross-border recognition mechanisms; and contribute to bridging the digital divide through easier availability of common solutions.

13. In the event there will be divergent approaches, article 27 suggests that Cooperation could facilitate an agreement on common definitions of technical standards, including levels of assurance and levels of reliability. However, competing national interests might cause bottlenecks, at best delays, in reaching an agreement on the required technical standards and other underlying data quality framework. UNCITRAL's leadership in setting the LEI as the prevailing identifier for legal entity identification can speed up the implementation process of electronic identification across borders and leverage a system that was established by regulators to address the shortcomings of national/regional/private identification schemes. As a proven and

[4] GLEIF (www.gleif.org).

functioning system, the LEI provides an interoperable and technically agnostic solution.

14. Digital transformation in global transaction banking is capable of reducing costs, improving efficiency, better regulatory controls with less risk and collaborative opportunities for stakeholders in the global economy. The creation and adaptation of IdM is a critical first step in the digitization process. The LEI is the only global standard for legal identity identification which is why BAFT endorses its inclusion in the text of the Draft Model Law.

## G. Plurinational State of Bolivia

[Original: Spanish]
[27 May 2022]

The following comments and observations on the draft model law have been submitted by the Telecommunications and Transport Regulatory Authority of the Plurinational State of Bolivia for consideration.

*Article 6. Obligations of identity management service providers*

Comment/observation:

It is recommended that it be considered an obligation to ensure the online availability and correct operation of an electronic identity or electronic signature validation system that makes it possible to verify the identity of the signatory and the validity of the chain of trust of the authorized certifying entity in the country of origin.

*Article 16. Electronic signatures*

Comment/observation:

It is recommended that consideration be given to the establishment of a mechanism for detecting any alteration to the data message and ensuring its authenticity, integrity and non-repudiation.

*Article 17. Electronic seals*

Comment/observation:

The authenticity, integrity and non-repudiation of the data message, as well as its legal and evidential validity, should be ensured in accordance with the regulations of the country where the identity management service provider is based.

## H. Islamic Republic of Iran

[Original: English]
[30 May 2022]

### 1. Scope of Application

**The use and cross-border recognition of identity management and trust services**

1. **Issue:** Pursuant of the mandate of UNCITRAL to harmonize and modernize the law of the international trade and in light of the task given to the working group IV to remove barriers in international electronic commerce, the Islamic Republic of Iran is of the view that the scope of the application of the model law is so broad and needs to be limited only to international area and circumstances involving a foreign fact element. In other words, in our understanding, in cases of domestic use and recognition of IdM and trust services, when no foreign element is included and all the participants involved in the life cycle of IdM and trust services are in the same country, it is expected that internal law of States govern the situation and regulate their domestic matters.

**Proposed solution**

2. It is recommended to restrict the scope of the model law to the cross-border use and recognition of IdM and trust services and to clarify that this instrument does not aim to intervene in national infrastructures related to IdM and trust services established in member states or to prevail over their national law governing their domestic matters. At the same time, we note that there can still be room for enacting jurisdictions to extend the applicability of this instrument to their domestic matters only if they wish to.

**Trade-related services**

3. **Issue:** With regard to the term "trade-related services" in article 2, it should be noted that despite the explanation in paragraph 95 of the explanatory document, in our understanding, this term is still vague and not easily identifiable by users and could be interpreted broader than what was envisaged under the model law or could inappropriately cover all the active systems of a country in the field of IdM and trust services which are not necessarily related to trade.

**Proposed solution**

4. The model law is recommended to focus on the situations encountered in the commercial activities. Nonetheless**,** the explanatory note could clarify that "nothing in the model law should prevent an enacting state from extending the scope of the model law to cover the use and cross-border recognition of the IdM and trust services in the context of trade-related services".

## 2. Protection of sovereignty and public policy of States

5. **Issue**: our delegation expresses its concern regarding the implicit implications of this model law on the matter of sovereignty of States whose nationals or businesses are users of cross-border IdM and trust services. In order to understand this concern, it may be sufficient to look at the reality of the market from the perspective of developing countries and look at how all relevant sectors of such countries have been dominated by global digital corporations located in a few leading digital countries which are providing their services to worldwide subscribership. Furthermore, involvement of digital service providers in the field of identity management services, when they had not been previously entrusted with this task by the relevant government, and particularly when attributes collected by them are closely linked to the foundational identity of persons, not only could be irrational and leads to untrusted results, but also due to the exclusive competence of States relating to the whole life cycle identity management of their citizens, could result in interference in their sovereign functions. This phenomenon also runs the risk of losing data, technology and cyber sovereignty of the developing countries and also loss of protection offered by their mandatory law to their citizens. Detrimental consequences of such practice become more apparent if one looks at the subordinate position of developing countries and the great pressure they are facing at global trade forums to opt in to the dominant global digital economy model of a handful of countries, home to most of the giant digital corporations. Therefore, the Islamic Republic of Iran is of the strong opinion that if developing countries are to benefit from the work of international organizations, first they should be able to safeguard their sovereignty and public policy. Against this backdrop, we believe that the provisions of the model law on the use and cross-border recognition of IdM and trust services, lack an explicit reference to protection of sovereignty of States, equality and non-interventions in matters which are exclusively within their domestic jurisdiction.

6. Of equal importance is the preservation of public policy of enacting States. Nowadays cross-border data flows and access of foreign service providers to data of nationals and businesses of other countries, have turned to a main public policy concern of many developing states. Unlike earlier UNCITRAL texts (for example, articles 6, 7, 8, 11, 12, 15 and 17 of the Model Law on Electronic Commerce), there

is no procedure available under this model law to limit the scope of the instrument or the effects of any of its articles if necessary, in particular, for the purposes of public policy of enacting States. in our view since the application of this model law may involve various issues of public policy which are to be left to each individual State, a degree of flexibility should be allowed to enable the courts of the enacting State or authorities responsible for the application of the Model Law to deny or nullify the legal effects resulting from the use of a foreign IdM or trust services on the basis of mandatory reasons including of their public policy.

**Proposed solutions**

7. This instrument should explicitly clarify that the model law should be carried out with respect to the principles of sovereignty of States, equality, and non-interference in their domestic matters. Moreover, this instrument shall not authorize foreign IdM/trust service providers to carry out functions which are of sovereignty nature and are exclusively under the competence of national States in accordance with their domestic law. Similarly, it is expected to refer to this fact as a general principle and a key concept in section F of the explanatory note.

8. In order to respond to public policy concerns and in keeping with the position traditionally taken by UNCITRAL in its earlier texts, it is advisable to consider three options:

First: to include some provisions in the model law which would allow enacting jurisdictions to exclude the application or effects of certain articles of this instrument in situations which would be contrary to their public policy (there are several precedents to this effect in earlier UNCITRAL texts).

Second: it would be possible to allow a degree of flexibility in wording of some articles which mitigates their absolute application. For instance, adding a phrase to the wording of subparagraph 3 of articles 10 and 22 to this effect that: “in determining the reliability of the method, unless otherwise considered necessary by the adjudicating body, no regard shall be had…”. In the same vein, subparagraph 4 of articles 11 and 23 can be amended as follows: “in designating an IdM/trust service, unless otherwise considered necessary by the [person, organ or authority, whether public or private, specified by the enacting jurisdiction as competent], no regard shall be had…”. Furthermore, replacing “shall” with “may” in articles 25 and 26, not only would allow flexibility in wordings of the cited articles for the sake of public policy concerns, but also in light of unclear recognized international standards in articles 25(2) and 26(2), sounds more sensible.

Third: if the two options cited above were not possible, it would be helpful to provide a generic rule under the model law which refers to public policy exception and leaves the details to each enacting jurisdiction to specify them in their legislation.

### 3. Overriding Mandatory Law

9. **Issue:** Nowadays, IdM/trust service providers are offering their services to nationals and businesses located in other States. While this phenomenon is unavoidable and is an indispensable element of global electronic commerce, precautionary measures should be taken to ensure the compliance of service providers with relevant overriding mandatory laws to which no derogation is permitted.

10. The Islamic Republic of Iran is aware of the fact that this instrument does not affect the application of any mandatory law which might arise under the scope of its provisions and also mindful that the model law is not intended to interfere with the operation of the rules of private international law. Nevertheless, we strongly believe that there is a need for inclusion of a specific provision in this instrument which would give effect to mandatory law of the country where the IdM or trust service is provided or directed to. There are several reasons for taking this approach. The first reason relates to the access of service providers to data of citizens, businesses and organizations of the considered country. Bearing in mind that data is a valuable

source, which in in the case of extraterritorial services, may fall into the hands of foreign service providers, we believe that owners of data would be in the best position if it were to be placed under the protection regime and mandatory law of the country where the service is provided or directed to them. The second reason would be the absence of a clear rule under private international law which would specify the applicable law and overriding mandatory rules for protection of users of electronic commerce services. Although, there seems to be a general consensus regarding applicable law for protection of consumers in consumer contracts, ambiguity might arise in the protection of subscribers in contracts with digital service providers which may fall out of the consumer protection law. The third reason relates to the contractual imbalance between subscribers and service providers. Subscribers are often in asymmetric positions when it comes to entering into a contract in digital environment and consenting to its governing operational rules, policies and practices. In our view, the terms incorporated in the contracts between a subscriber and a service provider are mostly non-negotiated and usually contain applicable law or forum choice clauses, which are more favourable to service providers and to the detriment of subscribers. Lack of any reference or giving effect to the law of the country where the service is provided or directed to under this model law, would leave subscribers without the necessary protection they are entitled to.

**Proposed solutions**

11. Finding adequate safeguards and solutions for responding to the above-mentioned concerns require greater international collaboration and policy dialogue, with the full involvement of developing countries, which are most of the time receivers of cross-border services. Nonetheless, here are some of our suggestions:

- "Compliance of the operational rules, policies and practices of the IdM/trust service providers with the mandatory law of the place where their service is provided or directed to" should be an obligation for IdM/trust service providers to comply with in articles 6 and 14 and also as an element to consider for both determining the reliability of the method (ex post) in articles 10(2), 22(2), and designation of reliable services (ex ante) in articles 11(2)(a) and 23(2)(a) and as a standard to apply for granting legal effect in cross-border application of services in articles 25 and 26.

- For the reason of giving effect to the mandatory law of the place where the service is provided or directed to, there would be the need for imposing further obligations on service providers in articles 6 and 14, which could be further elaborated in paragraphs 113 and 175 of the explanatory note. For instance, cooperation of service providers with law enforcement authorities of the country where the service is provided or directed to (e.g. in matters of data protection or situations which could lead to tort or criminal liability including criminal prevention, investigation, detection or prosecution of offences) and, to that end, establishing a local presence or designating a representative in that country, modification of the terms of services and policies of service providers in accordance with the mandatory law of the place where the service is provided or directed to and so on. We believe that breaching these obligations should establish a basis for liability of IdM/trust services under articles 12 and 24.

- Obeying the above-mentioned obligations could facilitate achieving the goal of mutual recognition in articles 25 and 26. Therefore, it would be highly desirable for enacting jurisdictions to make their mandatory legal requirements available through exchange of information in article 27. Such information could enable those foreign service providers who wish to offer their services extraterritorially to modify their terms of services and policies with relevant regulations in advance. Details of such cooperation could be further elaborated in paragraph 234 of the explanatory note.

### 4. Voluntary Use of IdM and Trust Services

12. **Issue:** the Islamic Republic of Iran expresses its concern with respect to the inference of consent of a person by their conduct in article 3(2) of the model law. Although this is an established rule under previous UNCITRAL texts, we strongly feel that it would be unfair to people with poor knowledge of technology who are not necessarily aware of this fact that by signing up for a service or use a specific electronic commerce software, they are allowing the use of an IdM or trust service supported by that software. Furthermore, this situation could result in more negative effects if one looks at the "take it or leave it" position of subscribers in conclusion of digital contracts and sometimes their blind acceptance of the terms and conditions set forth against them, which specify the situations under which they could be presumed to have expressed their consent to the contractual terms and conditions. We would like to draw the attention of commission to this fact that although European consumers are protected against unfair standard contract terms through the Unfair Contract Terms Directive (93/13/EEC), it seems to us that there is no extensive legislation to this effect in non-European countries.

**Proposed solution**

13. We would like to suggest some flexibility regarding the inference of a consent a person to use an IdM/trust service by their conduct and to emphasize that this implied consent should be determined in a clearer and more predictable way. Therefore, it would be useful for member states to discuss it in more details and find solutions on how this requirement could be better met with respect to contracts in digital environment. In our view, it would be helpful if the implied consent of parties takes the form of a presumption which then could be rebutted in later stage.

### 5. Electronic Archiving

14. **Issue:** We are mindful of the fact that the model law does not affect law applicable to data privacy and protection. Nonetheless, since this area of law is so relevant in the case of electronic archiving, we believe that there is a need for emphasizing under article 19 that in electronic archiving due regard is to be had to the mandatory data privacy and protection law. With regard to the mandatory law relevant to this case, attention should be paid to the functions of cross-border IdM/trust service providers and their close reliance on data of citizens, businesses and organizations of other countries. in light of the fact that transfer of such data across borders constitutes a major public policy concern and may deprive subscribers, of the data protection regime to which they are entitled to, we believe that there should be a room under this model law for giving legal effect to data protection law of the country where the service is provided or directed to and subscribers receive such service in that location. The Islamic Republic of Iran, would like to attract the attention of the commission to this fact that although data subjects in Europe are protected under the broad territorial scope of European General Data Protection Regulation (GDPR), there may be no such similar extensive regulation elsewhere, particularly in the third world countries, which would be of obligatory nature for foreign service providers and could coerce them to respect to the protection law of the place where their service is provided or directed to.

**Proposed solutions**

15. To explicitly reiterate under article 19 that: "retaining documents, records or information in article 19 should be subject to appropriate safeguards with regards to data privacy and protection law". In order to respond to the second concern cited above, we suggest inserting a paragraph to this effect that electronic archiving would not deprive subscribers of cross-border IdM/trust services of the data protection regime to which they are entitled to under the place where the service is offered or directed to.

### 6. Missing Items

16. In order to prepare a text which is more comprehensive in many ways, consideration should be given to the inclusion of some missing items in the model law. For instance, definition of the terms “Level of assurance”, “Level of reliability”, and “Relying party” in article 1, describing rights and obligations of relying party, and also taking an explicit and a more comprehensive approach to rights of subscribers.

## I. Bulgaria

[Original: English]
[8 June 2022]

1. The Bulgarian national and European Union (EU) law on electronic identification and trust (certification) services is based on EU Regulation No. 910/2014 on electronic identification and trust services within the internal market and trust services for electronic transaction repealing EU Directive 1999/93. The powers of the Regulation Commission (CER) are defined in article 32 of the Law on the electronic documents and the electronic certification services, according to which the CER is the national supervisory authority in the field of electronic certification services responsible for implementing the provisions of the said EU Regulation.

2. EU Regulation No. 910/2014 establishes a common legal framework for the use of certification services in the EU member States and the recognition of certification services originating in a State outside the EU is regulated in article 14 of the Regulation. Such services may be recognized in case of an agreement concluded between the EU and the respective third State or an international organization, in accordance with article 218 of the Treaty on the Functioning of the European Union.

3. In view of the above, the Bulgarian CER considers that the submitted draft model law prepared by UNCITRAL meets the main objectives and principles set out in EU Regulation No. 910/2014.

## J. Singapore

[Original: English]
[13 June 2022]

1. Singapore expresses its appreciation to Working Group IV on its work on the draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services.

2. We wish to draw the Commission’s attention to three aspects of the draft Model Law (as contained in A/CN.9/1112) which merit careful consideration, as summarized below.

(a) The first relates to the need to:

(i) Express more clearly the relationship between article 9 and article 10(1) (for identity management services) by inserting the words “in accordance with article 10(1)” in article 9 so that the phrase in article 9 reads “*if a method in accordance with article 10(1) is used for the electronic identification of the person for that purpose*”; and

(ii) Express more clearly the relationships between each of articles 16 to 21 and article 22(1) (for trust services) by inserting the words “in accordance with article 22(1)” in each of articles 16 to 21 so that the respective phrases in articles 16 to 21 read “*if a method in accordance with article 22(1) is used …*”.

(See detailed discussion at paragraphs 3 and 4 below)

(b) The second relates to the importance of retaining the "safety clauses" embodied in article 10(1)(b) (for the reliability of identity management services) and article 22(1)(b) (for the reliability of trust services). These safety clauses, which mirror clauses in article 9(3)(b)(ii) of the United Nations Convention on the Use of Electronic Communications in International Contracts 2007 (ECC)[5] and article 12(b) of the UNCITRAL Model Law on Electronic Transferable Records 2017 (MLETR), seek to avoid spurious legal challenges (i.e. that the method used was not as reliable as appropriate *in theory*), by providing that a method satisfies article 9 or articles 16 to 21 if it is proven in fact to have fulfilled the function described in article 9 or the respective functions described in article 16 to 21 (i.e. reliability *in fact*), which may be by itself or together with further evidence. In our view, articles 10(1)(b) and 22(1)(b) serve as critical safeguards against such spurious challenges and should be retained in the same form. Also, removing (or moving) articles 10(1)(b) and 22(1)(b) will render the draft Model Law inconsistent with the ECC and MLETR. In that case, the Commission will need to (a) take a view on what States which are a party to the ECC or have enacted the MLETR should do to deal with the inconsistency; and (b) decide on whether the Commission will continue to recommend the ECC and MLETR (with inconsistent provisions) to States that are considering becoming party to the ECC or implementation of the MLETR. We propose amendments to paragraphs 142 and 143 of the draft Explanatory Note to more accurately describe the purpose and effect of draft article 10(1)(b).

(See detailed discussion at paragraphs 5 to 16 below)

(c) The third relates to the phrase "*at least an equivalent level of reliability*" in articles 25 and 26. In our view, it is not viable to require exact equivalence in reliability as a condition for cross-recognition of a foreign identity management service or trust service. Levels of reliability cannot be determined with exact precision and requiring exact equivalence is bound to elicit practical difficulties with cross-border recognition. The phrase "*a substantially equivalent or higher level of reliability*"[6] would be more appropriate in a multilateral context.

(See detailed discussion at paragraphs 17 to 19 below)

## I. Relationship between article 9 and article 10(1) and relationship between articles 16 to 21 and article 22(1)

3. The draft Model Law is structured as follows:

(a) Article 9 sets out the functional equivalence rule for the identification of a person using identity management services, while article 10(1) sets out the reliability requirements that the method of identification in article 9 must comply with.

(b) Similarly, articles 16 to 21 set out the functional equivalence rules for electronic signatures (article 16), electronic seals (article 17), electronic timestamps (article 18), electronic archiving (article 19), electronic registered delivery services (article 20) and website authentication (article 21), while article 22(1) sets out the reliability requirements that each of the methods mentioned in articles 16 to 21 must comply with.

4. In our view, the relationship between article 9 and article 10(1), and between each of the articles in articles 16 to 21 and article 22(1) should be made clearer, by inserting the words "*in accordance with article 10(1)*" immediately after the words "*if a method*" in article 9, and by inserting the words "*in accordance with article 22(1)*" immediately after the words "*if a method*" in each of articles 16 to 21. This clarifies that the requirement is met if a method in accordance with article 10(1) or article 22(1) is used to fulfil the functions, so as to avoid any suggestion that *any*

[5] Similar to how article 10(1) sets out the reliability requirements for a method used for electronic identification, article 9(3)(b) of the ECC sets out the reliability requirements for a method used to create an electronic signature.

[6] This term was considered during the sixty-third session of the Working Group.

method would suffice. The revised versions of those articles are set out in the **Appendix** below.

## II. Articles 10(1)(b) and 22(1)(b)

### A. Preventing spurious legal challenges

5. Article 10(1) of the draft Model Law provides as follows:

> *Article 10. Reliability requirements for identity management services*
>
> 1. For the purposes of article 9, the method shall be:
>
> (a) As 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.

6. Article 22(1) of the draft Model Law, which has a similar structure, provides as follows:

> *Article 22. Reliability requirements for trust services*
>
> 1. For the purposes of articles 16 to 21, the method shall be:
>
> (a) As reliable as appropriate for the purpose for which the trust service is being used; or
>
> (b) Proven in fact to have fulfilled the functions described in the article.

7. The "safety clauses" in question are found in articles 10(1)(b) and 22(1)(b). They mirror and serve the same purpose as article 9(3)(b)(ii) of the ECC and article 12(b) of the MLETR – to prevent spurious legal challenges to validity.

(a) Article 9(3) of the ECC, which contains the functional equivalence rule for electronic signatures, reads as follows:

> 3. Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if:
>
> (a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication; and
>
> (b) The method used is either:
>
> (i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or
>
> (ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.

The problem that article 9(3)(b)(ii) of the ECC was designed to address was the risk of a spurious legal challenge to the validity of an electronic signature, not on the ground that the purported signer did not sign, or that the document that was signed had been altered, but only on the ground that the method of signature used was not as reliable *as appropriate* in the circumstances (that is, the reliability in principle/theory is not appropriate in the circumstances).[7] Article 9(3)(b)(ii) enables such a spurious

[7] This is explained in detail in paragraph 164 of the Explanatory Note to the ECC (reproduced below):
"164. However, UNCITRAL considered that the Convention should not allow a party to invoke the 'reliability test' to repudiate its signature in cases where the actual identity of the party and its actual intention could be proved. The requirement that an electronic signature needs to be 'as reliable as appropriate' should not lead a court or trier of fact to invalidate the entire contract on the ground that the electronic signature was not ***appropriately*** reliable if there is no dispute about

legal challenge to be defeated by proving that the method used had fulfilled the functions described in article 9(3)(a), that is, by demonstrating that the method used was *in fact* reliable.

(b) Article 12(b) of the MLETR contains a similar "safety clause" for the same reason.[8]

8. It should first be noted that the phrase "*as reliable as appropriate*" is used in articles 10(1)(a) and 22(1)(a) because the *appropriateness* of the reliability of the method used depends on the purpose for which the relevant service is being used, taking into account all relevant circumstances which may include the circumstances mentioned in articles 10(2) and 22(2). A particularly relevant circumstance would be any agreement between the parties as to the method to be used. In other words, the appropriateness of the reliability of the method used in a particular transaction depends on the circumstances of that transaction, and articles 10(1)(a) and 22(1)(a) refer to a level of reliability that is relative and not to a single monolithic level of reliability.

9. Like article 9(3)(b)(ii) of the ECC and article 12(b) of the MLETR, articles 10(1)(b) and 22(1)(b) seek to avoid spurious legal challenges based on the appropriateness in theory of the reliability of the method used (*reliability in theory*), by providing that the method satisfies article 9 or articles 16 to 21 if it is proven in fact to have fulfilled the function described in the article (*reliability in fact*), which may be by itself or together with further evidence.

10. Removing articles 10(1)(b) and 22(1)(b) would open the door to spurious legal challenges. That is undesirable.

(a) Without article 10(1)(b), opportunistic actors (such as a party in a transaction involving electronic identification who wishes to avoid its obligations or even a third party who benefits from the invalidation of the electronic identification) may be encouraged to challenge the validity of the resulting identification – not on the ground that identification did not occur, but on the (frivolous) ground that the method of electronic identification used was not "*as reliable* ***as appropriate***" in the circumstances;

(b) The same analysis applies in the context of trust services. Taking electronic signatures as an example, we see that without article 22(1)(b), a party to a transaction in which an electronic signature was used may be encouraged to try to avoid its obligations by denying that its own signature (or the counterparty's signature) was valid – not on the ground that the purported signer did not sign or that the document

---

the identity of the person signing or the fact of signing, that is, no question as to authenticity of the electronic signature. Such a result would be particularly unfortunate, as it would allow a party to a transaction in which a signature was required to try to escape its obligations by denying that its signature (or the other party's signature) was valid – not on the ground that the purported signer did not sign, or that the document it signed had been altered, but only on the ground that the method of signature employed **was not '*as reliable as appropriate*'** in the circumstances. In order to avoid these situations, paragraph 3(b)(ii) validates a signature method – regardless of its reliability in principle – whenever the method used is proven in fact to have identified the signatory and indicated the signatory's intention in respect of the information contained in the electronic communication."
[Emphasis in bold]

[8] See paragraphs 136 and 137 of the Explanatory Note to the MLETR (reproduced below):
"136. Subparagraph (b) provides a 'safety clause' with the purpose of ***preventing frivolous litigation by validating methods that have in fact achieved their function regardless of any assessment of their reliability***. It refers to the fulfilment of the function in the specific case under dispute and does not aim at predicting future reliability based on past performance of the method. The provision may operate with respect to any of the functions pursued with the use of electronic transferable records. A similar mechanism is contained in article 9, paragraph 3(b)(ii), of the Electronic Communications Convention, relating to the functional equivalence of electronic signatures.
137. In practice, the fact that the method used has achieved the function pursued with its use ***will prevent any discussion on the assessment of its reliability according to subparagraph (a)***."
[Emphasis in bold]

it signed has been altered, but on the (frivolous) ground that the method of signature used was not "*as reliable **as appropriate***" in the circumstances. A third party who has an interest in the invalidation of the transaction may also be incentivized to attempt the same.

11. It might be argued that the presence of articles 10(1)(a) and 22(1)(a) alone are sufficient to avoid the undesirable outcomes described above – because a court or trier of fact could reject the opportunistic legal challenge by making an ex post finding that the method used in the transaction was "*as reliable as appropriate*" for the purpose for which the service was used as described in article 9 (identification) or articles 16 to 21 (trust services). However, we see two problems with such an approach. The first problem is that even if an opportunistic legal challenge brought is not successful eventually, such legal challenges still represent unnecessary litigation in electronic commerce transactions. That is not desirable.

12. The second and more important problem with removing the safety clauses in articles 10(1)(b) and 22(1)(b) and thereby exposing to the risk of spurious legal challenges all electronic transactions carried out under domestic legislation enacting the Model Law which may involve electronic identification (article 9), or electronic signatures (article 16), electronic seals (article 17), electronic timestamps (article 18), electronic archiving (article 19), electronic registered delivery (article 20) or website authentication (article 21), is that it creates uncertainty in consensual business transactions. This is illustrated with the following example:

(a) Suppose in 2023 (when the Model Law has been enacted as domestic legislation in some jurisdictions), two parties agree to sign a contract using a digital signature that uses SHA2-256 hashing (which generates a 256-bit hash);

(b) There is no dispute that the parties signed the contract. There is also no allegation that the contract was altered in any way;

(c) Yet without a safety clause, it would be open for party A (who, for example, wants to repudiate the contract he signed with party B because it turned out to be a bad bargain) to challenge the validity of the digital signatures used to sign the contract by alleging that the hashing algorithm was not "*as reliable **as appropriate***", because SHA3-512 ought to have been used instead of SHA2-256 which is not appropriately reliable.

Such a situation would be unfortunate. In our view, while the "*as reliable as appropriate*" standard is a sufficiently flexible standard, it is necessary to address the risk of a legal challenge on the ground of theoretical appropriateness of the reliability of the method used. For business certainty, it is inappropriate to rely solely on the "*as reliable as appropriate*" standard. How would businesses (like party B in our example above) have the confidence that the electronic transactions they enter into in 2023 will not be vulnerable to a spurious legal challenge in the future? The safety clauses, as contained in articles 10(1)(b) and 22(1)(b) of the draft Model Law, seek to ensure that this will not happen.

## B. Keeping the draft Model Law consistent with the ECC and MLETR

13. Retaining articles 10(1)(b) and 22(1)(b) in the same form would also keep the draft Model Law consistent with the ECC, which is the most up-to-date UNCITRAL instrument on electronic transactions. It is crucial that the draft Model Law remains consistent with article 9(3)(b)(ii) of the ECC. Many States (including Singapore) are party to the ECC and as such, are not able to enact any laws that are inconsistent with the ECC. There are also States which are not party to the ECC but have enacted legislation on electronic transactions based on the ECC, including a safety clause.[9]

[9] For example, section 10(b)(ii) of Australia's Electronic Transactions Act 1999 tracks article 9(3)(b)(ii) of the ECC. Australia's section 10(b)(ii) states as follows:
If, under a law of the Commonwealth, the signature of a person is required, that requirement is taken to have been met in relation to an electronic communication if:
(a) In all cases – a method is used to identify the person and to indicate that person's

Removing articles 10(1)(b) and 22(1)(b) (in particular, article 22(1)(b)) will result in the draft Model Law being inconsistent with article 9(3)(b)(ii) of the ECC. This would also be a matter of concern for future States parties to the ECC.

14. States that have enacted or are intending to enact the MLETR in domestic legislation would also have a concern with the removal of articles 10(1)(b) and 22(1)(b) from the draft Model Law as that would result in the draft Model Law being inconsistent with the MLETR.

15. In the event articles 10(1)(b) and 22(1)(b) are not retained in the same form, the Commission will need to (a) take a view on what States which are a party to the ECC or have enacted the MLETR should do to deal with the inconsistency; and (b) decide on whether the Commission will continue to recommend the ECC and MLETR (with inconsistent provisions) to States that are considering becoming party to the ECC or implementation of the MLETR.

### C. Amendments to draft Explanatory Note to clarify purpose of articles 10(1)(b) and 22(1)(b)

16. In keeping with the correct understanding of the purpose of the "safety clause" in articles 10(1)(b) and 22(1)(b), paragraphs 142 and 143 of the draft Explanatory Note should be amended as follows:

> 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 **as** reliable **as appropriate** 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.
>
> The Model Law generally requires the use of reliable methods, and paragraph 1(b) does not aim to promote the use of unreliable methods, or to validate the use of those methods. Rather, it acknowledges that, from a technical perspective, function (in the case of article 9, identification) and reliability are two independent attributes, and ~~**clarifies**~~ **provides** that under the Model Law **the method shall be as reliable as appropriate for the purpose for which the IdM service is being used, or may be proven to have fulfilled the** identification ~~**may be achieved**~~ in fact ~~**or by using a reliable method**~~. In other words, **proof of the** achievement of identification in fact pre-empts the need to ascertain the **appropriateness of the** reliability of the method used.

## III. Articles 25 and 26

17. Articles 25 and 26 contain provisions that facilitate the cross-border recognition of identity management and trust services respectively. As a condition for the cross-recognition of electronic identification, and the result deriving from the use of a trust service, provided outside the enacting jurisdiction, draft articles 25 and 26 currently require that the method used by the identification management service and the method used by the trust service respectively must offer "*at least an equivalent level of reliability*".

18. In our view, the threshold standard "*at least an equivalent level of reliability*" is problematic as it operates unidirectionally, and would not work in a multilateral

---

intention in respect of the information communicated; and

(b) In all cases – the method used was either:

(i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or

(ii) ***Proven in fact to have fulfilled the functions described in paragraph (a), by itself or together with further evidence…***

[Emphasis in bold]

context where many different States enact this same Model Law. Furthermore, the level of reliability of a method used which is a function of legal, technical and process factors is a qualitative standard and not a quantitative one. This means that it would be very difficult for a State seeking to have its services cross-recognized (State A) to match the level of reliability of its services to be exactly the same as the level of reliability of services under the laws of the recognizing State (State B). This creates further problems. We invite the Commission to consider the following hypothetical scenario:

(a) Suppose State A wishes to have its identity management service, pitched at a level of reliability/assurance of "level 1", recognized in State B. State A's "level 1" is substantially equivalent to State B's highest level of reliability/assurance, pitched at "high". But because the laws of State B require the level of reliability/assurance of a service to be cross-recognized to be exactly equivalent or higher in reliability/assurance, the identity management service from State A cannot be cross-recognized in State B unless State A modifies its legal and technical standards such that the level of reliability/assurance of its "level 1" is exactly the same or higher than State B's "high".

(b) In doing so, it is likely that the enhanced level of reliability/assurance of State A's "level 1" will be higher than the level of reliability/assurance of State B's "high" (because reliability cannot be measured like an exact science, State A is likely to ensure that the enhanced level of reliability/assurance of its "level 1" is higher when raising the level of reliability/assurance in order to ensure successful cross-border recognition).

(c) As a result of State A's modification, the identity management service of "level 1" from State A would subsequently be of "*at least an equivalent level of reliability*" as the level of reliability/assurance of an identity management service of "high" standard in State B, and this will enable the identity management service to be cross-recognized as "high" in State B. However, this conversely means that an identity management service of the level of reliability/assurance "high" from State B, will not be able to be cross-recognized under the laws of State A as equivalent to "level 1", as State B's "high" will now be considered to be of a lower level of reliability/assurance when compared to State A's "level 1" (despite it perhaps being substantially equivalent).

19. Such a state of affairs is undesirable, and renders cross-border recognition on a mutual basis to be nearly impossible. It would render cross-border recognition on a multilateral basis among multiple jurisdictions even more unworkable. In the circumstances, it would be more appropriate if articles 25 and 26 use the "*substantially equivalent or higher level of reliability*" standard. Requiring a "*substantially equivalent or higher level of reliability*" would allow cross-border recognition to be carried out bi-directionally between two jurisdictions without requiring exact equivalence. This would enable the cross-recognition of State A's services pitched at "level 1" and State B's services pitched at "high" as long as both are of a substantially equivalent level of reliability/assurance.

## Appendix

*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 method **in accordance with article 10(1)** is used for the electronic identification of the person for that purpose.

*Article 16. Electronic signatures*

Where the law requires a signature of a person, or provides consequences for the absence of a signature, that requirement is met in relation to a data message if a method **in accordance with article 22(1)** is used: […]

*Article 17. Electronic seals*

Where the law requires a legal person to affix a seal, or provides consequences for the absence of a seal, that requirement is met in relation to a data message if a method **in accordance with article 22(1)** is used: […]

*Article 18. Electronic timestamps*

Where the law requires a document, record, information or data to be associated with a time and date, or provides consequences for the absence of a time and date, that requirement is met in relation to a data message if a method **in accordance with article 22(1)** is used: […]

*Article 19. Electronic archiving*

Where the law requires a document, record or information to be retained, or provides consequences for the absence of retention, that requirement is met in relation to a data message if a method **in accordance with article 22(1)** is used: […]

*Article 20. Electronic registered delivery services*

Where the law requires a document, record or information to be delivered by registered mail or similar service, or provides consequences for the absence of delivery, that requirement is met in relation to a data message if a method **in accordance with article 22(1)** is used: […]

*Article 21. Website authentication*

Where the law requires website authentication, or provides consequences for the absence of website authentication, that requirement is met if a method **in accordance with article 22(1)** is used: […]