**End-to-end trade digitalization: Questionnaire on regulatory analysis**

**Introduction**

The United Nations Commission on International Trade Law (UNCITRAL) at its fifty-seventh session requested the secretariat to conduct a stocktaking exercise to examine all UNCITRAL legislative texts that referred to electronic aspects, including both UNCITRAL texts on electronic commerce and other texts that include provisions on the use of electronic means (A/79/17, para. 299). The Commission also requested a survey of the enactment of those texts and of the references to such texts contained in trade agreements. The secretariat was requested to circulate a questionnaire inviting States to provide the information and to submit copies of the relevant laws.

This Questionnaire has been prepared by the International and Comparative Law Research Center (ICLRC) as a part of its research complementing the stocktaking exercise of the secretariat and is aimed at harmonizing the existing approaches to digital trade. The main objectives of the ICLRC research are to identify the current state of implementation of the UNCITRAL documents, as well as to outline the alternative approaches and possible gaps.

This Questionnaire embraces [MLEC](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf), [MLES](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf), [ECC](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/06-57452_ebook.pdf), [MLETR](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mletr_ebook_e.pdf), [MLIT](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mlit_en.pdf), [MLAC](https://uncitral.un.org/sites/uncitral.un.org/files/mlac_en.pdf). It consolidates the UNCITRAL’s provisions on end-to-end trade digitalization based on the existing model laws and the convention in a generalized form in order to avoid duplication.

**Instructions**

This Questionnaire consists of seven parts. The first part deals with the regulatory landscape of your country. Kindly check which areas of digital trade are already covered by specific laws and briefly describe how each of the UNCITRAL General Principles is implemented in your country.

Parts II to VI are based on the relevant model laws and the convention. When answering the questions, please use one of the three colours to fill in the cells in accordance with the colour coding of the study:

|  |  |  |
| --- | --- | --- |
| **no regulation:**  the subject matter is not subject to any specific regulation in your country, but general rules of commercial or contract law may apply | **UNCITRAL regulation:**  the relevant UNCITRAL provision is fully incorporated in the laws of your country. We kindly ask you to briefly describe this regulation | **alternative regulation:** the issue addressed by the relevant UNCITRAL provision is regulated in the alternative manner by the laws of your country. We kindly ask you to briefly describe your country's approach so that we can use it for the proposals for further harmonization and consolidation of UNCITRAL instruments. |

Part VII deals with the regulatory gaps and aims at identifying the areas not yet covered by the UNCITRAL instruments.

The ICLRC would appreciate receiving responses by the end of February to allow time for compilation and analysis. The ICLRC reserves the right to make the information you provide publicly available unless you indicate otherwise.

**Part I. General**

What special laws are there in your country?

on electronic commerce/digital trade

|  |
| --- |
| UNIFORM ELECTRONIC TRANSACTIONS ACT (1999) |

on electronic/digital signatures

|  |
| --- |
| Electronic Signatures in Global and National Commerce Act (E-Sign Act) (2000) |

on identity and trust services

|  |
| --- |
|  |

on automated contracting

|  |
| --- |
| UNIFORM ELECTRONIC TRANSACTIONS ACT (1999) |

on electronic/digital transferrable records

|  |
| --- |
| Electronic Signatures in Global and National Commerce Act (E-Sign Act) (2000) |

**Adherence to the UNCITRAL General Principles**

|  |  |  |
| --- | --- | --- |
| **UNCITRAL principle** | **Content of provision** | **Implementation in your country** |
| Non-discrimination | Non-discrimination between information on a paper medium and information communicated or stored electronically. | It applies to electronic records and electronic signatures relating to transactions |
| Technology neutrality | No discrimination should be made among the various techniques that may be used to communicate or store information electronically. | Implemented |
| Functional equivalence | Analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques. | Implemented |

**Part II. Electronic communications**

no regulation,UNCITRAL regulation**,** alternative regulation

|  |  |  |
| --- | --- | --- |
| **UNCITRAL provision** | **Content of provision** | **Implementation in your country** |
| Consent to use | Nothing requires a party to use or accept electronic communications, but a party’s agreement to do so may be inferred from the party’s conduct. | Implemented |
| Technological neutrality of communication | The rules do not depend on or presuppose the use of particular types of technology and could be applied to communication and storage of all types of information. | Implemented |
| Writing | The requirement to be in writing is met if the information is accessible so as to be usable for subsequent reference. | Implemented |
| Original | Requirement to be in original is met if the integrity of the information is assured from the time when it was first generated in its final form and, where it is required that the information it contains be made available, that information is capable of being displayed to the person to whom it is to be made available. | Implemented |
| Time of dispatch | The time of dispatch of an electronic communication is the time when it leaves an information system or, if the electronic communication has not left an information system, the time when the electronic communication is received. | Electronic record is sent when it:  (1) is addressed properly that the recipient has designated or uses for the purpose of receiving electronic records and from which the recipient is able to retrieve the electronic record;  (2) is in a form capable of being processed by that system; and  (3) enters an information processing system outside the control of the sender or enters a region of the information processing system designated or used by the recipient which is under the control of the recipient. |
| Time of receipt | The time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee. | Electronic record is received when:  (1) it enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records and from which the recipient is able to retrieve the electronic record; and  (2) it is in a form capable of being processed by that system. |
| Place of dispatch and receipt | An electronic communication is deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business. | Implemented |
| Invitations to make offers | Advertisement is to be considered as an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance. | No regulation |
| Withdrawal due to error | The party that made the error has the right to withdraw the portion of the electronic communication in which the input error was made if:  (a) other party was notified of the error as soon as possible after having learned of the error and indicates that he or she made an error in the electronic communication; and  (b) the party that made the error has not used or received any material benefit or value from the goods or services, if any, received from the other party. | There 3 approaches to withdrawal due to error.   1. If the parties have agreed to use a security procedure to detect errors and one party has conformed to the procedure, but the other party has not, and the nonconforming party would have detected the error had that party also conformed, the conforming party may avoid the effect of the erroneous electronic record.   Secured procedure is procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.   1. In an automated transaction involving an individual, the individual may avoid the effect of an electronic record that resulted from an error made by the individual in dealing with the electronic agent of another person if the electronic agent did not provide an opportunity for the prevention or correction of the error and, at the time the individual learns of the error, the individual:   (A) promptly notifies the other person of the error and that the individual did not intend to be bound by the electronic record received by the other person;  (B) takes reasonable steps to return to the other person or, if instructed by the other person, to destroy the consideration received, if any, as a result of the erroneous electronic record; and  (C) has not used or received any benefit or value from the consideration, if any, received from the other person.   1. If 2 cases above don't applies, the change or error has the effect provided by other law, including the law of mistake, and the parties’ contract, if any. |

**Part III. Electronic signatures**

no regulation,UNCITRAL regulation,alternative regulation

|  |  |  |
| --- | --- | --- |
| **UNCITRAL provision** | **Content of provision** | **Implementation in your country** |
| Signature technology neutrality | The law recognizes any method of creating an electronic signature that satisfies the requirements. | Implemented |
| Compliance with a requirement for a signature | Where the law requires a signature of a person (either in the form of an obligation or in the form of consequences for the absence of a signature), that requirement is met if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated. | Implemented |
| Reliability of signature | An electronic signature is considered to be reliable if:  (a) The signature creation data are linked to the signatory and to no other person;  (b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;  (c) Any alteration to the electronic signature, made after the time of signing, is detectable; and  (d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable. | Signature should be attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. |
| Conduct of the signatory | Signatory shall:  (a) Exercise reasonable care to avoid unauthorized use of its signature creation data;  (b) Without undue delay, notify that the signature creation data have been compromised; or there is a substantial risk that the signature creation data may have been compromised;  (c) Ensure the accuracy and completeness of all material representations that are included in the certificate;  (d) Bear the legal consequences of its failure to satisfy the above mentioned requirements. | No regulation. |
| Conduct of the certification service provider | Certification service provider shall:  (a) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate or that are included in the certificate;  (b) Provide reasonably accessible means that enable a relying party to identify the certification service provider, verify the signatory and its control of the signature creation data at the time when the certificate was issued; and to verify that signature creation data were valid at or before the time when the certificate was issued;  (c) Provide reasonably accessible means that enable a relying party to ascertain:  (i) The method used to identify the signatory;  (ii) Any limitation on the purpose or value for which the signature creation data or the certificate may be used;  (iii) That the signature creation data are valid and have not been compromised;  (iv) Any limitation on the scope or extent of liability stipulated by the certification service provider;  (v) Whether means exist for the signatory to give notice that the signature creation data have been compromised;  (vi) Whether a timely revocation service is offered;  (d) Bear the legal consequences of its failure to satisfy the above mentioned requirements. | No regulation |
| Requirements to certification service providers | In determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors:  (a) Financial and human resources, including existence of assets;  (b) Quality of hardware and software systems;  (c) Procedures for processing of certificates and applications for certificates and retention of records;  (d) Availability of information to signatories identified in certificates and to potential relying parties;  (e) Regularity and extent of audit by an independent body;  (f) The existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing;  (g) Any other relevant factor. | No regulation |
| Conduct of the relying party | A relying party shall bear the legal consequences of its failure:  (a) To take reasonable steps to verify the reliability of an electronic signature; or  (b) Where an electronic signature is supported by a certificate, to take reasonable steps:  (i) To verify the validity, suspension or revocation of the certificate; and  (ii) To observe any limitation with respect to the certificate. | No regulation |
| Recognition of foreign certificates and electronic signatures | A certificate issued or an electronic signature created or used outside [the enacting State] shall have the same legal effect in [the enacting State] as a certificate (or signature) issued (created or used) in [the enacting State] if it offers a substantially equivalent level of reliability.  In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability, regard shall be had to recognized international standards and to any other relevant factors. Where parties agree to use certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law. | It works only for electronic signatures. |

**Part IV. Identity and trust services**

no regulation,UNCITRAL regulation, alternative regulation

|  |  |  |
| --- | --- | --- |
| **UNCITRAL provision** | **Content of provision** | **Implementation in your country** |
| E-identification and identity proofing | Where the law requires the identification of a person, 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 identity proofing and electronic identification. | There is no common federal regulation, but in different spheres legislature created separate rules. |
| 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 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. | No regulation |
| 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 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. | No regulation |
| 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 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. | If a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be retained, that requirement is met by retaining an electronic record of the information in the contract or other record that—  (A)accurately reflects the information set forth in the contract or other record; and  (B)remains accessible to all persons who are entitled to access by statute, regulation, or rule of law, for the period required by such statute, regulation, or rule of law, in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise. |
| 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 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. | No regulation |
| 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. | No regulation |
| Ex post recognition of reliability | The method shall be deemed to be as reliable as appropriate if proven in fact by or before a court or competent adjudicative body to have fulfilled the designated function, by itself or together with further evidence.  In determining the reliability of the method, all relevant circumstances shall be taken into account, which may include compliance with the legal requirements or any applicable recognized international standards and procedures relevant for the provision of the service, as well as any supervision or certification provided with regard to the service. | No regulation |
| Ex ante designation | A [person, organ or authority, whether public or private, specified by the enacting jurisdiction as competent] may designate identity management or trust services that are presumed reliable. | No regulation |
| Obligations in case of data breach | If a breach of security or loss of integrity occurs that has a significant impact on a service, the service provider shall, in accordance with the law:  (a) Take all reasonable steps to contain the breach or loss, including, where appropriate, suspending or revoking the affected service;  (b) Remedy the breach or loss; and  (c) Notify the breach or loss. | Implemented, but at states level[[1]](#footnote-1) |
| Cross-border recognition | The result deriving from the use of an identity management or trust service provided outside [the enacting jurisdiction] shall have the same legal effect in [the enacting jurisdiction] as the result deriving from the use of an identity management or trust service provided in [the enacting jurisdiction] if the method used by the service offers:  (a) At least an equivalent level of reliability, where the reliability levels recognized by such jurisdictions are identical; or  (b) Substantially equivalent or higher level of reliability, in all other cases.  For the purposes of determining the reliability level regard shall be had to recognized international standards. The identity management or trust service shall be presumed to be reliable if [the person, organ or authority specified by the enacting jurisdiction] has ex ante determined the equivalence. | No regulation |

**Part V. Automated contracting**

no regulation,UNCITRAL regulation,alternative regulation

|  |  |  |
| --- | --- | --- |
| **UNCITRAL provision** | **Content of provision** | **Implementation in your country** |
| Legal recognition of automated contracting | A contract formed using an automated system shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in any action carried out in connection with the formation of the contract  An action carried out by an automated system in connection with the formation or performance of a contract shall not be denied legal effect, validity or enforceability on the sole ground that no natural person reviewed or intervened in the action. | A contract or other record relating to a transaction in or affecting interstate or foreign commerce may not be denied legal effect, validity, or enforceability solely because its formation, creation, or delivery involved the action of one or more electronic agents so long as **the action of any such electronic agent is legally attributable to the person to be bound**. |
| Computer code and dynamic information | A contract shall not be denied validity or enforceability on the sole ground that the terms of the contract are contained in data messages in the form of computer code.  A contract or an action in connection with it shall not be denied validity or enforceability on the sole ground that it is based on information from a data source that provides information that changes periodically or continuously. | No regulation |
| Attribution of actions carried out by automated systems | As between the parties to a contract, an action carried out by an automated system is attributed in accordance with a procedure agreed to by the parties. If this does not apply, an action carried out by an automated system is attributed to the person who uses the system for that purpose. | No regulation |
| Unexpected actions carried out by automated systems | Unless otherwise agreed by the parties, where an action carried out by an automated system is attributed to a party to a contract, the other party to the contract is not entitled to rely on that action if:  (a) The party to which the action is attributed could not reasonably have expected the action; and  (b) The other party knew or could reasonably be expected to have known that the party to which the action is attributed did not expect the action. | No regulation |
| Non-avoidance | Unless otherwise provided by law, a party shall not be relieved from the legal consequences of its failure to comply with a rule of law on the sole ground that it used an automated system. | No regulation |

**Part VI. Electronic transferrable records**

no regulation,UNCITRAL regulation,alternative regulation

|  |  |  |
| --- | --- | --- |
| **UNCITRAL provision** | **Content of provision** | **Implementation in your country** |
| Transferable documents or instruments | Where the law requires a transferable document or instrument, that requirement is met by an electronic record if:  (a) The electronic record contains the information that would be required to be contained in a transferable document or instrument; and  (b) A reliable method is used:  (i) To identify that electronic record as the electronic transferable record;  (ii) To render that electronic record capable of being subject to control from its creation until it ceases to have any effect or validity; and  (iii) To retain the integrity of that electronic record. | Transferable record means an electronic record that—  (A)would be a note under Article 3 of the Uniform Commercial Code if the electronic record were in writing;  (B)the issuer of the electronic record expressly has agreed is a transferable record; and  (C)relates to a loan secured by real property.  A transferable record may be executed using an electronic signature. |
| Control | Where the law requires or permits the possession of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if a reliable method is used:  (a) To establish exclusive control of that electronic transferable record by a person; and  (b) To identify that person as the person in control. | Implemented and explained in more detail what means «to have control of a transferable record». |
| Transfer | Where the law requires or permits transfer of possession of a transferable document or instrument, that requirement is met with respect to an electronic transferable record through the transfer of control over the electronic transferable record. | Implemented |
| Endorsement | Where the law requires or permits the endorsement in any form of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if the information required for the endorsement is included in the electronic transferable record and that information is compliant with the requirements. | Endorsement is carried out in the same way as the recording itself |
| Amendment | Where the law requires or permits the amendment of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if a reliable method is used for amendment of information in the electronic transferable record so that the amended information is identified as such. | Implemented |

**Part VII. Other issues**

Please identify the three most important issues related to the electronic commerce or digital trade that are not covered by UNCITRAL documents, but are or will be regulated in your country:

1.

2.

3.

1. <https://www.itgovernanceusa.com/data-breach-notification-laws#:~:text=Notice%20must%20be%20made%20without%20unreasonable%20delay%20when%20the%20entity,reporting%20agencies%20and%20state%20agencies>.

   <https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business> [↑](#footnote-ref-1)