**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

|  |
| --- |
| **Federal Decree Law No 46/2021 On Electronic Transactions and Trust Services**  **Cabinet Decisions No 28/2023** |

☐on electronic/digital signatures

|  |
| --- |
| **Federal Administrative Decision No 53 on the Adoption of Rules and Conditions Regulating the Tools for Setting-Up the Approved Electronic Signature and Electronic Stamp, and the Authentication and Approval Thereof** |

☐on identity and trust services

|  |
| --- |
| **Federal Decree Law No 46/2021 On Electronic Transactions and Trust Services** defines trust services and qualified trust services and sets regulations for their implementation. |

☐on automated contracting

|  |
| --- |
| **Federal Decree Law No 46/2021 On Electronic Transactions and Trust Services**, Article (1) Definitions  Definition of **electronic transactions** includes any contract or agreement made through electronic means: any transaction that is made, executed, provided or issued in whole or in part in electronic form, including contracts, agreements and other transactions and services. |

☐on electronic/digital transferrable records

|  |
| --- |
| **Federal Decree Law No 46/2021 On Electronic Transactions and Trust Services** does not explicitly use the phrase “digital transferable records,” it does address electronic documents, electronic signatures, and electronic stamps in legally binding transactions. These provisions ensure that electronically created, stored, and transferred records are given the same legal effect as traditional paper-based documents, provided they meet certain authenticity and reliability standards. |

**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. | **Federal Decree Law No. 46/2021 on Electronic Transactions and Trust Services (“the Law”)** explicitly addresses the principle of non-discrimination between paper-based and electronic information.  **Article (5) – Legal Recognition of Electronic Documents**:   * This article confirms that electronic documents shall not be denied legal effect, enforceability, or validity solely because they are in electronic form. * This establishes equivalence between paper and electronic formats in terms of legal recognition.   **Article (18) – Acceptance and Res Judicata of Electronic Evidence and Trust Services**:   * It ensures that electronic records, signatures, and transactions cannot be disregarded or treated differently from physical records simply because they are digital. * This guarantees that electronic information holds the same evidentiary weight as paper-based documents in legal proceedings.   **Article (28) – Acceptance of Electronic Deal and Trust Services**   * It reinforces that electronic transactions, signatures, and stamps have the same legal status as handwritten signatures and physical records. * This ensures that electronic documents and records are as legally binding as traditional paper contracts. |
| Technology neutrality | No discrimination should be made among the various techniques that may be used to communicate or store information electronically. | Article 1  Electronic: Electromagnetic, photoelectric, digital, optical, or the like.  Electronic Transactions: Any transaction that is concluded, executed, provided or issued, in whole or in part, in Electronic form, and includes contracts, agreements, and other transactions and services.  Electronic Deal: Create, sign, send, receive, save or retrieve Electronic Documents.   * Information Technology Means: Any Electronic tool for performing logical and arithmetic operations, or for storing Data, or for sending and receiving Data. |
| 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. | The Lawincludes an analysis of the purposes and functions of traditional paper-based requirements and examines how those functions can be fulfilled through electronic commerce techniques.  The Law establishes a legal framework for electronic transactions, providing that electronic documents, electronic signatures, and other electronic transactions have the same legal validity as their paper-based counterparts. It removes legal obstacles to electronic dealings by ensuring that electronic records and contracts are legally recognized, enforceable, and admissible as evidence in court.  Key provisions in the Law that reflect this analysis include:  **Legal Recognition of Electronic Transactions and Documents**  The Law states that an electronic document shall not lose its legal force or enforceability merely because it is in electronic form (**Article 5**).  It ensures that an electronic document can satisfy legal requirements for written records (**Article 7**).  It allows electronic signatures and stamps to be used in place of traditional signatures and stamps (**Articles 8 and 9**).  Functional Equivalence Between Paper and Electronic transactions  The law ensures that electronic documents, when saved in a certain way, meet legal requirements for retention and retrieval (**Article 6**).  It enables electronic contracts, affirming that offer and acceptance can be expressed electronically and that contracts formed via automated electronic systems are valid (**Articles 10 and 11**).  Authentication and Trust Services  The Law defines the use of electronic signatures, digital identities, and trust services to verify the authenticity and integrity of electronic transactions (**Articles 17-22**).  It recognizes qualified electronic signatures as having the same legal effect as handwritten signatures (**Article 19**).  Acceptance and Use of Electronic Deal  The Law mandates that government authorities accept electronic transactions and documents, provided they meet security and trust standards (**Article 28**).  Thus, the decree effectively replaces traditional paper-based legal formalities with equivalent electronic processes while ensuring the integrity, reliability, and legal enforceability of electronic transactions. |

**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. | There is no legal requirement or obligation on parties to use electronic documents. Parties to the contract must agree to the use of an electronic document to conclude a transaction but party’s consent can be inferred from its conduct (Article 5 (3)). |
| 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. | Yes, the Law supports technology neutrality, meaning that the rules do not depend on or require the use of specific types of technology. Instead, they establish a legal framework that can be applied to the communication and storage of all types of information, regardless of the technology used. |
| Writing | The requirement to be in writing is met if the information is accessible so as to be usable for subsequent reference. | Yes, the Law aligns with the principle that the requirement for a document to be "in writing" is met if the information is accessible and usable for subsequent reference (Article 7). |
| 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. | Yes, the Law aligns with the principle that the requirement for a document to be in its "original" form is met if the integrity of the information is assured from the time it was first generated and if it remains accessible for display when required (Art. 9). |
| 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. | Sending the Electronic Document is deemed to have taken place when it **enters an information system that is not**  **under the control of the Originator** or the Person who sent the document on behalf of the Originator. (Art.14) |
| 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. | The Law defines the time of receipt as when the electronic communication enters the recipient’s information system and is accessible for retrieval.  If the recipient has specified an information system (e.g., an official email for legal notices), receipt occurs when the message enters that system.  If no system is specified, receipt occurs when the message enters any system used by the recipient. |
| 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. | Art. 14 (2)  Place of Dispatch   * The place where the electronic communication originates or is sent from. * If an electronic message leaves the sender’s information system, then the place of dispatch is usually where that system is located. * If the message remains in the same system, the place of dispatch is still where the sender is located.   Place of Receipt   * The place where the electronic communication is received and becomes accessible to the recipient. * If the recipient has designated a specific electronic address (e.g., a company email, official portal), the place of receipt is the location of that system. * If no specific address is designated, the place of receipt is generally where the recipient’s business or residence is located. |
| 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. | The law does address electronic contracts, offer, and acceptance but does not explicitly mention "invitation to make an offer."  Yes, the concept of invitation to make an offer is covered under the UAE Civil Transactions Law (Federal Law No. 5 of 1985, as amended). |
| 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. | The law recognizes the right to withdraw an electronic document or correct errors under specific conditions, particularly when a mistake arises from a system malfunction. However, it does not provide a general right to withdraw an electronic document solely on the basis of an input error by the sender unless other conditions (such as acknowledgment requirements) apply.  Provision is covered under the UAE Civil Transactions Law |

**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. | Yes, the Law recognizes any method of creating an electronic signature that satisfies the prescribed requirements. |
| 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. | Yes, the Law establishes that an electronic signature has the same legal effect as a handwritten signature if it meets the requirements of reliability and appropriateness for its intended purpose. |
| 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. | Electronic signature have to identify creator and his acceptance with information, which he signed (Electronic Signature: A signature consisting of letters, figures, codes, sound, fingerprint or processing system of Electronic form attached or logically linked to an Electronic Document, which verifies the identity of the Signatory and the acceptance of the latter of the content of the Data associated thereto.)  But for confirmation of originality of document or for qualified and approved e-signature it is important. |
| 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. | The Law places specific duties on individuals using electronic signatures, ensuring the integrity, security, and proper use of their signatures. The signatory must:   * Maintain exclusive control over their electronic signature creation data. * Prevent unauthorized access to their signature creation devices or authentication mechanisms. * Use the signature only for its intended purpose and ensure its integrity in transactions. * Exercise due diligence to prevent unauthorized use of their Electronic Signature or Stamp Creation Data. * Notify the relevant Licensee if they suspect any compromise in the security or validity of the Electronic Signature or Stamp Creation Data. |
| 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. | Ensuring the accuracy of material data in electronic authentication certificates throughout their validity.  Yes, the Law sets out requirements to the conduct of the certification:   * Providing accessible means for signatories to report any doubts about the trust services. * Offering authentication certificate cancellation services. * Using technically reliable systems and products to ensure security. * Maintaining electronic documents, electronic signatures, and evidence of authentication for a period specified by the authorities. * Providing means to report any facts that raise doubts about any of the services |
| 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. | A Qualified Trust Service Provider must:   1. Ensure the accuracy and completeness of the information contained in electronic authentication certificates and maintain their accuracy throughout the validity period. 2. Use technically reliable and secure systems that ensure proper protection against unauthorized modifications, changes, or breaches. 3. Keep databases updated for authentication certificates and promptly report any security risks to the competent authority. 4. Verify the identity and qualifications of certificate holders before issuing an electronic authentication certificate. 5. Implement proper security measures to prevent unauthorized access to signature creation data. 6. Ensure that services provided meet the technical, security, and regulatory standards determined by the relevant authorities. 7. Provide users with clear instructions and terms of service related to the issuance and use of authentication certificates. 8. Ensure that revocation services are available and that compromised certificates can be promptly invalidated. 9. Maintain transparency in operations and make relevant information available to relying parties. 10. Bear the legal consequences of failing to meet these obligations. |
| 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. | Verification of Validity:   1. A Relying Party must take necessary measures to confirm the validity and enforceability of an authentication certificate before relying on it. 2. The Relying Party must ensure the validity and enforceability of a digital identity when using it.   Due Diligence Before Reliance:  When relying on an electronic signature or stamp, the Relying Party must:   1. Determine the appropriate security level based on the nature, value, and importance of the transaction. 2. Verify the identity of the signatory and the validity of the authentication certificate. 3. Confirm that the electronic signature or stamp meets the legal requirements. 4. Ensure that the electronic signature, stamp, or authentication certificate has not been compromised or revoked. 5. Consider any previous agreements or transactions with the signatory. 6. Take into account any other relevant factors affecting the reliability of the electronic signature or stamp.   Liability for Improper Reliance:   1. If the Relying Party fails to conduct proper due diligence and relies on an invalid or compromised electronic signature or stamp, it bears the risk of invalidity. 2. The Relying Party will be responsible for any damages caused to the owner of the electronic signature/stamp or to third parties due to improper reliance. |
| 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. | Approved Trust Services provided by Approved Service Providers outside the State shall be recognised if they are similar to the level of services provided by approved service providers in accordance with the provisions of the law. |

**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. | Yes, the Law addresses identity proofing and electronic identification reliability.  Qualified Trust Service Provider must verify the identity and capacity of a person when issuing a Qualified Authentication Certificate through the following means:   1. Ensuring the physical presence of the person or their legal representative. 2. Using a Digital Identity that meets high-level security conditions under the law. 3. Issuing a Qualified Electronic Signature or Stamp Authentication Certificate based on a previous certificate. 4. Any legally recognized method equivalent to physical presence, as specified by the Executive Regulations. |
| Electronic stamps | Where the law requires a legal person to affix a stamp, or provides consequences for the absence of a stamp, 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. | Yes, the Law does provide the requirement for a legal person to affix a stamp or its equivalent in electronic transactions.  The Law allows an electronic method to meet the requirement of a legal person affixing a stamp, as long as it provides reliable assurance of the document’s origin and ensures its integrity. |
| 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. | Yes, the Law covers the requirement that a document, record, information, or data must be associated with a time and date, or provides consequences for the absence of a time and date.  This requirement is met if a reliable method is used:   1. To indicate the time and date, including by reference to the time zone. 2. To associate that time and date with the data message.   This provision aligns with the concept of a Approved Electronic Time Stamp, as referenced in Article 23 of the Law, which states that an approved timestamp must:   * Bind the electronic document to a specific time to establish evidence that its content existed at that time. * Be linked to an accurate time source (such as Coordinated Universal Time (UTC)). * Be signed or stamped using a Qualified Electronic Signature or Stamp by an Approved Trust Service Provider. |
| 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. | Yes, the Law addresses the requirement for retaining documents, records, or information. Specifically, **Article 6 (Saving Electronic Documents)** outlines the conditions under which electronic documents can be stored to meet legal retention requirements.  **Fulfillment of Storage Requirement**: If any legislation in force requires storing a document, record, or information, this requirement is met if it is stored as an Electronic Document, provided that:   1. It is saved in the form in which it was created, sent, or received, or in a form that accurately represents the original information. 2. The information is stored in a manner that allows it to be used and referenced later. 3. Sufficient details are stored to identify the Originator, Recipient, and the date and time of sending and receiving. 4. Exclusion of Transmission Data: Information that is necessarily and automatically created merely to enable the sending or receiving of a document is not required to be retained. 5. Third-Party Compliance: A person can comply with saving requirements by using the services of another entity, provided that entity meets the required legal conditions. 6. Government Authority Requirements: Government bodies may impose additional requirements for storing electronic documents under their jurisdiction, provided they do not conflict with the law.   This provision ensures that electronic records are legally recognized for retention purposes as long as they meet the integrity, accessibility, and identifiability criteria outlined above. |
| 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. | Yes, the Law covers the use of electronic methods for delivery when a law requires a document, record, or information to be delivered by registered mail or similar service.  Specifically, **Article 24** of the law recognizes **Approved Electronic Delivery Service**, which is a service for transmitting data electronically that provides:   * Evidence of sending and receiving the data, * Protection against loss, theft, damage, or unauthorized alterations, * Confirmation of the identity of the sender and recipient. |
| 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. | Yes, the Law deals with website authentication through Trust Services.  A reliable method includes, but is not limited to, the issuance of an Authentication Certificate for the website by a Trust Service Provider in accordance with the conditions in the Law. |
| 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. | The Law allows courts or adjudicative bodies to determine the reliability of a method based on evidence. A method is deemed as reliable as appropriate if proven in fact before a competent body to have fulfilled its designated function. |
| 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. | Yes, the Law incorporates ex ante designation, meaning that certain electronic methods and trust services are pre-approved by law rather than being determined case-by-case.  Pre-Designation of Trust Services and Qualified Trust Services  Article 17 explicitly defines and pre-approves specific Trust Services and Approved Trust Services, including:   * Qualified Electronic Signatures and Stamps * Qualified Electronic Time Stamps * Qualified Electronic Delivery Services * Website Authentication Certificates |
| 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. | Immediate Notification to Authorities and Affected Parties  Article 35(1) requires Trust Service Providers to immediately notify:   * TDRA (Telecommunications and Digital Government Regulatory Authority) * Competent Authorities (such as cybersecurity or data protection bodies) * Affected persons   This notification must occur as soon as the provider becomes aware of the breach or within the period specified by TDRA. |
| 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. | Foreign e-signatures are e-signatures having an authentication certificate issued by an approved trust service provider outside of the UAE. Reliance on a foreign e-signature is possible, as long as the two following conditions are fulfilled:   * the foreign certification provider has equally reliable standards as those in the UAE; and * the requirements for the issuance of a foreign certificate are similar to those for a UAE certificate.   If the parties agree to use a specific certification service provider or type of foreign digital certificate, such agreement will be binding. |

**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. | Yes, the Law fully supports the validity and enforceability of contracts formed through automated systems, even if no natural person intervened.   1. Automated contracts are explicitly recognized under UAE law. 2. A party cannot deny a contract’s enforceability just because it was executed automatically. 3. Electronic signatures, stamps, and authentication methods ensure validity. 4. Liability for automated transactions is attributed to the controlling party. |
| 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. | 1. No specific 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. | Yes, the Law:   * Supports the principle of attribution based on agreed procedures between parties. * Provides a default rule that actions by an automated system are attributed to the person who uses the system. * Establishes safeguards to prevent wrongful attribution when fraud or error is evident.   Art. 12 (2(b)) |
| 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. | Yes, the Law supports the principle that an automated system’s action cannot always be relied upon if it was unexpected and the other party knew or should have known about the issue.   * Automated actions are generally attributed to the controlling party (Article 12(2)(b)). * A party cannot rely on an automated action if it was not reasonably expected by the attributed party Article 12(4)(a)). * If the relying party knew or should have known the action was unintended, they cannot enforce it (Article 12(4)(b)). |
| 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. | Yes, the Law supports the principle that:   * A party is not relieved from legal consequences simply because an automated system was used. * Liability for non-compliance with legal obligations remains, regardless of automation. * Automation does not override statutory obligations, including verification, security, and compliance duties. |

**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. | Yes, the Law recognizes that a transferable document or instrument requirement is met by an electronic record, provided that:   * It contains all the required information. * It meets integrity and authenticity requirements. * Reliable electronic signatures and security measures ensure trustworthiness. |
| 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. | Yes, the Law recognizes electronic possession of transferable documents through reliable control mechanisms, ensuring that:   * An electronic transferable record can replace a paper-based document. * A reliable method (electronic signature, time stamp) must be used to establish control. * The person in possession must be identifiable and legally recognized. * Control mechanisms must prevent unauthorized modifications and track ownership history. |
| 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. | Yes, the Law recognizes the transfer of possession of electronic transferable records through the transfer of control.  Electronic records can be used in place of traditional transferable documents.   * Control over an electronic transferable record serves as legal possession. * Secure electronic signatures and time stamps verify control transfers. * The UAE Trust List ensures trusted service providers manage electronic control transfers. |
| 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. | Yes, the Law recognizes electronic endorsements on transferable records, ensuring that:   * Electronic transferable records can be endorsed just like paper instruments. * The endorsement must be included within the electronic record. * Reliable electronic signatures and authentication methods confirm endorsement validity. * Electronic endorsements are legally binding and enforceable. |
| 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. | Yes, the Law recognizes and regulates amendments to electronic transferable records, ensuring that: Amended information is clearly identified as such.   1. Reliable methods (electronic signatures, time stamps) track and authenticate changes. 2. Electronic amendments are legally binding and enforceable. 3. Parties can agree on amendment procedures within contractual terms. |

**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. **Artificial Intelligence (AI) in E-Commerce**: Currently, there is a lack of specific regulations governing the use of AI in e-commerce, particularly concerning transparency, accountability, and consumer consent but with a new AI ministry, there is an expectation of new relevant regulation.
2. **Data Protection Specific to E-Commerce**: There is an expectation in the market on the release of the executive regulations for the data protection law. Expectation is that there will be special provisions dealing with data protection in e-commerce.
3. **Digital Assets**: Digital Assets Law has been passed in the DIFC and ADGM, two common law financial free zones. It is expected that the mainland will follow.