Federal Decree Law No. (46) of 2021 on Electronic Transactions and Trust Services

We, Khalifa bin Zayed Al Nahyan, President of the United Arab Emirates,

After perusal of:

- The Constitution;
- Federal Law No. (1) of 1972 on the Competencies of the Ministries and Powers of the Ministers, as amended;
- Federal Law No. (5) of 1985 promulgating the Civil Transactions Law, as amended;
- Federal Law No. (10) of 1992 promulgating the Law of Evidence in Civil and Commercial Transactions, as amended;
- Federal Law No. (11) of 1992 promulgating the Civil Procedure Code, as amended;
- Federal Law No. (35) of 1992 promulgating the Criminal Procedure Code, as amended;
- Federal Law No. (4) of 2000 on the Emirates Securities and Commodities Authority and Market, as amended;
- Federal Decree Law No. (3) of 2003 Regulating the Telecommunications Sector, as amended;
- Federal Law No. (1) of 2006 on Electronic Commerce and Transactions;
- Federal Law No. (29) of 2006 on the Rights of People with Disabilities, as amended;

- Federal Law No. (4) of 2013 Regulating the Notary Public Profession, as amended;
- Federal Law No. (5) of 2017 on the Use of Remote Communication Technology in Criminal Proceedings;
- Federal Decree Law No. (14) of 2018 on the Central Bank and Organization of Financial Institutions and Activities, as amended;
- Federal Decree Law No. (14) of 2021 Establishing the Federal Authority for Identity, Citizenship, Customs and Port Security; and
- Based on the proposal of the Minister of Cabinet Affairs and the approval of the Cabinet,

have issued the following Decree Law:

Chapter One Definitions and General Provisions

Article (1) Definitions

In applying the provisions of this Decree Law, the following words and expressions shall have the meanings ascribed thereto respectively, unless the context otherwise requires:

State:	United Arab Emirates.
TDRA:	Telecommunications and Digital Government Regulatory Authority.
Board:	Board of Directors of TDRA.

Chairman:	Chairman of the Board of Directors of TDRA.
Government Authorities:	Federal and local government authorities.
Competent Authorities:	Government Authorities responsible for matters related to data protection and electronic security in the State, and the Federal Authority for Identity and Citizenship, as the case may be.
Federal Authority for Identity and Citizenship:	The Federal Authority for Identity, Citizenship, Customs and Port Security.
Electronic:	Electromagnetic, photoelectric, digital, optical, or the like.
Electronic Transactions:	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.
Electronic Dealing:	Creating, signing, sending, receiving, storing or retrieving Electronic Documents.
Information	Any electronic tool for performing logic and arithmetic

Technology Means:	operations or for storing, sending and receiving data.
Electronic Document:	An electronic record or message, or an information statement that is created, stored, extracted, copied, sent, communicated or received by Information Technology Means, on any medium, and is retrievable in a readable manner.
Data:	A set of facts, measurements and observations in the form of numbers, letters, symbols, or special shapes that are collected to be used.
Electronic Information:	Any data or information that can be stored, processed, generated and transmitted by Information Technology Means in the form of text, images, audio, video, numbers, letters, symbols, signs and else.
Electronic Information System:	A set of Information Programs and Information Technology Means designed to create, process, manage, store and exchange Electronic Information or the like.
Originator:	A person, by whom, or on whose behalf, the Electronic Document is created or sent, whatever the case may be, but does not include a person who provides services related to processing, sending or storing such Electronic Document or

	other relevant services.
Addressee:	A person who is intended by the Originator to receive the Electronic Document, but does not include a person who provides services related to receiving, processing or storing Electronic Documents or other relevant services.
Information Program:	A set of data, instructions and commands processable by Information Technology Means, intended to perform a certain task.
Automated Electronic Medium:	An Electronic Information System that operates automatically and independently, in whole or in part, without intervention by any natural person at the time of operation or response.
Automated Electronic Transactions:	Transactions made or executed in whole or in part by an Automated Electronic Medium.
Authentication Procedures:	Electronic procedures that aim to verify the identity of a person or his/her legal representative or the authenticity and integrity of the data received in any electronic form, including any procedure that uses algorithms, symbols, words, identification numbers, encryption and other data protection measures.

Electronic Identification System:	Technical and organizational measures that use a person's data to verify his/her identity and capacity for the purpose of issuing his/her Electronic Identifiers.
Electronic Identifier:	Any material or immaterial identifier issued through the Electronic Identification System that includes personal identification elements or data for the purpose of verifying a person's identity.
Digital Identity:	A special Electronic Identifier that gives a person access to carry out Electronic Transactions, signatures and seals with government or non-government authorities that adopt such an identifier to provide their services.
Trust Services:	The electronic services specified under Clause (1) of Article (17) hereof which a Trust Service Provider is licensed to provide according to the License issued thereto.
Qualified Trust Services:	The electronic services specified under Clause (2) of Article (17) hereof which a Qualified Trust Service Provider is licensed to provide according to the License issued thereto.
Electronic Signature Authentication	A document issued in electronic form by a Trust Service Provider that links between the verification data of the

Certificate:	Electronic Signature and a specific person and attributes it to his/her Electronic Signature, confirming the name and identity of such person or his/her pseudonym.
Qualified Electronic Signature Authentication Certificate:	An electronic signature authentication document issued by a Qualified Trust Service Provider based on the Electronic Identification System and Authentication Procedures that meets the conditions approved by TDRA in this regard.
Electronic Signature:	A signature consisting of letters, numbers, symbols, sound, fingerprint, or an electronic form processing system, attached to, or logically associated with an Electronic Document, verifying the identity of the Signatory and his/her approval of the information contained in such document.
Reliable Electronic Signature:	An electronic signature that meets the conditions specified in Article (19) hereof.
Qualified Electronic Signature:	A Reliable Electronic Signature that is created by a qualified electronic signature device, and is issued based on a Qualified Electronic Signature Authentication Certificate.
Electronic Seal:	Data in electronic form that is attached to or logically associated with an Electronic Document, used to verify the

	identity of the relevant person and the authenticity and integrity of the data source in such document.
Reliable Electronic Seal:	An electronic seal that meets the conditions specified in Article (19) hereof.
Qualified Electronic Seal:	A Reliable Electronic Seal that is created by a qualified electronic seal device, and is issued based on a Qualified Electronic Seal Authentication Certificate.
Electronic Seal Authentication Certificate:	A document issued in electronic form by a Trust Service Provider that links between the verification data of the electronic seal and a specific legal person, confirming the name and identity of such person.
Qualified Electronic Seal Authentication Certificate:	An electronic seal authentication document that meets the conditions approved by TDRA in this regard and is issued by a Qualified Trust Service Provider based on the Electronic Identification System and Authentication Procedures.
Electronic Signature or Seal Creation Data:	Unique electronic data that is owned, supervised and controlled by the Signatory and used to create an electronic signature or seal.

Signatory:	A person who creates an electronic signature or seal.
Electronic Signature or Seal Device:	Systems, software or devices that are used to create an electronic signature or seal of its various levels in accordance with this Decree Law.
Qualified Electronic Time Stamp:	Data in electronic form which binds an Electronic Document to a particular time establishing evidence that its content existed at that time.
Qualified Electronic Delivery Service:	A service for the transmission of data between persons by electronic means that provides evidence of sending and receiving the data, protects transmitted data against the risk of loss, theft, damage or any unauthorized alterations, and confirms the identity of such persons.
Person:	A natural or legal person.
Relying Party:	A person who relies on electronic Trust Services to provide services or transactions or to perform any other act.
Qualified Trust Mark:	A mark or logo that proves that the Trust Service Provider is qualified by TDRA to provide qualified electronic Trust Services.

Trust Service Provider:	A person who is licensed by TDRA, in accordance with the provisions of this Decree Law and the Executive Regulations thereof, to provide one or more Trust Services.
Qualified Trust Service Provider:	A Trust Service Provider who is granted the qualified status by TDRA to provide Trust Services and Qualified Trust Services, according to the status granted thereto.
Licensee:	A legal person who is licensed by TDRA in accordance with the provisions of this Decree Law and the Executive Regulations thereof.
License:	An authorization issued pursuant to the provisions of this Decree Law and the Executive Regulations thereof allowing the Licensee to proceed with any Trust Services or Qualified Trust Services.
UAE Trust List:	A list prepared and published by TDRA that determines Trust Service Providers, Qualified Trust Service Providers, the services and data related thereto, the status of license and their compliance with this Decree Law, the Executive Regulations thereof, and the decisions issued by TDRA in implementation thereof.

Compliance Assessment:	An assessment made by TDRA, or any other entity authorized thereby, to ascertain whether the license applicants and Licensees comply with the conditions, controls and standards approved under this Decree Law and the decisions issued in implementation thereof.
Coordinated Universal Time (UTC):	The time scale, based on the standard second, as defined by the international standards.

Article (2) Applicability of the Decree Law

1. The provisions of this Decree Law shall apply to:
   a. Persons who adopt Electronic Transactions, Trust Services and Qualified Trust Services specified in accordance with the provisions of this Decree Law.
   b. Electronic Transactions, Electronic Documents, Trust Services, Qualified Trust Services, and the necessary procedures for completion thereof.
2. The Cabinet may add, delete or exclude any transaction, document, service or procedure mentioned in Paragraph (B) of Clause (1) of this Article, and may exclude any entity from all or some of the provisions of this Decree Law.

Article (3) Objectives of the Decree Law

This Decree Law aims to:

1. Enhance trust, encourage and facilitate Electronic Transactions of all kinds, and protect the rights of customers.
2. Keep pace with technological development to enhance Electronic Transactions in all sectors.
3. Promote digital transformation, investment, and provide electronic services to the public.

Article (4) Competencies of TDRA

For the purposes of applying the provisions of this Decree Law, TDRA shall have the following competencies:

1. Regulating the work and activities of the Licensees, including issuing, renewing, amending, suspending and canceling Licenses, exempting from licensing or some or all of its conditions, and granting or withdrawing the qualified status, after ensuring that the Licensees comply with the controls, standards and requirements agreed upon with the Competent Authorities.
2. Issuing controls, procedures and standards related to the Electronic Identification System, Authentication Procedures and Digital Identity, after coordination with the Competent Authorities.
3. Issuing controls, procedures and standards related to Trust Services and Qualified Trust Services, in particular the mechanism for creating, saving and validating Electronic

Signatures, Electronic Seals, Electronic Documents electronically signed or sealed, and Qualified Trust Mark specifications, after coordination with the Competent Authorities.

4. Assessing license applicants or those licensed thereby or by the compliance assessment body and setting controls and conditions for regulating the work of compliance assessment bodies.
5. Preparing, publishing and updating the UAE Trust List of Licensees, Trust Services and Qualified Trust Services.
6. Supervising, controlling and inspecting Licensees, provided that coordination is made with the Central Bank of the United Arab Emirates regarding the inspection of the financial institutions licensed thereby.
7. Receiving and adjudicating complaints and taking the necessary procedures and measures with respect thereto.
8. Any other competencies assigned thereto by the Cabinet.

Chapter Two Electronic Transactions

Article (5) Electronic Documents

1. An Electronic Document shall not lose its legal force or enforceability for being in electronic form.
2. The data contained in Electronic Documents shall not lose its legal force for being received, whenever the details of such data are accessible, within the Electronic Information System of its Originator, with the Electronic Documents indicating the way of such access.
3. Nothing in this Decree Law requires a person to use an Electronic Document without the

consent thereof.

4. A person's consent to the use of the Electronic Document may be inferred from any conduct that indicates such consent.

Article (6) Storage of Electronic Documents

1. If any legislation in force in the State requires the storage of a document, record or information, for any reason, this requirement shall be fulfilled if that document, record or information is stored in the form of an Electronic Document, while observing the following:
   a. Storing the Electronic Document in the form in which it is created, sent or received, or in any form that may prove that it accurately represents the information originally created, sent or received.
   b. Keeping the information stored in a way that allows it to be used and referenced later.
   c. Storing such information, if any, that enables identification of the Originator of the Electronic Document, the destination thereof, and the date and time of sending and receiving same.
2. The obligation to store documents, records or information in accordance with Paragraph (C) of Clause (1) of this Article shall not extend to include any information that is necessarily and automatically created merely to enable the sending or receiving of the document.
3. Any person may fulfill the requirements stipulated in Clause (1) of this Article by using the services of any other person, as long as such person complies with the conditions stipulated in that Clause.

4. Government Authorities may set any additional requirements, that do not conflict with the provisions of this Decree Law, for maintaining Electronic Documents that fall under their jurisdiction.

Article (7) Writing

If any legislation in force in the State requires any information, statement, document, record, transaction or evidence to be in writing, or stipulates certain consequences in the event of no writing, this requirement shall be considered met by the Electronic Document if the information contained therein is stored in a way that allows it to be used and referenced.

Article (8) Signatures and Seals on Electronic Documents

1. If any legislation in force in the State requires the affixation of a signature or seal on a document or record, or stipulates certain consequences in the event of not signing or sealing a document or record, this requirement shall be considered met in the following cases:
    a. Using a means of identifying a person and indicating the intention of such person with respect to the information contained in the Electronic Document.
    b. If the means used meets either of the following two conditions:
        1) To be qualified for the purpose for which the Electronic Document is created or sent.
        2) To meet the requirements set forth in Paragraph (A) of Clause (1) of this Article, either alone or with any other evidence.
2. Any person may use any form of electronic authentication unless the law provides otherwise.

Article (9) Original Document

If any legislation in force in the State requires the submission or storage of any document, record, information or message in its original form, this requirement shall be considered met by the Electronic Document in the following cases:

1. If there is technical evidence confirming the integrity of the information contained in the Electronic Document since the time when the document, record or information is created for the first time in its final form as an Electronic Document.
2. If the Electronic Document allows presenting the information required to be submitted whenever requested.
3. If there are any additional conditions related to the submission or storage of Electronic Documents as determined by the Government Authority that supervises the submission or storage of such records or information.

Article (10) Creation and Validity of Contracts

1. For contracting purposes, offer and acceptance may be expressed electronically.
2. A contract shall not lose its validity, evidential weight or enforceability merely because it is made in the form of one or more Electronic Documents.

Article (11) Automated Electronic Transactions

1. A contract may be made between Automated Electronic Mediums that include one or more Electronic Information Systems that are prepared and programmed in advance for this purpose. Such contract shall be valid, enforceable and legally effective even in the

absence of personal or direct interference by any natural person in the process of making the contract in these systems.

2. A contract may be made between an automated Electronic Information System in the possession of a particular person and another person if the latter knows, or is supposed to know, that such system will make or execute the contract automatically.

Article (12) Attribution

1. An Electronic Document is considered issued by the Originator if he has issued it himself.
2. In the relationship between the Originator and Addressee, an Electronic Document shall be considered issued by the Originator in the following cases:
    a. If it is sent by a person who has the authority to act on behalf of the Originator.
    b. If it is sent by an electronic medium automated and programmed to operate automatically by or on behalf of the Originator.
3. In the relationship between the Originator and Addressee, the Addressee shall have the right to consider the Electronic Document as issued by the Originator and to act on this basis in the following cases:
    a. If the Addressee correctly applies a procedure previously approved by the Originator for the purpose of ensuring that the Electronic Document has been issued by the Originator for this purpose.
    b. If the Electronic Document received by the Addressee has resulted from the actions of a person who, based on his relationship with the Originator or any agent of the Originator, can access a method used by the Originator to prove that the Electronic Document is issued thereby.

4. The provisions of Clause (3) of this Article shall not apply in the following cases:
    a. If the Addressee receives a notification from the Originator that the Electronic Document has not been issued thereby, provided that the Addressee has been given reasonable time to act according to the notification.
    b. If the Addressee has known, or should have known, that the Electronic Document is not issued by the Originator.
    c. If it is unreasonable for the Addressee to consider the Electronic Document to be issued by the Originator or to act on this basis.
5. If an Electronic Document is issued or considered to be issued by the Originator or if the Addressee has the right to act on this basis in accordance with Clauses (1), (2) and (3) of this Article, the Addressee may, within the framework of its relationship with the Originator, consider the Electronic Document received as the document that the Originator has intended to send and to act on this basis.
6. The Addressee may consider every Electronic Document received thereby as a separate document and to act on this basis. Clause (7) of this Article shall not apply if the Addressee has known, or should have known, that the Electronic Document is a second copy.
7. The provisions of Clauses (5) and (6) of this Article shall not apply if the Addressee has known, or should have known, that an error has occurred in the Electronic Document as a result of a technical failure during transmission.

Article (13) Acknowledgment of Receipt

1. If the Originator has not agreed with the Addressee that the acknowledgment of receipt shall be in a certain form or manner, the acknowledgment of receipt may be made by the

following:

a. Any message from the Addressee, whether by electronic, automated or any other means.

b. Any conduct on the part of the Addressee which shall be sufficient to notify the Originator of receipt of the Electronic Document.

2. If the Originator has stated that the Electronic Document is conditional on receiving an acknowledgment of receipt, it shall not have any legal effect until the Originator receives the acknowledgment.
3. Without prejudice to the provision of Clause (2) of this Article, if the Originator requests an acknowledgment of receipt without specifying a date for receiving the acknowledgment within a reasonable period, and unless a particular time has been specified or agreed upon, the Originator may send a notification to the Addressee stating that it has not received any acknowledgment of receipt and specifying a reasonable period during which the acknowledgment must be received. If the acknowledgment of receipt is not received within the specified period, then it may deal with the Electronic Document as if it has not been sent.
4. The provisions of Clauses (1), (2) and (3) of this Article shall apply in cases where the Originator has requested or agreed with the Addressee, before or when sending the Electronic Document or through the Electronic Document, to send an acknowledgment of receipt of the Electronic Document.
5. If the Originator receives an acknowledgment of receipt from the Addressee, the Addressee shall be deemed to have received the relevant Electronic Document, unless proven otherwise, and an acknowledgment of receipt does not mean acknowledgment of the content of the Electronic Document.

6. If the acknowledgment of receipt received by the Originator states that the relevant Electronic Document has met the technical conditions, whether agreed upon or specified in the applicable standards, those conditions shall be considered met, unless proven otherwise.
7. The provisions of this Article shall not apply if there is an agreement between the Originator of the Electronic Document and the Addressee to the contrary.

Article (14) Time and Place of Sending and Receiving Electronic Documents

1. Unless an agreement is made between the Originator and Addressee on the place and time of sending and receiving the Electronic Document, the following shall apply:
    a. The Electronic Document shall be considered sent when it enters an information system that is not under the control of the Originator or the person who has sent the document on behalf of the Originator.
    b. The time of receiving the Electronic Document shall be determined according to the following:
        1) If the Addressee has designated an information system for the purpose of receiving the Electronic Document, the Electronic Document shall be considered received at the time it enters the designated information system or at the time the Addressee extracts the Electronic Document, if it is sent to an information system belonging thereto, other than the information system designated to receive the document.
        2) If the Addressee has not designated an information system, the Electronic Document shall be considered delivered when it enters an information system belonging to the Addressee, regardless of the difference between the

place where the information system is located and the place where the Electronic Document is considered to have been received in accordance with Clause (2) of this Article.

2. Unless otherwise agreed between the Originator and Addressee, the Electronic Document shall be considered to have been sent from the place where the Originator has its place of business and received at the place where the Addressee has its place of business.
3. In applying the provisions of this Article:
    a. If the Originator or Addressee has more than one place of business, the place of business shall be the one that is most closely connected with the relevant transaction or the principal place of business if there is no such transaction.
    b. If the Originator or Addressee does not have a place of business, it shall be considered their respective habitual residences.
    c. The habitual residence of a legal person shall be the headquarters or the place where it is incorporated.

Chapter Three Service Provider Licensing

Article (15)

1. No person may provide Trust Services except after obtaining a license from TDRA in accordance with the provisions of this Decree Law and the Executive Regulations thereof.
2. No person may provide Qualified Trust Services except after obtaining a license from TDRA and the qualified status in accordance with the provisions of this Decree Law and

the Executive Regulations thereof.

3. The Executive Regulations of this Decree Law shall set the conditions, controls, standards and procedures for the licensing referred to in this Article.

Article (16)

1. The Federal Authority for Identity and Citizenship shall set the controls, standards, and requirements that must be met by the license applicant, service provider, or Qualified Service Provider in the following two cases:
    a. Trust Services or Qualified Trust Services directed to the government sector.
    b. Trust Services or Qualified Trust Services that depend on the data or services of the Federal Authority for Identity and Citizenship.
2. TDRA shall verify that the license applicant, service provider or Qualified Service Provider complies with the controls, standards and requirements stipulated in Clause (1) of this Article.
3. TDRA shall suspend or cancel the License granted to a Trust Service Provider or a Qualified Trust Service Provider in the event of a violation of or non-compliance with the controls, standards and requirements stipulated in Clause (1) of this Article.
4. TDRA shall coordinate with the Federal Authority for Identity and Citizenship in all cases stipulated in this Article.

Article (17) Trust Services and Qualified Trust Services

Trust Services and Qualified Trust Services shall be determined according to the following:

1. Trust Services, including the following:
    a. Creating an Electronic Signature and a Reliable Electronic Signature.

b. Issuing an Authentication Certificate for the Reliable Electronic Signature.

c. Creating an Electronic Seal and a Reliable Electronic Seal.

d. Issuing an Authentication Certificate for the Reliable Electronic Seal.

e. Issuing an Authentication Certificate for the website.

2. Qualified Trust Services, including the following:

a. Qualified Electronic Signature creation services, including the following:

1) Issuing an Authentication Certificate for the Qualified Electronic Signature.

2) Issuing the Electronic Signature Device.

3) Managing the Qualified Electronic Signature Device remotely.

4) Storing data of the Qualified Electronic Signature.

5) Validating the Qualified Electronic Signature.

b. Qualified Electronic Seal creation services, including the following:

1) Issuing an Authentication Certificate for the Qualified Electronic Seal.

2) Issuing the Qualified Electronic Seal Device.

3) Managing the Qualified Electronic Seal Device remotely.

4) Storing data of the Qualified Electronic Seal.

5) Validating the Qualified Electronic Seal.

c. Qualified Electronic Time Stamp creation service.

d. Qualified Electronic Delivery Service.

Article (18) Admissibility and Authenticity of Electronic Evidence and Trust Services

1. The admissibility of an Electronic Document, Electronic Signature, Electronic Seal or Electronic Transactions as evidence in any legal proceeding shall not be precluded by the

mere fact that it is received in electronic form and processed through Trust Services and Qualified Trust Services.

2. A hard copy of an official Electronic Document shall be considered conclusive evidence to the extent that it is identical to the original of such document.
3. A Qualified Electronic Signature shall be considered equal in its authenticity to a manual signature and shall have the same legal effect so long as it meets the conditions stipulated in this Decree Law and the Executive Regulations thereof.
4. A Qualified Electronic Seal of a legal person shall be considered evidence of the validity and integrity of the original information to which the Electronic Seal is linked.
5. A qualified date and time shall be verified through the Qualified Electronic Time Stamp whenever it is linked to correct data.
6. The Qualified Electronic Delivery Service shall be considered valid and legally effective if it meets the conditions stipulated in this Decree Law and the Executive Regulations thereof.
7. The Reliable Electronic Signature and the Reliable Electronic Seal shall be considered valid and legally effective if the conditions stipulated in this Decree Law and the Executive Regulations thereof are met.
8. Trust Services and Qualified Trust Services shall meet the conditions stipulated in this Decree Law and the Executive Regulations thereof.

Article (19) Reliable Electronic Signature and Reliable Electronic Seal

An Electronic Signature or Electronic Seal shall be reliable if the following conditions are met:

1. Be linked to, and fall under the full and exclusive control of, the Signatory.

2. Be capable of identifying the Signatory.
3. Be linked to the signed data in a way that can detect any alteration to such data.
4. Be created using technical and security techniques in accordance with the technical requirements specified by the Executive Regulations of this Decree Law.
5. Any other conditions specified by the Executive Regulations of this Decree Law.

Article (20) Qualified Electronic Signature and Qualified Electronic Seal

1. A Qualified Electronic Signature or Qualified Electronic Seal shall be valid if the following conditions are met:
    a. The Electronic Signature and Electronic Seal are created based on a valid and qualified Authentication Certificate in accordance with the provisions of this Decree Law.
    b. The Electronic Signature and Electronic Seal are created using a Qualified Electronic Signature or Seal Device.
    c. The data proving the validity of the Qualified Electronic Signature and Qualified Electronic Seal is identical to the data submitted to the Relying Party.
    d. The data identifying the Signatory in the qualified Authentication Certificate is properly submitted to the Relying Party, and in case of using pseudonymization techniques, the Relying Party must be informed.
    e. It is created using technical and security techniques in accordance with the requirements specified by the Executive Regulations of this Decree Law.
    f. Any other conditions specified by the Executive Regulations of this Decree Law.
2. The Qualified Electronic Signature and Qualified Electronic Seal validation service shall be provided by the Qualified Trust Service Provider in accordance with the controls

specified by the Executive Regulations of this Decree Law.

3. The Qualified Electronic Signature and Qualified Electronic Seal validation service shall provide the Relying Party with the correct result to validate the signature and seal in an automated, effective and reliable manner, and ensure the absence of any hacks.
4. The validation result of the Qualified Electronic Signature and Qualified Electronic Seal shall be signed with a Reliable Electronic Signature or Reliable Electronic Seal by a Qualified Service Provider or by any other method specified by the Executive Regulations of this Decree Law.

Article (21) Conditions for the Qualified Electronic Signature and Qualified Electronic Seal Device

The Qualified Electronic Signature or Qualified Electronic Seal Device shall meet the following conditions:

1. Ensuring the confidentiality of the Electronic Signature or Seal Creation Data used.
2. Protecting the Electronic Signature or Seal Creation Data against any use by third parties or forgery using the available technology.
3. The Electronic Signature or Seal shall be created once only.
4. The data to be signed shall not be modified or withheld from the Signatory before the signing or sealing process.
5. The Electronic Signature Creation Data shall be managed or created on behalf of the Signatory by the Qualified Trust Service Provider in accordance with the conditions, standards and procedures specified by the Executive Regulations of this Decree Law.
6. Complying with the approved controls and procedures for the security and protection of

information.

7. Any other conditions specified by the Executive Regulations of this Decree Law.

Article (22) Storing the Data of Qualified Electronic Signatures and Qualified Electronic Seals

A Qualified Trust Service Provider shall, when providing a data storage service for Qualified Electronic Signatures and Qualified Electronic Seals, comply with the procedures and techniques that maintain the continuity of Trust Services and ensure the continued validity of the Qualified Electronic Signature in accordance with the conditions and period specified by the Executive Regulations of this Decree Law.

Article (23) Qualified Electronic Time Stamp

The Qualified Electronic Time Stamp shall meet the following conditions:

1. The date and time are linked to the data in a way that prevents undetectable alteration of the data.
2. Relying on an accurate time source linked to UTC.
3. To be signed or sealed using a Reliable Electronic Signature or a Reliable Electronic Seal by a Qualified Trust Service Provider, or by any other method specified by the Executive Regulations of this Decree Law.
4. Any other conditions specified by the Executive Regulations of this Decree Law.

Article (24) Qualified Electronic Delivery Service

The Qualified Electronic Delivery Service shall meet the following conditions:

1. To be provided by one or more Qualified Trust Service Providers.
2. Ensuring the identification of the sender based on a high level of security and trust, as specified by the Executive Regulations of this Decree Law.
3. Ensuring the identification of the Addressee before the data is delivered.
4. Signing or sealing the sent data with a Reliable Electronic Signature or a Reliable Electronic Seal by a Qualified Trust Service Provider or by any other method specified by the Executive Regulations of this Decree Law.
5. Notifying both the sender and recipient of any necessary change in the sent data as required by the service.
6. Stamping the time of sending and receiving data and any alterations thereto with a Qualified Electronic Time Stamp.
7. Any other conditions specified by the Executive Regulations of this Decree Law.

Article (25) Authentication Certificates

1. An Authentication Certificate shall no longer be valid from the date of its cancellation. Such cancellation shall not apply retroactively to any Electronic Signature or Electronic Seal made based on such certificate prior to that date.
2. No person may publish an Authentication Certificate if he knows that it is invalid or cancelled, or if the person to whom it is addressed has refused to receive it.

Article (26) Qualified Trust Mark

A Qualified Trust Service Provider shall, when using a Qualified Trust Mark, comply with the following requirements:

1. Indicating the Qualified Trust Services it is licensed to provide.
2. Linking the mark to an electronic link available to the public through its website that leads to the UAE Trust Services List published by TDRA.

Article (27) UAE Trust List

1. TDRA shall create a list of the Licensees and their services and a list of the Electronic Identification System and the Qualified Electronic Signature and Seal Devices, include them in the UAE Trust List and publish them by any means it deems appropriate.
2. The two lists referred to in Clause (1) of this Article must include the basic information about the Qualified Trust Service Providers, the Qualified Trust Services provided thereby, and the details of the Qualified Electronic Signature and Qualified Electronic Seal Devices.
3. The Executive Regulations shall set the controls and conditions for the inclusion of Licensees, Trust Services and Qualified Trust Services in the UAE Trust List.

Article (28) Acceptance of Electronic Dealing and Trust Services

1. Nothing in this Decree Law requires a person to use or accept Electronic Dealing. However, a person's consent to Electronic Dealing may be inferred from any conduct that indicates such consent.
2. A person may use any form of Electronic Signatures or Electronic Seals, unless the legislation in force provides otherwise.
3. The Digital Identity issued in accordance with the requirements of the Electronic Identification System approved by TDRA, in coordination with the Federal Authority for Identity and Citizenship, shall be adopted as a means of accessing the electronic services

and transactions provided by Government Authorities.

4. The use of the Digital Identity issued through the Electronic Identification System to access government electronic services shall be considered to meet the requirements for identification and personal presence if the Digital Identity provides the level of trust and security required for dealing with those services in accordance with the provisions of this Decree Law.
5. Government Authorities shall accept the use of Electronic Signatures, Electronic Seals, Digital Identities of persons or Electronic Documents in the electronic services provided thereby, by other Government Authorities or by whoever is delegated thereby, in accordance with the form, standards and levels of trust and security determined by TDRA.
6. Government Authorities may, according to their respective areas of competence established in the legislation in force, make Electronic Transactions, which will have the same legal effect, in the following cases:
    a. Accepting the filing, submission, creation or storage of documents in the form of electronic records.
    b. Issuing any document, permit, license, decision or approval in the form of electronic records.
    c. Collecting fees or paying any other money in electronic form.
    d. Tendering and receiving and awarding bids related to government procurement electronically.
7. If the Government Authority decides to carry out any of the acts mentioned in Clause (6) of this Article, it may specify the following:
    a. The way or form in which such Electronic Documents shall be created, filed,

stored, submitted or issued.

b. The controls, conditions, and procedures for tendering, receiving and awarding bids and concluding government procurements.
c. The form of the Electronic Signature and Seal, and the level of security required.
d. The way and form in which such signature or seal shall be affixed to the Electronic Document and the technical criteria that must be met by the Trust Service Provider to whom the document is submitted for storage and filing.
e. Processes, controls and procedures of monitoring related to the safety, security and confidentiality of Electronic Documents, payments or fees.
f. Terms and conditions related to sending paper documents, if required in relation to the Electronic Documents for payments and fees.

8. Government Authorities shall archive Electronic Documents affixed with a Reliable or Qualified Electronic Signature or with a Reliable or Qualified Electronic Seal in accordance with the controls specified by the Executive Regulations of this Decree Law.

Article (29) Responsibilities of the Relying Party

1. A Relying Party shall be held responsible for the consequences of the failure thereof to take the necessary measures to ensure the validity and enforceability of an Authentication Certificate and to observe any restrictions thereon.
2. A Relying Party shall be held responsible for the consequences of the failure thereof to take the necessary measures to ensure the validity and enforceability of a Digital Identity when using it.
3. A Relying Party, in order to trust and rely on an Electronic Signature or Electronic Seal, shall observe the following:

a. Determining the security level of the Electronic Signature or Electronic Seal according to the nature, value or importance of the transaction that is intended to be confirmed by the Electronic Signature or Electronic Seal.
b. Taking the necessary measures to verify the identity of the Signatory and the validity of the Authentication Certificate.
c. Taking the necessary measures to verify that the Electronic Signature or Electronic Seal used meets the requirements.
d. Whether it knows, or is supposed to know, that the Electronic Signature, Electronic Seal or Electronic Authentication Certificate has been breached or cancelled.
e. Any previous agreement or transaction between the Signatory and the Relying Party that has relied on the Electronic Signature, Electronic Seal or Authentication Certificate.
f. Any other relevant factors.

4. If the reliance on the Electronic Signature or Electronic Seal is not acceptable, according to Clause (3) of this Article, the party who has relied on them shall bear the risk of invalidity of such signature or seal and shall be responsible for any damage caused to the owner of the Electronic Signature or Electronic Seal or third parties.

Article (30) Responsibilities of the Signatory

A Signatory shall be held responsible for the consequences of the failure thereof if the following measures are not observed:

1. Exercising due diligence to avoid any unauthorized use of the Electronic Signature or Seal Creation Data.

2. Notifying the concerned Licensee if it becomes known that there are doubts about the level of security or validity of the Electronic Signature or Seal Creation Data thereof that is used to create such signature or seal.
3. Ensuring the accuracy and integrity of any material data provided thereby in relation to the Authentication Certificate throughout its validity period, in cases where the use of this certificate is required.
4. Reporting any changes to, or lack of confidentiality of, the information contained in the Authentication Certificate.
5. Using valid Authentication Certificates.

Article (31) Responsibilities of the Digital Identity Owner

The owner of the Digital Identity shall be held responsible for the consequences of the failure thereof if the following measures are not taken:

1. Exercising due diligence to avoid any unauthorized use of the Digital Identity.
2. Notifying the concerned parties and persons immediately if it becomes known that there are doubts about the level of security of the Digital Identity used in an electronic service or transaction.
3. Ensuring the accuracy and integrity of any material data provided thereby in relation to the Digital Identity throughout its validity period.

Article (32) Availability of Trust Services for People with Disabilities

Trust Services and Qualified Trust Services shall, whenever possible, be made available to natural persons with disabilities, in accordance with the procedures and techniques that suit

their needs or the nature of their special situation.

Article (33) Electronic Identification System Security Levels

1. The levels of security and trust of the Electronic Identification System and the Digital Identity issued thereby are three: low, medium and high, according to the following general classifications:
    a. Low level: means a low level of security and trust in the Electronic Identification System that provides a limited degree of trust and acceptability of the alleged identity of a person, and refers to technical and administrative standards and procedures aimed at reducing the risks of misuse or manipulation of that identity.
    b. Medium level: means a medium level of security and trust in the Electronic Identification System that provides a medium degree of trust and acceptability of the alleged identity of a person, and refers to technical and administrative standards and procedures aimed at minimizing the risks of misuse or manipulation of that identity.
    c. High level: means a high level of security and trust in the Electronic Identification System that provides a high degree of trust and acceptability of the alleged identity of a person, and refers to technical and administrative standards and procedures aimed at eliminating any risks and preventing misuse or manipulation of that identity.
2. A Licensee shall observe the following:
    a. Indicating to the Relying Party the levels of security and trust of the Digital Identity issued under the Electronic Identification System.
    b. Ensuring compliance with the technical specifications, standards and procedures

for the relevant level of security in the Electronic Identification System and Digital Identity as approved by TDRA.

3. The Digital Identity used in Qualified Trust Services shall meet a high level of security and trust.
4. TDRA shall, after coordination with the Competent Authorities, set the technical conditions and standards that must be met in terms of security and trust levels, provided that the following are observed:
    a. Setting criteria for differentiating between the levels of security and trust according to the degree of trust and acceptability.
    b. Authentication Procedures for the person requesting the issuance of the Digital Identity.
    c. The technical and security specifications of the Digital Identity, the procedures for its issuance, and its issuing entity.
    d. Authentication Procedures to confirm the identity of any person to the Relying Party.
    e. Types of transactions and services provided by public or private entities.

Article (34) Issuance of Authentication Certificates

A Qualified Trust Service Provider shall, when issuing a Qualified Authentication Certificate, verify the identity and capacity of the person to whom the certificate will be issued, by any of the following means:

1. Ensuring the presence of the person or the legal representative of the legal person.
2. Using a Digital Identity that meets the conditions stipulated in this Decree Law regarding high levels of security.

3. A Qualified Electronic Signature Authentication Certificate or a Qualified Electronic Seal Authentication Certificate issued by another Qualified Trust Service Provider.

4. Any procedure applicable in the State that is equivalent to the person's presence, in accordance with the conditions and procedures specified by the Executive Regulations of this Decree Law.

Article (35) Obligations of Licensees

The Licensees shall have the following obligations:

1. Notifying TDRA, the Competent Authorities and the concerned person of any violation or breach of the security and integrity of the data, immediately upon becoming aware of such violation or within the period specified by the decisions issued by TDRA.
2. Indicating to the Relying Party the levels of security and trust of the Digital Identity issued under the Electronic Identification System.
3. Ensuring compliance with the technical and security specifications, standards and procedures for the level of security required in the Electronic Identification System as approved by TDRA.
4. Submitting a biennial report issued by the compliance assessment body to TDRA regarding compliance with the terms of the License issued thereto and the decisions issued thereby.
5. Protecting personal data and implementing controls and procedures in accordance with the requirements of the competent authorities and the legislation in force.
6. Taking all necessary measures to manage any risks that may arise to ensure the security and safety of electronic Trust Services and Qualified Trust Services in a way that prevents the occurrence of any security incidents or breaches or minimizes their effects if

they occur.

7. Preparing a service termination plan in accordance with the requirements specified by the Executive Regulations of this Decree Law.
8. Any other obligations specified by the Executive Regulations of this Decree Law or other legislation in force in the State.

Article (36) Obligations of Qualified Trust Service Providers

Qualified Trust Service Providers shall have the following obligations:

1. Complying with the terms of Licenses issued thereto.
2. Ensuring the accuracy of the material data in electronic Authentication Certificates throughout their validity period.
3. Providing an appropriate means for the Signatories that enables them to report any facts that raise doubts about any of the services provided thereby in accordance with the Licenses issued thereto.
4. Providing Authentication Certificate cancellation service.
5. Notifying TDRA of any amendment to the data contained in the license application or of their desire to suspend submission thereof in accordance with the conditions and procedures specified by the Executive Regulations of this Decree Law.
6. Using technically reliable systems and products that ensure technical security and are protected against any changes, modifications or hacks, as determined by TDRA and as approved by the Competent Authorities in this regard.
7. Keeping Electronic Documents, Electronic Signatures and Seals, and evidence related to identification for the period specified by TDRA.
8. Processing personal data in accordance with the legislation in force and the

provisions of this Decree Law.

9. Creating and maintaining an updated database of Authentication Certificates, in case the Authentication Certificate service is provided by the Qualified Trust Service Provider.
10. Developing an updated plan to terminate the provision of the electronic Trust Service to ensure the continuity of the service.
11. Refraining from providing the services in case of doubt about the accuracy of the data or the validity of the document submitted to verify the information provided for identification or establishment of the right to representation, or if there is a security impediment or risk.
12. Relying on official data sources of persons in the State to provide any of the Qualified Trust Services specified in the Licenses issued thereto.
13. Any other obligations specified by the Executive Regulations of this Decree Law or other legislation in force in the State.

Article (37) International Trust Services

Qualified Trust Services provided by Qualified Trust Service Providers outside the State shall be recognized if they are similar to the level of services provided by Qualified Trust Service Providers in accordance with the provisions of this Decree Law and the decisions issued by TDRA.

Article (38) Civil Liability

Trust Service Providers shall bear civil liability for any damages incurred by any person as a result of breach of the obligations stipulated in this Decree Law, the Executive Regulations

thereof and decisions issued by TDRA.

Chapter Four Penalties

Article (39)

Shall be punished by imprisonment and/or a fine of not less than one hundred thousand (100,000) Dirhams and not more than three hundred thousand (300,000) Dirhams whoever forges or participates in the forgery of an Electronic Document, Electronic Signature, Electronic Seal, Authentication Certificate, Trust Services and other Qualified Trust Services.

Shall be punished by temporary imprisonment and a fine of not less than one hundred and fifty thousand (150,000) Dirhams and not more than seven hundred and fifty thousand (750,000) Dirhams whoever forges or participates in the forgery of an Electronic Document, Electronic Signature, Electronic Seal, Authentication Certificate, Trust Services and other Qualified Trust Services of the federal or local government or federal or local public authorities or institutions.

Whoever knowingly uses the forged Electronic Document shall be punished with the same penalty prescribed for the crime of forgery, as the case may be.

Article (40)

Shall be punished by imprisonment for a period of not more than one year and/or a fine of not less than one hundred thousand (100,000) Dirhams and not more than one million (1,000,000) Dirhams whoever:

1. Unlawfully exploits any Trust Services or Qualified Trust Services.
2. Uses fraudulent methods or takes a false name or an incorrect capacity to obtain any Qualified Trust Services.

If any of the foregoing acts are carried out with the intention of committing a crime, this shall be considered an aggravating circumstance.

Article (41)

Shall be punished by imprisonment for a period of not more than one year and/or a fine of not less than fifty thousand (50,000) Dirhams and not more than five hundred thousand (500,000) Dirhams whoever creates, publishes or provides another person with an Authentication Certificate, while being aware of any of the following:

1. The certificate is not issued by the Licensee whose name appears thereon.
2. The certificate is rejected by the Signatory whose name appears thereon.
3. The certificate is cancelled, unless the purpose of publication is to confirm any Electronic Signature or Electronic Seal used prior to such cancellation.
4. The certificate contains incorrect data.

Article (42)

1. Shall be punished by temporary imprisonment and/or a fine of not less than five hundred thousand (500,000) Dirhams any person who, by any authority granted thereto hereunder, has access to confidential information of a sensitive nature in electronic records, documents or correspondence, and intentionally discloses any of such information in violation of the provisions of this Decree Law.

2. The penalty shall be imprisonment and/or a fine of not less than two hundred and fifty thousand (250,000) Dirhams and not more than five hundred thousand (500,000) Dirhams, if the confidential information is not of a sensitive nature.The penalty shall be imprisonment and/or a fine of not more than five hundred thousand (500,000) Dirhams, if the negligence of the violator causes the disclosure of any sensitive or non-sensitive confidential information. The cases where information is disclosed for the purposes of implementing the provisions of this Decree Law or any judicial procedure shall be excluded from the provisions of Clause (1) of this Article.

Article (43)

Shall be punished by imprisonment for a period of not more than six months and/or a fine of not less than twenty thousand (20,000) Dirhams and not more than one hundred thousand (100,000) Dirhams whoever intentionally submits incorrect data to the Licensee in order to issue or cancel an Authentication Certificate.

Article (44)

Shall be punished by a fine of not less than fifty thousand (50,000) Dirhams and not more than two hundred and fifty thousand (250,000) Dirhams whoever:

1. Is licensed to provide Trust Services or Qualified Trust Services and has violated the provisions stipulated in this Decree Law, the Executive Regulations thereof and the decisions issued in implementation thereof with respect to these services.
2. Refuses to have its systems and operations from Trust Service Providers or Qualified Trust Service Providers audited by compliance assessment bodies in accordance with

the provisions of this Decree Law, the Executive Regulations thereof and the decisions issued in implementation thereof.

3. Publishes an announcement or provides a description regarding the Trust Services, Qualified Trust Services, or Qualified Trust Mark, with the intention of promoting or misleading, in contradiction with the decisions issued by TDRA.

Article (45)

Shall be punished by imprisonment and/or a fine of not less than five hundred thousand (500,000) Dirhams and not more than one million (1,000,000) Dirhams whoever:

1. Proceeds with any of the Trust Services or Qualified Trust Services without being licensed or exempted from obtaining a license in accordance with the provisions of this Decree Law, whether for the benefit of himself or others, or for the facilitation for others.
2. Deliberately alters, destroys or conceals any document or information requested by TDRA in accordance with the provisions of this Decree Law.

Article (46)

Without prejudice to the rights of bona fide third parties, the court shall order the confiscation of tools and devices used in committing any of the crimes provided for in this Decree Law.

Article (47)

Imposition of the penalties stipulated in this Decree Law shall not prejudice any more severe

penalty stipulated in any other law.

Article (48) Violations and Administrative Penalties

The Cabinet shall issue a decision specifying the acts that constitute a violation of the provisions of this Decree Law, the Executive Regulations thereof and the decisions issued in implementation thereof, as well as the administrative penalties to be imposed.

Article (49) Law Enforcement Capacity

The TDRA's employees who are designated by a resolution of the Minister of Justice, in agreement with the Chairman, shall act as law enforcement officers to identify the violations of the provisions of this Decree Law, the Executive Regulations thereof and the decisions issued in implementation thereof, within their respective competencies.

Chapter Five Final Provisions

Article (50) Transitional Provisions

Those who are subject to the provisions hereof shall regularize their status in accordance with the provisions of this Decree Law and the Executive Regulations thereof within a period not exceeding one year from the date of enforcement. Such period may be extended for another period or periods by a decision issued by the Cabinet based on a proposal of the Chairman.

Article (51) Fees

The Cabinet shall issue a decision determining the fees required for the implementation of the provisions of this Decree Law.

Article (52) Executive Regulations

The Cabinet shall, based on a proposal of the Chairman and after coordination with the Competent Authorities, issue the Executive Regulations of this Decree Law.

Article (53) Repeals

1. Federal Law No. (1) of 2006 on Electronic Commerce and Transactions shall be repealed.
2. Any provision contrary to or in conflict with the provisions of this Decree Law shall be repealed.
3. The decisions and regulations applicable prior to the enforcement of the provisions of this Decree Law shall remain applicable, without prejudice to the provisions of this Decree Law, until superseded by other decisions and regulations to be issued in accordance with the provisions of this Decree Law.

Article (54) Publication and Entry into force of the Decree Law

This Decree Law shall be published in the Official Gazette and shall enter into force as of 2 January 2022.

Khalifa bin Zayed Al Nahyan

President of the United Arab Emirates

Issued by us, at the Presidential Palace in Abu Dhabi:

On: 13 Safar 1443 AH

Corresponding to: 20 September 2021 AD