FEDERAL DECREE-LAW NO. (46) OF 2021
On Electronic Transactions and Trust Services

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,

- Having considered the Constitution; and
- Federal Law No. 1/1972 on the Competencies of Ministries and Powers of Ministers, as amended; and
- Federal Law No. 5/1985 promulgating the Civil Transactions Law, as amended; and
- Federal Law No. 10/1992 promulgating the Law of Evidence in Civil and Commercial Transactions, as amended; and
- Federal Law No. 11/1992 promulgating the Civil Procedure Law, as amended; and
- Federal Law No. 35/1992 promulgating the Penal Procedure Law, as amended; and
- Federal Law No. 4/2000 concerning the Emirates Securities and Commodities Authority and Market, as amended; and
- Federal Law by Decree No. (3) of 2003 on the Regulation of the Telecommunications Sector, as amended; and
- Federal Law No. 1/2006 on Electronic Commerce and Transactions, as amended; and
- Federal Law No. 29/2006 on the Rights of People with Special Needs, as amended; and
- Federal Law No. (4) of 2013 Regulating the Notary Public Profession, as amended; and
- Federal Law No. (5) of 2017 on the Use of Remote Communication Technology in Criminal Procedure, as amended; and
- Federal Law by Decree No. (14) of 2018 regarding the Central Bank and the Regulation of Financial Institutions and Activities, as amended; and
- Federal Law by Decree No. (14) of 2021 establishing the Federal Authority for Identity, Citizenship, Customs and Ports Security; and
- acting upon the proposal of the Minister of Cabinet Affairs and the approval of the Cabinet,

have issued the following Decree-Law:

Chapter One
DEFINITIONS & GENERAL PROVISIONS
Article (1)
Definitions

In applying this Decree-Law, the following terms and expressions shall have the following meanings, unless the context requires otherwise:

UAE or State	:	the United Arab Emirates.
Authority	:	the Telecommunications and Digital Government Regulatory Authority (TDRA).
Board of Directors	:	TDRA's Board of Directors.
Chairman	:	chairman of the Board of Directors.
Government Entity(ies)	:	Federal and local Government Entities.
Concerned Entities	:	Government Entities concerned with Data protection and cybersecurity matters in the State, and the ICP, as the case may be.
Federal Authority for Identity & Citizenship (ICP)	:	Federal Authority for Identity, Citizenship, Customs & Ports Security.
Electronic	:	electromagnetic, photoelectric, digital, optical or the like.
Electronic Transactions	:	any transaction, including contracts, agreements and other such transactions or services concluded, executed, provided or issued, in whole or in part, in Electronic form.
Electronic Dealing(s)	:	creating, signing, sending, receiving, saving or retrieving Electronic Documents.
Information Technology (IT) Means	:	any Electronic tool for performing logical and arithmetic operations, or for storing, sending and receiving Data.
Electronic Document	:	an Electronic record, Electronic message/e-mail, or an informational statement that is created, stored, extracted, copied, sent, communicated, or received by Information

		Technology Means, on any medium, and is retrievable in perceivable form.
Data	:	a set of facts, measurements and observations in the form of numbers, letters, symbols or special forms collected for use.
Electronic Information	:	any Data or information which can be stored, processed, generated and transmitted, through Information Technology Means, in the form of writings, images, audio, video, figures, letters, symbols, signs, etc.
Electronic Information System	:	a set of computer Software and Information Technology Means for creating, processing, managing, storing and exchanging Electronic Information or the like.
Originator	:	a Person by whom, or on whose behalf, an Electronic Document is created and sent, whichever the case may be. An Originator shall not be considered a Person who provides services in relation to processing, sending or saving that Electronic Document or other related services.
Addressee/Recipient/Consignee	:	a Person to whom an Originator intends to address an Electronic Document. An Addressee shall not be considered a Person who provides services in relation to receiving, processing or saving Electronic Documents or other related services.
Software	:	a set of Data, instructions and commands executable by Information Technology Means and designed to complete a task.
Automated Electronic Agent	:	an Electronic Information System that operates automatically and

		autonomously, in whole or in part, without intervention from a natural person at the time of operation or response.
Automated Electronic Transactions	:	transactions concluded or executed, in whole or in part, by an Automated Electronic Medium.
Verification Procedure	:	Electronic procedures aimed at establishing the identity of a Person or their legal representative, or confirming the origin and integrity of Data contained in an Electronic form, including any procedure that uses computational approaches, codes, words, identification numbers or encryption and other methods of Data safeguards.
Electronic Identification System	:	technical and regulatory procedures that use a Person's Data to establish their identity and capacity for the purpose of issuing their Electronic Identification Tools.
Electronic Identification Tool	:	any physical or non-physical tool issued through the Electronic Identification System, including personal identification factors or Data for the purpose of confirming a Person's identity.
Digital ID	:	a special Electronic Identification Tool allowing a Person to access and execute Electronic Transactions, Signatures and Seals with Government or non-Government Entities that adopt such tool as a channel to deliver their services.
Trust Services	:	Electronic services specified under Article 17(1) of this Decree-Law, which a Trust Service Provider (TSP) is authorized to provide as per the license granted thereto.

Qualified Trust Services (QTS)	:	Electronic services specified under Article 17(2) of this Decree-Law, which a Qualified Trust Service Provider (QTSP) is authorized to provide as per the license granted thereto.
Electronic Signature (Authentication) Certificate	:	a TSP-issued document in Electronic form, which links and attributes E-Signature verification Data to a particular Person and their own E-Signature to establish the name, identity or pseudonym of that Person.
Qualified E-Signature Certificate	:	an authenticated E-Signature document issued by a QTSP based on the Electronic Identification System and Verification Procedure, and compliant with TDRA-approved requirements in this regard.
Electronic Signature (E-Signature)	:	a signature consisting of letters, numbers, symbols, voice, fingerprint, or processing system of Electronic form, attached or logically linked to an Electronic Document, which verifies the identity of a Signatory and their acceptance of the Data content associated thereto.
Advanced E-Signature (AdES)	:	an Electronic Signature that meets the requirements set forth under Article (19) of this Decree-Law.
Qualified E-Signature (QES)	:	an Advanced E-Signature created by a Qualified E-Signature Device and issued based on a Qualified E-Signature Certificate.
Electronic Seal (E-Seal)	:	Data in Electronic form, related or logically linked to an Electronic Document, used to verify a Person’s identity, as well as the Data source origin and integrity therein.

Advanced E-Seal (AdESeal)	:	an E-Seal that meets the requirements set forth under Article (19) of this Decree-Law.
Qualified E-Seal	:	an Advanced E-Seal created by a Qualified E-Seal Device and issued based on a Qualified E-Seal Certificate.
E-Seal (Authentication) Certificate	:	a TSP-issued document in Electronic form, which links E-Seal verification Data to a legal person, establishing their name and identity.
Qualified E-Seal Certificate	:	an authenticated E-Seal document compliant with relevant TDRA-approved requirements and issued by a QTSP based on the Electronic Identification System and Verification Procedure.
E-Signature/E-Seal Creation Data	:	unique, Signatory-specific Electronic Data, to and of which the Signatory has full access and control, used to create an E-Signature or E-Seal.
Signatory	:	a Person creating an E-Signature or E-Seal.
E-Signature/E-Seal Device	:	systems, Software or devices used to create a different-level E-Signature/E-Seal in accordance with this Decree-Law.
Qualified Electronic Time Stamp	:	Data in Electronic form which binds a particular time to an Electronic Document establishing evidence that the latter Data existed at that time.
Qualified Electronic Delivery Service (QeDel)	:	a person-to-person Electronic Data transfer service indicating Data send/receive status and ensuring Data protection against loss, theft, damage or unauthorized modification, all while confirming their identity.
Person	:	a natural or legal person.
Relying Party	:	a Person who relies on Electronic Trust Services to provide own services or

		transactions, or perform any other action.
Qualified Trust Mark	:	a mark or sign proving that the TSP is qualified by TDRA to provide Qualified Electronic Trust Services.
Trust Service Provider (TSP)	:	a Licensee authorized by TDRA, in accordance with this Decree-Law and its Executive Order, to provide one or more Trust Services.
Qualified Trust Service Provider (QTSP)	:	a TSP granted the qualified status by TDRA to provide Trust Services and Qualified Trust Services accordingly.
Licensee	:	a legal person who is licensed by TDRA in accordance with the provisions of this Decree-Law and its Executive Order.
License	:	an authorization issued pursuant to the provisions of this Decree-Law and its Executive Order, according to which a Licensee is allowed to carry out any of the Trust Services or Qualified Trust Services.
UAE Trust List	:	a list prepared and published by TDRA, identifying TSPs, QTSPs, their services and Data relating thereto. It also checks the status of a License, and the extent of compliance with this Decree-Law, Executive Order, and the decisions issued by TDRA in implementation thereof;
Conformity Assessment	:	an audit conducted by TDRA or any other entity delegated by TDRA, to determine the extent of compliance of a License applicant and Licensees with the conditions, controls and standards adopted under this Decree-Law and the decisions issued in implementation thereof.

Coordinated Universal Time (UTC)	:	the primary time standard by which the world regulates clocks and time.

Article (2)
Scope of Application of the Decree-Law

1. The provisions of this Decree-Law shall apply to:
   a. Persons relying on Electronic Transactions, Trust Services and Qualified Trust Services as specified in accordance with this Decree-Law.
   b. Electronic Transactions, Electronic Documents, Trust Services, Qualified Trust Services and procedures for their completion.
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 it may also 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 in, encourage and facilitate all types of Electronic Transactions, and protect customers' rights.
2. Keep pace with technological development to boost Electronic Transactions across all sectors.
3. Encourage digital transformation, investment, and providing Electronic services to the public.

Article (4)
Competences of the Authority

For the purposes of applying the provisions of this Decree-Law, the Authority shall be competent with the following:

1. Organize the work and activities of Licensees, including issuing, renewing, amending, suspending and revoking Licenses, exemption from License or some or all of its conditions; confer or withdraw the qualified status, after ensuring that Licensees satisfy the rules, standards and requirements agreed upon with the Concerned Entities.
2. Issue controls, procedures and standards related to the Electronic Identification System, Verification Procedure and Digital ID, following coordination with the Concerned Entities.
3. Issue controls, procedures and standards of Trust Services and Qualified Trust Services, in particular the mechanism for creating, saving and validating E-Signatures, E-Seals and Electronic Documents signed/sealed Electronically, and specifications of the Qualified Trust Mark, following coordination with the Concerned Entities.

4. Assess a License applicant or Licensee by TDRA or by the Conformity Assessment body, and set rules and conditions regulating the work of Conformity Assessment entities.
5. Prepare, publish and update the UAE Trust List of Licensees, Trust Services and Qualified Trust Services.
6. Supervise, control and inspect Licensees, provided that coordination is made with the Central Bank of the UAE regarding the inspection of financial institutions licensed by it.
7. Receive and adjudicate complaints, and take necessary measures and procedures in their regard.
8. Any other functions assigned to TDRA by the Cabinet.

Chapter Two
ELECTRONIC TRANSACTIONS

Article (5)
Electronic Document

1. An Electronic Document is not without legal force and effect merely on the grounds that it is in Electronic form.
2. Data contained in Electronic Documents shall not lose their legal force as they were received - so far as details of such Data are accessible - within the Electronic Information System of their Originator(s), and reference was made in the Electronic Documents on the method of access.
3. Nothing in this Decree-Law shall compel any Person to use an Electronic Document without their consent.
4. A Person's consent to use an Electronic Document may be inferred from any conduct by them indicating the same.

Article (6)
Retention of Electronic Documents

1. Where any legislation in force in the State requires that documents, records or information be retained for any reason, then such requirement shall be met by retaining those documents, records or information in the form of an Electronic Document, while taking the following into account:
   a. The Electronic Document is retained in the format in which it was created, sent or received, or in a format which can accurately represent the original information created, sent or received.
   b. Saved information remains accessible so as to be usable for subsequent reference.
   c. Retaining information, if any, to enable identifying the origin and destination of an Electronic Document and the date/time it was sent or received.
2. An obligation to retain documents, records or information in accordance with Paragraph (c) of Clause (1) of this Article shall not

extend to any information necessarily and automatically created simply to enable the sending or receiving of a document.

3. A Person may fulfil the requirements stipulated in Clause (1) of this Article by using the services of any other Person so long as compliance with conditions in that Clause is met.
4. Government Entities may specify additional requirements that do not conflict with the provisions of this Decree-Law in order to retain Electronic Documents that fall within their purview.

Article (7)
Writing

If any applicable legislation in the State requires any information, statement, document, record, transaction or evidence be (made) in writing, or provides for certain consequences in the event of non-writing, the Electronic Document shall be deemed as satisfying this requirement if the information contained therein is saved in such a way allowing use and reference thereto.

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 provides for 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 signifying their intent with respect to the information contained in the Electronic Document.
   b. If the means used satisfies either of the following two conditions:
      1) It is qualified for the purpose for which the Electronic Document is created or sent.
      2) It meets the requirements set forth in Paragraph (a) of Clause (1) of this Article, either alone or with any other evidence.
2. Absent contrary statutory provision, a Person may use any form of Electronic authentication.

Article (9)
Original Document

If any legislation in force in the State requires the submission or retention of any document, record, information or message in its original form, that requirement shall be met by an Electronic Document if:

1. there exists reliable assurance as to the integrity of information contained in the Electronic Document from the time the document, record or information was first created in its final form, as an Electronic Document.
2. the Electronic Document allows, where required, viewing information to be submitted.

3. it complies with any additional conditions related to the submission or retention of Electronic Documents as determined by the Government Entity overseeing the submission or retention 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 by way of one or more Electronic Documents.

Article (11)
Automated Electronic Transactions

1. Contracting may be made between Automated Electronic Agents, including one or more Electronic Information Systems pre-set and pre-programmed to do so. Such contract shall be valid, enforceable and legally effective even if no natural person was personally or directly involved in the conclusion of the contract within said systems.
2. A contract may be made between an automated Electronic Information System in the possession of a Person, and another Person, where the latter knows, or is supposed to know, that such system will automatically conclude or execute the contract.

Article (12)
Attribution

1. An Electronic Document shall be deemed issued by an Originator if they themselves issued the same.
2. In the relationship between an Originator and a Recipient, an Electronic Document shall be deemed to be that of the Originator in the following cases:
   a. It is sent by a Person who has the authority to act on behalf of the Originator.
   b. It is sent by an Automated Electronic Agent programmed by or on behalf of the Originator to operate automatically.
3. In the relationship between an Originator and a Recipient, the latter shall have the right to consider that the Electronic Document as having been issued by the former, and act on that assumption, in the following cases:
   a. If the Recipient properly applies a procedure already approved by the Originator in order to ensure that the Electronic Document has been issued by the Originator for that purpose.
   b. If the Electronic Document, as received by the Recipient, is a result of the actions of a Person who, by virtue of their relationship with the Originator or any agent thereof, enable access to a

method used by the Originator to prove that the Electronic Document is issued therefrom.

4. The provisions of Clause (3) of this Article shall not apply to the following cases:
   a. If an Addressee receives a notice from the Originator that the Electronic Document has not been issued by them, provided that the Addressee is given sufficient time to act according to the notice.
   b. If the Recipient has known, or presumably knows, that the Electronic Document is not issued by the Originator.
   c. If it is unreasonable for the Recipient to deem an Electronic Document as having been issued by the Originator or to act on that assumption.
5. If an Electronic Document is issued or is deemed to have been issued by an Originator, or if an Addressee has the right to act on that assumption in accordance with Clauses (1), (2) and (3) of this Article, the Addressee may, in their relationship with the Originator, deem that the received Electronic Document is the document the Originator has intended to send, and to act accordingly.
6. An Addressee may treat every Electronic Document received thereby as a separate document, and to act accordingly. 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. Provisions of Clauses (5) and (6) of this Article shall not apply whenever the Addressee knows, or presumably knows, that an error has occurred in the Electronic Document as a result of a technical malfunction during transmission.

Article (13)
Acknowledgement of Receipt

1. If an Originator has not agreed with an Addressee that the acknowledgement of receipt shall be in a certain form or manner, the acknowledgment of receipt may be made by the following:
   a. any communication from the Addressee, whether by Electronic, automated or any other means.
   b. any conduct on the part of an Addressee sufficient to inform an Originator of the receipt of an Electronic Document.
2. If an Originator has stated that an Electronic Document is conditional on receiving an acknowledgment of receipt, this shall not entail any legal effect until the Originator receives the acknowledgment.
3. Without prejudice to Clause (2) of this Article, if an 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 they have not received any acknowledgment of receipt while allowing reasonable time during which the acknowledgment must be received. If such acknowledgment is not received within the specified

period, then the Electronic Document may be treated as if it has not been sent.

4. Clauses (1), (2) and (3) of this Article shall apply in cases where an Originator has requested or agreed with an Addressee, prior to or upon sending an Electronic Document, or by means of the Electronic Document, to send an acknowledgment of receipt of the same.
5. If an Originator receives an Addressee's acknowledgment of receipt, it is presumed, unless evidence to the contrary is adduced, that the Addressee has received the relevant Electronic Document. An acknowledgment of receipt shall not mean acknowledgment of the content of an Electronic Document.
6. If an acknowledgment of receipt received by an Originator states that a relevant Electronic Document has met the technical requirements, either agreed upon or set forth in applicable standards, it is presumed, unless proven otherwise, that those requirements have been met.
7. Provisions of this Article shall not apply if there is an agreement between an Originator of an Electronic Document and an Addressee to the contrary.

Article (14)
Time and Place of Sending and Receiving an Electronic Document

1. Unless an agreement is reached between an Originator and an Addressee on the place and time of sending and receiving an Electronic Document, the following shall apply:
   a. The dispatch of an Electronic Document occurs when it enters an information system outside the control of the Originator or the Person who sent the document on behalf thereof.
   b. The time of receipt of an Electronic Document shall be determined as follows:
      1) if an Addressee has designated an information system for the purpose of receiving an Electronic Document, receipt occurs at the time the Electronic Document enters the designated information system, or when the Addressee retrieves an Electronic Document sent to an information system belonging thereto, other than the information system designated to receive the document.
      2) If an Addressee has not designated an information system, receipt occurs when an Electronic Document enters an information system of that Addressee, notwithstanding that the place where the information system is located differs from the place where the Electronic Document is deemed to have been received in accordance with Clause (2) of this Article.
2. Unless otherwise agreed between an Originator and an Addressee, an Electronic Document shall be deemed to have been sent from the

Originator's place of business and received at that of the Addressee's.

3. In applying this Article:
   a. if an Originator or an Addressee has more than one place of business, the place of business shall be that which has the closest relevance to the respective transaction or, where there is no such transaction, the principal place of business.
   b. if an Originator or an Addressee has no place of business, the same shall be their respective habitual residences.
   c. the habitual residence of a legal person shall be the headquarters or their place of incorporation.

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 being granted the qualified status in accordance with the provisions of this Decree-Law and the Executive Regulations thereof.
3. Executive Regulations of this Decree-Law shall set the licensing terms, conditions, criteria and procedure referred to in this Article.

Article (16)

1. The Federal Authority for Identity & Citizenship (ICP) shall set the rules, criteria and requirements to be met by the License applicant, service provider or Qualified Service Provider, in the following two cases:
   a. Trust Services or Qualified Trust Services intended for the government sector.
   b. Trust Services or Qualified Trust Services that rely on the Data or services of the ICP.
2. TDRA shall verify that the License applicant, service provider or Qualified Service Provider meets the rules, criteria and requirements stipulated in Clause (1) of this Article.
3. TDRA shall suspend or revoke the License granted to a Trust Service Provider or a Qualified Trust Service Provider in the event of their violation of or non-compliance with the rules, criteria and requirements stipulated in Clause (1) of this Article.
4. TDRA shall coordinate with the ICP in all cases provided for in this Article.

Article (17)
Trust Services and Qualified Trust Services

Trust Services and Qualified Trust Services shall be determined as follows:

1. Trust Services, including:
   a. creation of an E-Signature and an Advanced E-Signature.
   b. issuance of an Advanced E-Signature (Authentication) Certificate.
   c. creation of an E-Seal and an Advanced E-Seal.
   d. issuance of an Advanced E-Seal (Authentication) Certificate.
   e. issuance of website authentication certificate.
2. Qualified Trust Services, including:
   a. Qualified E-Signature creation services, including:
      1) issuance of a Qualified E-Signature (Authentication) Certificate.
      2) issuance of an E-Signature Device.
      3) remote management of a Qualified E-Signature Device.
      4) Qualified E-Signature Data Preservation.
      5) Qualified E-Signature validation.
   b. Qualified E-Seal creation services, including:
      1) issuance of a Qualified E-Seal (Authentication) Certificate.
      2) issuance of a Qualified E-Seal Device.
      3) remote management of a Qualified E-Seal Device.
      4) Qualified E-Seal Data Preservation.
      5) Qualified E-Seal validation.
   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 Transaction as evidence in any legal proceeding shall not be precluded by the mere fact that it is in Electronic form, and has been processed through Trust Services and Qualified Trust Services.
2. A hard copy of an official Electronic Document shall have cogency against all to the extent it is conformant to the original of such document.
3. A Qualified E-Signature shall be deemed equally authentic to a handwritten signature and shall have the same legal effect so long as it meets the conditions stipulated in this Decree-Law and the Executive Regulation thereof.
4. A Qualified E-Seal of a legal person shall be evidence of authenticity and integrity of the original information with which such E-Seal is associated.
5. A qualified date and time shall be validated through a Qualified Electronic Time Stamp whenever it is linked to valid Data.
6. A Qualified Electronic Delivery Service shall be relied upon and have legal effect so long as it meets the conditions stipulated under this Decree-Law and the Executive Regulation thereof.

7. An Advanced E-Signature and an Advanced E-Seal shall be relied upon and have legal effect so long as the conditions prescribed by this Decree-Law and its Executive Regulation are met.
8. Trust Services and Qualified Trust Services shall meet the conditions as stipulated under this Decree-Law and the Executive Regulations thereof.

Article (19)
Advanced E-Signature and Advanced E-Seal

Electronic Signatures and Electronic Seals shall be Advanced once the following requirements are met:

1. They are completely and exclusively associated with Signatory and under their control.
2. They have a feature of identifying the Signatory.
3. They are linked to the signed Data in such a way as to detect any modification to that Data.
4. They are created using technical and security techniques in accordance with the technical requirements specified by the Executive Regulation of this Decree-Law.
5. Any other requirements specified by the Executive Regulation of this Decree-Law.

Article (20)
Qualified E-Signature and Qualified E-Seal

1. Qualified E-Signatures and Qualified E-Seals shall be valid once the following requirements are met:
   a. The E-Signature/E-Seal is created based on a valid, qualified authentication certificate in accordance with the provisions of this Decree-Law.
   b. The E-Signature/E-Seal is created using a Qualified E-Signature/E-Seal Device.
   c. The Qualified E-Signature/E-Seal validation Data matches the Data submitted to the Relying Party.
   d. Data identifying the Signatory of a qualified authentication certificate is properly submitted to the Relying Party, and in the event that personal Data concealment (pseudonymization) techniques are used, the Relying Party is informed of the same.
   e. They are created using technical and security techniques in accordance with the requirements specified by the Executive Regulation of this Decree-Law.
   f. Any other requirements specified by the Executive Regulation of this Decree-Law.
2. The Qualified E-Signature/E-Seal validation service shall be provided by a Qualified TSP in line with controls/rules issued by the Executive Regulation of this Decree-Law.
3. The Qualified E-Signature/E-Seal validation service shall provide the Relying Party with the correct result to substantiate the

Signature/Seal in an automated, effective and reliable manner, without relevant breaches.

4. The validation result of a Qualified E-Signature/E-Seal shall be signed with an Advanced E-Signature/E-Seal from a qualified service provider or in any other manner as determined by the Executive Regulation of this Decree-Law.

Article (21)
Qualified E-Signature and Qualified E-Seal Device Conditions

A Qualified E-Signature/E-Seal Device must satisfy the following conditions:

1. Ensure confidentiality of Creation Data of the E-Signature/E-Seal in use.
2. Protect the E-Signature/E-Seal Creation Data against any use by a third party or tampering using available technology.
3. One-time only creation of the E-Signature/E-Seal.
4. Not to modify the data to be signed or withheld from the Signatory before the signing or sealing process.
5. E-Signature Creation Data is managed or created on behalf of the Signatory by a QTSP according to the conditions, criteria and procedures established by the Executive Regulation of this Decree-Law.
6. Controls and procedures for the security and protection of qualified information are adhered to.
7. Any other conditions specified by the Executive Regulation of this Decree-Law.

Article (22)
Preservation of Qualified E-Signature/E-Seal Data

A QTSP shall, upon providing a Qualified E-Signature/E-Seal Data Preservation service, comply with procedures and techniques conducive to the continuity of Trust Services, and ensure continued validity of Qualified E-Signatures subject to the terms and duration prescribed by the Executive Regulation of this Decree-Law.

Article (23)
Qualified Electronic Time Stamp

A Qualified Electronic Time Stamp must fulfil the following requirements:

1. Binds the date and time to Data in such a manner as to reasonably preclude undetectable changes to the Data.
2. Based on an accurate time source linked to UTC.
3. Signed with an Advanced E-Signature or sealed with an Advanced E-Seal of a QTSP or by any other method specified by the Executive Regulation of this Decree-Law.

4. Any other requirements specified by the Executive Regulation of this Decree-Law.

Article (24)
Qualified Electronic Delivery Service

A Qualified Electronic Delivery Service must fulfil the following requirements:

1. To be provided by one or more QTSPs.
2. Ensure a highly secure and trustable identification of the sender, as specified by the Executive Regulation of this Decree-Law.
3. Ensure identification of the Consignee prior to the delivery of Data.
4. Data transmitted is signed with an Advanced E-Signature or sealed with an Advanced E-Seal of a QTSP or by any other method specified by the Executive Regulation of this Decree-Law.
5. Indicate to both the sender and receiver any necessary, service-required change to the transmitted Data.
6. The date of sending, receipt and any change of Data must be indicated by a Qualified Electronic Time Stamp;
7. Any other requirements specified by the Executive Regulation of this Decree-Law.

Article (25)
Authentication Certificates

1. An Authentication Certificate shall no longer be valid as of the date of its revocation. Such revocation shall not apply retroactively to any E-Signature/E-Seal made based on such certificate prior to that date.
2. No Person may publish an Authentication Certificate if they are aware of its invalidity or revocation, or if the Person to whom it is addressed has refused to receive it.

Article (26)
Qualified Trust Mark

When using a Qualified Trust Mark, a QTSP shall adhere to the following:

1. Refer to the Qualified Trust Services they are licensed to provide.
2. Bind the mark to a publically available Electronic link on their website redirecting to the UAE Trust List published by TDRA.

Article (27)
UAE Trust List

1. TDRA shall create a list of Licensees and their services and a list of the Electronic Identification System and Qualified E-Signature/E-Seal Devices, include the same 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 basic information about the QTSPs and their provided QTSs, and details of the Qualified E-Signature/E-Seal Devices.

3. The Executive Regulation shall set 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 shall require a Person to use or accept an Electronic Dealing, however, that Person's consent to the same may be inferred from any conduct thereof indicating such consent.
2. A Person may use any form of E-Signatures/E-Seals, unless otherwise provided for by the legislation in force.
3. The Digital ID issued in accordance with the requirements of the Electronic Identification System approved by TDRA, in coordination with the ICP, shall be adopted as a means of accessing services and Electronic Transactions/Dealings provided by Government Entities.
4. The use of a Digital ID issued through the Electronic Identification System to access government E-services shall be deemed compliant with the requirements of identification and personal presence so long as the Digital ID provides the level of trust and security required for dealing with these services in accordance with the provisions of this Decree-Law.
5. Government Entities shall accept the use of Persons' E-Signatures, E-Seals and Digital IDs, or the use of Electronic Documents in Electronic services provided by those Entities, other Government Entities, or by whoever they delegate as per the manner/form, standards and levels of trust and security determined by TDRA.
6. Government Entities may, within their respective purviews established in applicable legislation, make Electronic Transactions, of equal legal effect, in the following situations:
   a. accepting the deposit, submission, creation or retention 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 rendering payments in Electronic form.
   d. tendering and receiving/awarding bids related to government procurement by Electronic means.
7. Should a Government Entity decide to perform any of the actions outlined in Clause (6) of this Article, the Government Entity may specify:
   a. the manner or form in which such Electronic Documents shall be created, filed, retained, submitted or issued.
   b. controls, terms and procedures for tendering, receiving and awarding bids, and concluding government procurement.
   c. the form of E-Signature/E-Seal and required security level.
   d. the manner and form in which such signature or seal shall be affixed to the Electronic Document, and the technical criteria to be met by the TSP to whom the document is submitted for filing and retention.

e. oversight processes, controls and procedures for the integrity, safety, security and confidentiality of Electronic Documents, payments or fees.
f. terms and conditions for sending paper documents, if required in relation to Electronic Documents of payments and fees.

8. Government Entities shall archive Electronic Documents affixed with an Advanced or Qualified E-Signature/E-Seal in accordance with the controls established by Executive Regulation of this Decree- Law.

Article (29)
Responsibility of the Relying Party

1. A Relying Party shall be held responsible for the consequences of own failure to take the necessary measures to ascertain the validity and enforceability of an Authentication Certificate, and shall observe any restrictions thereon.
2. A Relying Party shall be held responsible for the consequences of own failure to take the necessary measures to ascertain the validity and enforceability of a Digital ID, if used.
3. In order to trust and rely upon an E-Signature/E-Seal, a Relying Party shall observe the following:
   a. Determine the security level of the E-Signature/E-Seal according to the nature, value or importance of the transaction intended to be supported by the E-Signature/E-Seal.
   b. Take the necessary measures to verify the identity of the Signatory and validate the Authentication Certificate.
   c. Take the necessary measures to verify that the E-Signature/E-Seal used meets the requirements.
   d. The extent of its awareness or presumed knowledge that the E-Signature, E-Seal or Electronic (Authentication) Certificate has been violated or revoked.
   e. Previous agreement or dealing between the Signatory and the party relying on the E-Signature, E-Seal or Authentication Certificate.
   f. Any other relevant factors.
4. If the reliance on an E-Signature/E-Seal is unacceptable according to Clause (3) of this Article, the party relying thereon shall bear the risk of invalidity of such signature/seal and shall be responsible for any damage to the signer, sealer or third parties.

Article (30)
Responsibility of the Signatory

A Signatory shall bear consequences of its failure to observe the following procedures:

1. exercising due diligence to avoid unauthorized use of E-Signature/E-Seal Creation Data.

2. notifying the concerned Licensee upon learning that their E-Signature/E-Seal Creation Data used to create such signature or seal has been compromised in terms of security and validity.
3. ensuring the accuracy and completeness of material Data submitted thereby in relation to the Authentication Certificate throughout its validity period, in cases where using such certificate is required.
4. reporting any changes to the information contained in the Authentication Certificate or if it is no longer confidential.
5. using valid Authentication Certificates.

Article (31)
Responsibility of the Digital ID Holder

A Digital ID holder shall bear consequences of its failure to take the following actions:

1. exercising due diligence to avoid unauthorized use of the Digital ID.
2. immediately notifying the relevant entities and Persons upon learning that a Digital ID used in a service or Electronic Dealing has been exposed to what raises doubts about its security.
3. ensuring the accuracy and completeness of material Data provided thereby in relation to the Digital ID throughout its validity period.

Article (32)
Accessibility to Trust Services by People of Determination

Trust Services and Qualified Trust Services should, wherever possible, be made available to a natural person of the people of determination, in accordance with procedures and techniques that suit their needs or the nature of their own condition.

Article (33)
Electronic Identification System Security Levels

1. Security and trust levels of the Electronic Identification System and Digital ID issued thereby are on three levels: low, medium and high, according to the following general classifications:
   a. Low level: a low level of security and trust in an Electronic Identification System provides a limited degree of trust and acceptance of a Person's alleged identity, and refers to technical and administrative standards and procedures to mitigate the risk of misuse of or tampering with that identity.
   b. Medium level: a medium level of security and trust in an Electronic Identification System provides an average degree of trust and acceptance of a Person's alleged identity, and refers to technical and administrative standards and procedures to substantially mitigate the risk of misuse of or tampering with that identity.
   c. High level: a high level of security and trust in an Electronic Identification System provides an increased level of trust and acceptance of a Person's alleged identity, and refers to technical

and administrative standards and procedures to eliminate any risks and prevent misuse of or tampering with that identity.

2. A Licensee shall observe the following:
   a. Indicate to the Relying Party the levels of security and trust of a Digital ID issued under an Electronic Identification System.
   b. Ensure that technical specifications, standards and procedures of the relevant security level are met in the Electronic Identification System and Digital ID as approved by the TDRA.
3. A Digital ID used in Qualified Trust Services must meet the High level of security and trust.
4. TDRA shall, following coordination with Concerned Entities, develop technical requirements and standards to be met in security and trust levels, while bearing in mind the following:
   a. Develop criteria for differentiating between levels of security and trust according to trustability and acceptability.
   b. Verification Procedure for a Person requesting the issuance of a Digital ID.
   c. Digital ID technical & security specifications, issuance procedures and issuer.
   d. Verification Procedure to confirm the identity of any Person to the Relying Party.
   e. Types of transactions and services provided by Government Entities or the private sector.

Article (34)
Issuance of Authentication Certificates

Upon issuing a qualified Authentication Certificate, the QTSP shall verify the identity and capacity of the Person to whom the certificate will be issued, by way of one of the following methods:

1. Presence of the Person or legal representative of the legal person.
2. Use of a Digital ID that meets the High security level requirements set forth in this Decree-Law.
3. Qualified E-Signature/E-Seal Authentication Certificate issued by another QTSP.
4. Any procedure applicable in the UAE that is equivalent to a Person's presence, in accordance with the conditions and procedures specified by the Executive Regulations of this Decree-Law.

Article (35)
Licensee Obligations

A Licensee shall commit to:

1. Notify TDRA, Concerned Entities and the Person concerned, of any violation or breach of Data security and integrity upon learning of such violation or within the period decided by TDRA.
2. Indicate to the Relying Party the security and trust levels of the Electronic Identification System-issued Digital ID.

3. Ensure that the technical and security specifications, standards and procedures of the required security level are met in the Electronic Identification System as approved by TDRA.
4. Submit a biennial report issued by the Conformity Assessment body to TDRA regarding (the Licensee's) compliance with terms of the License issued thereto and the decisions issued thereby.
5. Protect personal Data and implement controls and procedures in accordance with the requirements of competent authorities and the legislation in force.
6. Take all necessary measures to manage risks that may arise to ensure security and integrity of Electronic Trust Services and Qualified Trust Services, in a way that prevents security incidents or breaches from occurring, or mitigates them should they occur.
7. Prepare a service termination plan in accordance with the requirements set by the Executive Regulations of this Decree-Law.
8. Any other obligations determined by the Executive Regulations of this Decree-Law or other applicable legislation in the UAE.

Article (36)
Obligations of QTSPs

A QTSP shall adhere to:

1. Their License terms and conditions.
2. Guaranteeing the accuracy of material Data in Electronic Authentication Certificates throughout their validity period.
3. Providing an appropriate means for Signatories to report any incident casting doubt on any of the services provided thereby in accordance with their (the QTSP's) License.
4. Providing the Authentication Certificate revocation service.
5. Notifying TDRA of any Data modification in the License application or of their (the QTSP's) wish to cease providing the same, subject to the conditions and procedures specified by the Executive Regulations of this Decree-Law.
6. Using technically reliable systems and products that guarantee technical security and are protected against any changes, modifications or breaches, as determined by TDRA and as approved by Concerned Entities in this regard.
7. Retaining Electronic Documents, E-Signatures, E-Seals and identification evidence for the period prescribed by TDRA.
8. Personal Data processing according to legislation in effect and stipulations of this Decree-Law.
9. Creating and maintaining an updated database of Authentication Certificates in case the Authentication Certificate service is provided by the QTSP.
10. Devising an updated E-Trust Service termination plan to ensure service continuity.
11. Refraining from providing services if there is doubt as to the accuracy of Data or validity of the document submitted to verify the information

provided for identification or vindication of right to representation, or if there is an impediment or a security risk.

12. Relying on official data sources of Persons in the UAE in delivering any of the Qualified Trust Services provided for under their (the QTSP's) License.
13. Any other obligations determined by the Executive Regulations of this Decree-Law or other applicable legislation in the UAE.

Article (37)
International Trust Services

Qualified Trust Services provided by QTSPs outside the UAE shall be recognized if they are on a comparable level to those provided by other QTSPs as provided for in this Decree-Law and decisions of TDRA.

Article (38)
Civil Liability

TSPs shall bear civil liability for any damage to any Person for breach of obligations under this Decree-Law and its Executive Regulations and the decisions issued by TDRA.

Chapter Four
PENALTIES
Article (39)

Shall be punished by imprisonment and/or a fine of no less than one hundred thousand (100,000) Dirhams and no more than three hundred thousand (300,000) Dirhams, whoever forges or is involved in the forgery of an Electronic Document, Electronic Signature, Electronic Seal, Authentication Certificate or Trust Services and other Qualified Trust Services.

Shall be punished by temporary imprisonment and a fine of no less than one hundred and fifty thousand (150,000) Dirhams and no more than seven hundred and fifty thousand (750,000) Dirhams, whoever forges or is involved in the forgery of an Electronic Document, Electronic Signature, Electronic Seal, Authentication Certificate or Trust Services and other Qualified Trust Services of the federal/local government or federal/local public authorities or organizations.

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

Article (40)

Shall be penalized with imprisonment for no more than a year and/or fined with no less than one hundred thousand (100,000) Dirhams and no more than one million (1,000,000) Dirhams, whoever:

1. unrightfully uses any Trust Service or Qualified Trust Service.
2. uses fraud/scam, assumes false name or incorrect capacity to obtain a Qualified Trust Service.

Committing any of the foregoing acts with the intent to perpetrate a crime shall be considered an aggravating circumstance.

Article (41)

Shall be penalized with imprisonment for no more than a year and/or a fine of no less than fifty thousand (50,000) Dirhams and no 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 has not been issued by the Licensee whose name appears thereon.
2. The Certificate has been rejected by the Signatory whose name appears thereon.
3. The Certificate has been revoked, unless the purpose of publication is to confirm any E-Signature or E-Seal used prior to such revocation.
4. The Certificate contains incorrect Data.

Article (42)

1. Shall be penalized by temporary imprisonment and/or a fine of not less than five hundred thousand (500,000) Dirhams any Person who, by any power vested therein hereunder, has access to confidential information of sensitive nature in Electronic records, documents or correspondence, and who deliberately discloses any of such information in violation of the provisions of this Decree-Law.
   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 in question is not sensitive in nature.
   A further penalty of imprisonment and/or a fine of not more than five hundred thousand (500,000) Dirhams shall be imposed, should their negligence cause the disclosure of any sensitive or non-sensitive confidential information.
2. Cases of information disclosure that are made for the purposes of enforcing this Decree-Law or taking any legal action, shall be excluded from Clause (1) of this Article.

Article (43)

Shall be punished by imprisonment for a period not exceeding six months and/or a fine of no less than twenty thousand (20,000) Dirhams and no more than one hundred thousand (100,000) Dirhams, whoever deliberately submits incorrect Data to a Licensee for issuing or revoking an Authentication Certificate.

Article (44)

Shall be penalized with a minimum fine of fifty thousand (50,000) Dirhams up to a maximum of 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, its Executive Regulations and the decisions issued in implementation thereof, with respect to such services.
2. Refuses to subject their systems and processes from TSPs or QTSPs to auditing by Conformity Assessment bodies according to this Decree-Law, its Executive Regulations and the decisions issued in implementation thereof.
3. Disseminates/releases/makes an announcement or provides a description of Trust Services, Qualified Trust Services or a Qualified Trust Mark, with the intent of promotion or misinformation/misleading, contrary to the decisions of TDRA.

Article (45)

Shall be penalized with imprisonment and/or fined with no less than five hundred thousand (500,000) Dirhams and no more than one million (1,000,000) Dirhams, whoever:

1. Conducts 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 own or other's benefit, or in facilitation of the same for others.
2. Intentionally alters, destroys or conceals any document or information requested by TDRA pursuant to 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)

The imposition of penalties prescribed by this Decree-Law shall not prejudice a stricter penalty prescribed by any other law.

Article (48)
Administrative Violations and Penalties

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

Article (49)
Judicial Officers (Law Enforcement Capacity)

TDRA's employees designated by decision of the Minister of Justice, in agreement with the Chairman, shall be bestowed the status of judicial officers in establishing violations to the provisions of this Decree-Law, its Executive Regulations, and the decisions issued in implementation thereof, within their respective purviews.

Chapter Five
FINAL PROVISIONS

Article (50)
Transitional Provisions

Those who are subject to this Decree-Law shall adjust/regularize their status/situation according to its provisions and those of its Executive Regulations within a period not exceeding one year as of the date of its coming into force. Such period may be extended for another period(s) by decision of the Cabinet based on the Chairman's proposal.

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–upon the Chairman's proposal and after coordination with Concerned Entities–issue the Executive Regulations of this Decree-Law.

Article (53)
Repeals/Abrogation

1. Federal Law No. 1/2006 on Electronic Commerce and Transactions shall be repealed.
2. Any provision contrary to the provisions of this Decree-Law shall be abrogated.
3. Applicable decisions and regulations prior to the coming into force of this Decree-Law shall remain applicable, in a manner not inconsistent with its provisions, until superseded/replaced under the provisions of this Decree-Law.

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

This Decree-Law shall be published in the Official Gazette, with effect from 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/1443H
Corresponding: 20/September/2021