Law No. (2) of 2002

Concerning Electronic Transactions and E-Commerce[1]

We, Maktoum bin Rashid Al Maktoum, Ruler of Dubai,

Seeking to achieve the Government of Dubai objective of utilising modern technological means in commercial transactions and trade exchange,

Do hereby issue this Law.

Chapter One

Definitions
Article (1)

This Law will be cited as "Law No. (2) of 2002 Concerning Electronic Transactions and E-Commerce".

Article (2)

The following words and expressions will have the meaning indicated opposite each of them unless the context implies otherwise:

Government:	The Government of Dubai, including any of the Government departments or the public agencies and authorities affiliated to the Government.
Emirate:	The Emirate of Dubai.
Chairman:	The chairman of the Dubai Technology, E-Commerce, and Media Free Zone Authority.
Electronic:	Anything relating to modern technology and having electrical, digital, magnetic, wireless, optical,

[1] *Every effort has been made to produce an accurate and complete English version of this legislation. However, for the purpose of its interpretation and application, reference must be made to the original Arabic text. In case of conflict, the Arabic text will prevail.*

	electromagnetic, automated, photonic, or similar capabilities.
Electronic Information:	Electronic data in the form of text, codes, sounds, graphics, images, Computer programmes, or any other type of databases.
Electronic Information System:	An Electronic System used for creating, generating, sending, receiving, storing, displaying, or processing Information and messages electronically.
Electronic Record or Document:	A record or document that is created, stored, generated, copied, sent, communicated, or received electronically, on a tangible medium or any Electronic medium; and that is retrievable in a perceivable form.
Computer:	An Electronic device that processes information and data by analysing, programming, displaying, saving, sending, and receiving it through Electronic Information programmes and systems; and that can function independently or in communication with other Electronic devices or systems.
Originator:	A natural or legal person by whom or on whose behalf an Electronic Message is sent, as the case may be. This does not include an entity that acts as service provider in respect of producing, processing, sending, or storing the Electronic Message or any other related services.
Addressee:	A natural or legal person who is intended by the Originator to receive the Electronic Message. This does not include a person who provides services in relation to receiving, processing, or storing the Electronic Message or any other related services.
Computer Programme:	A set of data or instructions used directly or indirectly in an Electronic Information processing system for the purpose of creating or accomplishing specific results.
Electronic Message:	Electronic Information sent or received electronically, regardless of the method of retrieval at the place of receipt.

Electronic Communication:	Sending and receiving Electronic Messages.
Electronic Signature:	A signature comprising letters, numbers, symbols, a sound, or an electronic process attached to or logically associated with an Electronic Message with the intention of authenticating or approving the same.
Secure Electronic Signature	An Electronic Signature which meets the requirements set out in Article (20) of this Law.
Signatory:	A natural or legal person who holds an Electronic Signature Creation Device and by whom or on whose behalf a signature is applied to an Electronic Message through the use of that device.
Electronic Signature Creation Device:	A uniquely configured device or Electronic Information that is designed to create, independently or in conjunction with other devices or Electronic Information, an Electronic Signature of a specific person. This process involves any systems or devices which generate or capture unique information, such as codes, algorithms, letters, numbers, private keys, personal identification numbers, or personal attributes.
Automated Electronic Agent:	A Computer Programme or Electronic system used to initiate an action or response independently, in whole or in part, without supervision by a natural person at the time of the action or response.
Automated Electronic Transactions:	Transactions which are concluded or performed, in whole or in part, using Electronic means or Electronic Records; and in which, unlike in the regular course of concluding and performing contracts and transactions, the relevant acts and records are not subject to monitoring or review by a natural person.
Attestation Service Provider:	An accredited or recognised person or entity that issues Electronic Attestation Certificates; or performs any services or duties related to these certificates, or to the Electronic Signatures, regulated pursuant to the provisions of Chapter Five of this Law.

Electronic Attestation Certificate:	A certificate issued by an Attestation Service Provider confirming the identity of a person or entity holding an Electronic Signature Creation Device.
Secure Authentication Procedures:	Procedures aimed at verifying that an Electronic Message is originated by a specific person and detecting any error or alteration in the content, communication, or storage of an Electronic Message or Electronic Record during a specific period of time. These may involve the use of algorithms, codes, identifying words or numbers, encryption, callback or acknowledgement procedures, or any other information protection procedures.
Relying Party:	A party that acts in reliance on an Electronic Attestation Certificate, or an Electronic Signature.
Electronic Transaction:	Any transaction, contract, or agreement concluded or performed, in whole or in part, through Electronic Communications.
E-Commerce:	Commercial transactions conducted through Electronic Communications.

Interpretation
Article (3)

This law will be interpreted in line with the common practice in Electronic Transactions and E-Commerce and in a way that achieves the following objectives:

1. to facilitate Electronic Communications by means of reliable Electronic Records;

2. to facilitate E-Commerce and other Electronic Transactions, and eliminate any obstacles facing the same as a result of any uncertainty related to the relevant writing and signing requirements; and to promote the development of the legal and business infrastructure required for implementing secure E-Commerce;

3. to facilitate the exchange of Electronic documents with Government entities and agencies and enhance the efficiency of service delivery by these entities and agencies by means of reliable Electronic Communications;

4. to minimise the incidence of forgery in Electronic Communications, alteration of the same, and fraud in E-Commerce and other Electronic Transactions;

5. to establish uniform rules, regulations, and standards for the authentication and validation of Electronic Communications;

6. to enhance public trust in the validity and authenticity of Electronic Transactions, Electronic Communications, and Electronic Records; and

7. to promote the development of E-Commerce and other transactions on the national and international levels through the use of Electronic Signatures.

Article (4)

In implementing the provisions of this Law, the international commercial custom relating to Electronic Transactions and E-Commerce, and the relevant technological advances in communicating the same, will apply.

Scope of Application
Article (5)

1. This Law applies to Electronic Records and Electronic Signatures that relate to Electronic Transactions and E-Commerce, but does not apply to:

   a. transactions and matters relating to family affairs, such as marriage, divorce, and wills;

   b. deeds of title to immoveable property;

   c. negotiable bonds;

   d. transactions involving the sale, purchase, lease (for a term of more than 10 years), and other dispositions of immoveable property; and the registration of any other rights relating to immoveable property; and

   e. any document legally required to be attested by a notary public.

2. The Chairman may, pursuant to a decision issued by him, add to, delete from, or otherwise amend, the list of transactions and matters stated in sub-paragraph (1) of this Article.

Acceptance of Electronic Transactions
Article (6)

1. Nothing in this Law requires any person to use or accept information in Electronic format. However, a person's consent to use or accept the same may be inferred from his affirmative conduct.

2. Any parties involved in generating, sending, receiving, storing, or processing Electronic Records may agree to enter into contracts without compliance with the provisions of Chapter Two through Chapter Four of this Law.

3. Notwithstanding the provisions of paragraph (1) of this Article, the Government must express explicit consent to dealing electronically in transactions to which it is a party.

Chapter Two
Electronic Transaction Requirements

Electronic Communications
Article (7)

1. An Electronic Message will not cease to be legally effective or enforceable merely on the grounds that it is in Electronic format.

2. Any information referred to in an Electronic Message, without providing details, will not cease to be legally effective or enforceable so long as the details of the same are accessible in the Electronic System of the Originator and the Electronic Message indicates the method of accessing the same.

Retention of Electronic Records
Article (8)

1. Where the law requires that certain documents, records or information be retained for any reason, that requirement will be met by retaining the same in an Electronic Record subject to the following conditions:

    a. The Electronic Record must be retained in the format in which it was generated, sent, or received; or in a format which can be demonstrated to represent accurately the original information generated, sent, or received.

    b. The relevant information must remain accessible for subsequent use and reference.

    c. The information that enables the identification of the Originator , the destination of the Electronic Message, and the date and time of sending and receiving it must be retained.

2. The obligation to retain documents, records, or information in accordance with sub-paragraph (1)(c) of this Article does not extend to any information necessarily or automatically generated solely for the purpose of enabling a record to be sent or received.

3. A person may satisfy the requirements stipulated in paragraph (1) of this Article by engaging the services of any other person, provided that he fulfils the requirements stipulated in that paragraph.

4. Nothing in this Article will prejudice:

   a. the provisions of any law which expressly stipulates the retention of documents, records, or information in the form of Electronic Records using a specific Electronic Information System or through specific procedures, or their retention or communication through a specific Electronic Agent; or

   b. the Government's power to prescribe additional requirements for the retention of Electronic Records that fall within its jurisdiction.

Writing
Article (9)

If the law requires that any statement, document, record, transaction, or proof be in writing, or provides for certain consequences in case of failure to meet this requirement, an Electronic document or Electronic Record will be deemed to have satisfied that requirement if the provisions of paragraph (1) of the preceding Article are complied with.

Electronic Signature
Article (10)

1. Where the law requires that a signature be affixed to a document, or provides for certain consequences in the absence of a signature, that requirement will be deemed satisfied if the document contains a reliable Electronic Signature as per the meaning of Article (21) of this Law.

2. Unless otherwise provided by law, a person may use any form of Electronic authentication.

Electronic Original
Article (11)

An Electronic document or Electronic Record will be deemed an original document or record if it is processed through a tool that:

1. provides a reliable technical assurance as to the validity of the information contained in the document or record at the time when it was first generated in its final form as an Electronic document or Electronic Record; and

2. allows the display of the relevant information upon request.

Acceptance and Evidential Value of Electronic Proofs
Article (12)

1. An Electronic Message or Electronic Signature may not be denied as evidence:

    a. merely on the grounds that the message or signature is in Electronic format; or

    b. merely on the grounds that the message or signature is not original or is not in its original form, provided that the message or signature is the best evidence reasonably expected to be obtained by the person relying on it.

2. Electronic Information will have its due evidential value. In assessing the evidential value of Electronic Information, the following will be taken into consideration:

    a. the reliability of the manner in which one or more of the operations of entering, creating, processing, storing, presenting or communicating is performed;

    b. the reliability of the manner in which the validity of the information is maintained;

    c. the reliability of the source of information, if identifiable;

    d. where applicable, the reliability of the manner in which the Originator is identified; and

    e. any other factor that may be relevant.

3. In the absence of proof to the contrary, a Secure Electronic Signature will be presumed:

    a. to be reliable;

    b. to be the signature of the person to whom it is attributed; and

    c. to be affixed by that person with the intention of signing or approving the Electronic Message to which it is applied or with which it is reasonably associated.

4. In the absence of proof to the contrary, a Secure Electronic Record will be presumed:

    a. to have remained unaltered since its creation; and

    b. to be reliable.

Chapter Three
Electronic Transactions

Formation and Validity of Contracts
Article (13)

1. For the purpose of contracting, an offer or the acceptance of an offer may be expressed, in whole or in part, by Electronic Communication.

2. A contract will not cease to be valid or enforceable merely on the grounds that one or more Electronic Communication has been used in its formation.

Automated Electronic Transactions
Article (14)

1. A contract may be formed through the interaction of Automated Electronic Agents that include two or more Electronic Information Systems pre-set and pre-programmed to carry out the relevant tasks. The contract will be valid and enforceable even if there is no direct intervention by a natural person in the conclusion of the contract in these systems.

2. A contract may be formed between an automated Electronic Information System that belongs to a natural or legal person and another natural person, provided the latter is aware or is presumed to be aware that the system will conclude or perform the contract.

Attribution
Article (15)

1. An Electronic Message is deemed to have been dispatched by the Originator if it is sent by the Originator himself.

2. As between the Originator and the Addressee, an Electronic Message is deemed to be dispatched by the Originator if it is sent:

    a. by a person who has the authority to act on behalf of the Originator in respect of the Electronic Message; or

    b. by an automated Electronic Information System programmed by or on behalf of the Originator to operate automatically.

3. As between the Originator and the Addressee, the Addressee may presume that an Electronic Message is dispatched by the Originator, and may act upon this presumption, if:

    a. the Addressee correctly follows a procedure previously agreed upon with the Originator for verifying that the Electronic Message is dispatched by the Originator; or

    b. the Electronic Message, as received by the Addressee, is dispatched as a result of the acts of a person who, by virtue of his relationship with the Originator or with any of the Originator's agents, has managed to access a method used by the Originator to prove that the Electronic Message is dispatched by him.

4. The provisions of paragraph (3) of this Article will not apply:

    a. as of the time when the Addressee receives a notification from the Originator informing the Addressee that the Electronic Message has not been dispatched by him, provided that the Addressee has enough time to act upon this notification;

    b. where the Addressee is aware that the Electronic Message has not been dispatched by the Originator, or would have become aware of that fact had he exercised reasonable care or followed any agreed-upon procedure; and

    c. where it is not reasonable for the Addressee to presume that the Electronic Message has been dispatched by the Originator, or to act upon that presumption.

5. Where the Electronic Message is dispatched or is deemed to have been dispatched by the Originator, or where the Addressee is entitled pursuant to paragraphs (1), (2), and (3) of this Article to act upon that presumption, the Addressee may, as between him and the Originator, presume that the received Electronic Message is intended to be sent by the Originator, and to act accordingly.

6. An Originator is entitled to presume that each Electronic Message he receives is independent and to act solely based on this presumption. Paragraph (7) of this Article will not apply where the Addressee is aware that the Electronic Message is a second copy, or would have become aware of that fact had he exercised reasonable care or followed any agreed-upon procedure.

7. The Addressee is not entitled to adopt any of the presumptions or conclusions set forth in paragraphs (5) and (6) of this Article if he is aware that the dispatch has resulted in any error in the Electronic Message received by him, or would have become aware of that fact had he exercised reasonable care or followed any agreed-upon procedure.

Acknowledgement of Receipt
Article (16)

1. The provisions of paragraphs (2), (3) and (4) of this Article will apply if the Originator requests or agrees with the Addressee, on or before sending the Electronic Message or in this message, to acknowledge the receipt of the message.

2. Where the Originator has not agreed with the Addressee that the acknowledgement be made in a particular form or using a particular method, the acknowledgement of receipt may be made by:

   a. any Electronic, automated, or other message sent by the Addressee; or

   b. any conduct by the Addressee,

   which is sufficient to inform the Originator that the Electronic Message has been received.

3. Where the Originator has stated that the Electronic Message is conditional upon the receipt of the acknowledgement, the Electronic Message will be treated as if it had never been sent, in respect of creating any legal rights and or obligations between the Originator and the Addressee, until the acknowledgement is received by the Originator.

4. Where the Originator requests an acknowledgement but does not state that the Electronic Message is conditional upon the receipt of that acknowledgement within a specific or agreed-upon deadline, or within a reasonable period if no deadline is specified or agreed upon, the Originator may:

   a. serve notice on the Addressee stating that no acknowledgement has been received and specifying a reasonable deadline within which the acknowledgement must be received; and

   b. upon sending a notice to the Addressee, treat the Electronic Message as if it has never been sent, or exercise any other rights to which he is entitled, if the acknowledgement is not received within the deadline mentioned in sub-paragraph (4)(a) of this Article.

5. Where the Originator receives the Addressee's acknowledgement of receipt, it will be presumed, unless evidence to the contrary is provided by the Addressee, that the relevant Electronic Message has been received by the Addressee. However, this presumption does not imply that the content of the Electronic Message sent by the Originator corresponds to the content of the message received by him from the Addressee.

6. Where the acknowledgement received by the Originator states that the relevant Electronic Message meets the technical requirements agreed upon or determined by the applicable standards, it will be presumed, unless the contrary is established, that those requirements have been met.

7. Except as it relates to sending or receiving an Electronic Message, this Article does not apply to the legal consequences that may result from that Electronic Message or from the acknowledgement of its receipt.

Time and Place of Dispatch and Receipt of Electronic Messages
Article (17)

1. Unless otherwise agreed by the Originator and the Addressee:

    a. the dispatch of an Electronic Message occurs when it enters an Electronic Information System which is not under the control of the Originator or the control of the person who sent the Electronic Message on behalf of the Originator.

    b. The time of receipt of an Electronic Message will be determined as follows:

        1) If the addressee has designated an Electronic Information System for the purpose of receiving Electronic Messages, the receipt occurs:

            A. at the time when the Electronic Message enters the designated Electronic Information System; or

            B. if the Electronic Message is sent to an Electronic Information System of the Addressee other than the designated Electronic Information System, at the time when the Electronic Message is retrieved by the Addressee.

        2) If the addressee has not designated an Electronic Information System, the receipt occurs when the Electronic Message enters an Electronic Information System that belongs to the Addressee.

2. Sub-paragraph (1)(b) of this Article applies even if the place where the Electronic Information System is located is different from the place where the Electronic Message is deemed received under paragraph (3) below.

3. Unless otherwise agreed by the Originator and the Addressee, an Electronic Message will be deemed sent from the place where the Originator's place of business is located, and will be deemed received at the place where the Addressee’s place of business is located.

4. For the purposes of this Article:

    a. Where the Originator or the Addressee has more than one place of business, the place of business will be deemed the one that has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business.

    b. Where the Originator or the Addressee does not have a place of business, any reference to the place of business of that person will be deemed a reference to its usual place of residence.

    c. A "usual place of residence", in relation to a legal person, means the place where its head office is located or where it has been incorporated.

Article (18)

Articles (15), (16), and (17) of this Law will not apply to the cases that may be specified pursuant to the relevant decision, bylaw, or regulation issued by the Chairman for this purpose.

Chapter Four
Secure Electronic Records and Signatures

Secure Electronic Records
Article (19)

1. If a prescribed Secure Authentication Procedure or a commercially reasonable Secure
   Authentication Procedure agreed upon by the parties involved has been properly applied to an Electronic Record to verify that the record has not been altered since a specified point in time, the record will be treated as a Secure Electronic Record as from the specified point in time to the time of verification.

2. For the purposes of this Article and Article (20) of this Law, to determine whether or not Secure Authentication Procedures are commercially reasonable, consideration will be given to these procedures and to the relevant commercial circumstances at the time the procedures were used. This includes:

    a. the nature of the transaction;

    b. the knowledge and skill of the parties;

    c. the volume of similar transactions conducted by either or both of the parties;

    d. the availability of alternative procedures;

e. the cost of alternative procedures; and

f. the procedures generally used for similar types of transactions.

Secure Electronic Signature
Article (20)

1. A signature will be treated as a Secure Electronic Signature if, through the application of a Secure Authentication Procedure prescribed in this Law or a commercially reasonable Secure Authentication Procedure agreed upon by the parties involved, it can be verified that the Electronic Signature was, at the time it was made:

   a. unique to the person using it;

   b. capable of identifying that person;

   c. under the sole control of the Signatory, in terms of its creation or method of use, at the time of signing; and

   d. linked to the Electronic Message to which it relates in a manner that provides reliable assurance as to the validity of the signature, so that if the Electronic Record is changed the Electronic Signature will become insecure.

2. Notwithstanding the provisions of Article (21) of this Law, the reliance on a Secure Electronic Signature will be deemed reasonably acceptable in the absence of evidence to the contrary.

Reliance on Electronic Signatures and
Electronic Attestation Certificates
Article (21)

1. A person may rely on an Electronic Signature or an Electronic Attestation Certificate to the extent that such reliance is reasonably acceptable.

2. Where an Electronic Signature is supported by an Electronic Attestation Certificate, the Relying Party in respect of that signature will bear the legal consequences for its failure to take necessary the reasonable steps to verify that the certificate is valid and enforceable, to ascertain whether or not it is suspended or revoked, and to verify compliance with any restrictions related to the certificate.

3. In determining whether it is reasonable for a person to rely on an Electronic Signature or ac Electronic Attestation Certificate, regard will be had, where applicable, to the following:

a. the nature of the underlying transaction that the Electronic Signature is intended to support;

b. the value or importance of the underlying transaction, if this is known to the party relying on the Electronic Signature;

c. whether the Relying Party in respect of the Electronic Signature or the Electronic Attestation Certificate have taken appropriate steps to determine the reliability of the Electronic Signature or the Electronic Attestation Certificate;

d. whether the Relying Party in respect of the Electronic Signature have taken appropriate steps to ascertain whether the Electronic Signature is supported or is reasonably expected to have been supported by an Electronic Attestation Certificate;

e. whether the Relying Party in respect of the Electronic Signature or the Electronic Attestation Certificate is aware or is presumed to be aware that the Electronic Signature or the Electronic Attestation Certificate has been compromised or revoked;

f. any agreement or context of dealings between the Originator and the Relying Party in respect of the Electronic Signature or the Electronic Attestation Certificate; or any prevailing commercial custom; and

g. any other relevant factor.

4. Where the reliance on the Electronic Signature or the Electronic Attestation Certificate is not reasonably acceptable given the relevant circumstances and in view of the factors stipulated in paragraph (2) of this Article, the party relying on an Electronic Signature or the Electronic Attestation Certificate will assume the risks resulting from invalidity of the Electronic Signature or the Electronic Attestation Certificate.

Obligations of Signatories
Article (22)

1. A Signatory must:

   a. exercise reasonable care to avoid any unauthorized use of his Electronic Signature Creation Device;

   b. without undue delay, notify the concerned persons if:

      1) the Signatory becomes aware that the security of his Signature Creation Device has been compromised; or

2) the circumstances known to the Signatory indicate a strong possibility that the security of the Signature Creation Device has been compromised; and

c. where an Electronic Attestation Certificate is required for the use of the Electronic Signature Creation Device, exercise reasonable care to ensure the accuracy and completeness of all data and material representations made by the Signatory in relation to the Electronic Attestation Certificate and throughout its validity period.

2. A Signatory will be liable for his failure to satisfy the requirements stipulated in paragraph (1) of this Article.

Chapter Five
Provisions Relating to Electronic Attestation Certificates and Attestation Services

Attestation Service Controller
Article (23)

1. For the purposes of this Law, the Chairman will appoint, pursuant to a resolution issued by him in this regard, an attestation service controller, particularly in relation to licensing, approving, monitoring, and overseeing the activities of Attestation Service Providers. That resolution will be published in the Official Gazette.

2. The attestation service controller may, as he deems appropriate, delegate any of his responsibilities under this Chapter to any person.

3. The attestation service controller, or his authorised representative, will be deemed a public servant.

4. In exercising any of the powers delegated to him by the attestation service controller, a delegatee must, upon the request of any person with whom he deals, present a proof of the powers vested in him by the attestation service controller.

Duties of the Attestation Service Provider
Article (24)

1. An Attestation Service Provider must:

   a. act in accordance with the representations made by him with respect to his practices;

   b. exercise reasonable care to ensure the accuracy and completeness of all material representations that are made by him and are relevant to, or included in, the Electronic Attestation Certificate throughout the period of its validity;

c. provide a reasonably accessible means which enables any Relying Party to verify:

   1. the identity of the Attestation Service Provider;

   2. that the person identified in the Electronic Attestation Certificate holds, at the time in question, the Electronic Signature Creation Device referred to in the certificate;

   3. the method used to identify the Signatory;

   4. the existence of any restrictions regarding the purpose or value for which the Electronic Signature Creation Device may be used;

   5. that the Electronic Signature Creation Device is valid and has not been compromised;

   6. whether the Signatory has the means to serve a notice pursuant to sub-paragraphs (1)(a) and (1)(b) of Article (22) of this Law; and

   7. whether a timely signature revocation service is offered.

d. provide a means for Signatories to serve a notice that the Signature Creation Device has been compromised, and ensure the availability of a timely signature revocation service;

e. use, in performing its services, trustworthy systems, procedures, and human resources; and

f. be licensed by the attestation service controller if operating in the Emirate.

2. To determine whether any systems, procedures, and human resources are trustworthy, for the purposes of sub-paragraph (1)(e), regard must be had to the following factors:

   a. availability of financial and human resources, including the existence of assets within the relevant jurisdiction;

   b. reliability of Computer hardware and software systems;

   c. procedures for applying for, processing, and issuing Electronic Attestation Certificates; and retention of records;

   d. availability of information to the Signatories specified in Electronic Attestation Certificates and to the parties relying on attestation services;

   e. frequency and extent of audit by an independent entity;

f. the existence of a declaration by the Government, an accrediting body, or the Attestation Service Provider regarding compliance with or existence of the foregoing;

g. the Attestation Service Provider's submission to the jurisdiction of the courts of the Emirate; and

h. the extent of conflict between the law applicable to the activities of the Attestation Service Provider and the laws of the Emirate.

3. An Electronic Attestation Certificate must state:

a. the identity of the Attestation Service Provider;

b. that the person identified in the certificate has control, at the time in question, over the Electronic Signature Creation Device referred to in the certificate;

c. that the Electronic Signature Creation Device has been effective on or before the date when the certificate is issued;

d. the existence of any restrictions on regarding the purpose or value for which the Electronic Signature Creation Device may be used; and

e. the existence of any restrictions regarding the scope or extent of the liability accepted by the Attestation Service Provider as towards any person.

4. If any harm is caused as a result of the invalidity of an Electronic Attestation Certificate or any defects in the same, the Attestation Service Provider will be liable for the harm suffered by:

a. any party who has contracted with the Attestation Service Provider for the provision of an Electronic Attestation Certificate; or

b. any person who reasonably relies on an Electronic Attestation Certificate issued by the Attestation Service Provider.

5. An Attestation Service Provider will not be liable for any harm if:

a. it includes in the Electronic Attestation Certificate a statement limiting the scope or extent of its liability towards any relevant person; or

b. it proves that it has not committed any fault or negligence, or that the harm has resulted due to reasons beyond its control.

Regulation of the Work of Attestation Service Providers
Article (25)

The attestation service controller will draft the rules regulating the work of and licensing the Attestation Service Providers operating in the Emirate, and will submit the same to the Chairman for approval. These rules will govern the following:

1. the applications for licences or renewal of licences of Attestation Service Providers and their authorised representatives, and all matters related thereto;

2. the activities of Attestation Service Providers, including the manner, place, and method of soliciting business from the public;

3. the standards and rules which Attestation Service Providers have to adopt and follow in their business;

4. the appropriate standards with respect to the qualifications and experience of Attestation Service Providers, and the training of their employees;

5. the conditions subject to which Attestation Service Providers will conduct their business;

6. the contents of written, printed, or visual materials and advertisements that may be distributed or used in respect of any Electronic Attestation Certificate or digital key;

7. the form and content of an Electronic Attestation Certificate or digital key;

8. the details that must be entered into the account statements maintained by Attestation Service Providers;

9. the qualifications which the auditors of Attestation Service Providers must hold;

10. the regulations governing the inspection and audit of the activities of Attestation Service Providers;

11. the conditions for the establishment of any Electronic Information System by an Attestation Service Provider, either solely or jointly with other Attestation Service Providers, and the enforcement and amendment of these conditions as deemed appropriate by the Attestation services controller;

12. the manner in which licensees conduct deal with their clients, including in the event of conflict of interests; and their duties towards these clients with respect to digital Electronic Attestation Certificates;

13. the fees that must be paid in respect of any matter required under the provisions of Chapter Five of this Law and the bylaws issued in pursuance hereof; and

14. any forms for the purposes of this Article.

Recognition of Foreign Electronic Attestation Certificates and Electronic Signatures
Article (26)

1. In determining whether an Electronic Attestation Certificate or an Electronic Signature is legally effective, no regard may be had to the place where the certificate or signature was issued, nor to the jurisdiction in which the place of business of the issuer of the Certificate or Electronic Signature is located.

2. Electronic Attestation Certificates issued by foreign Attestation Service Providers will be deemed as certificates issued by Attestation Service Providers operating under this Law, provided that the practices of the foreign Attestation Service Providers ensure a level of reliability which is at least equivalent to the level required from Attestation Service Providers operating in accordance with this Law, as provided under Article (24), and taking into consideration recognised international standards.

3. Signatures complying with the requirements of laws of another country may be recognised as legally equivalent to signatures under this Law if the laws of the other country require a level of reliability at least equivalent to that required for such signatures under this Law.

4. In relation to the recognition stipulated in paragraphs (2) and (3) of this Article, regard must be had to the factors stated in paragraph (2) of Article (24) of this Law.

5. In determining whether an Electronic Signature or Electronic Attestation Certificate is legally effective, regard must be had to any agreement between the parties in relation to the transaction for which that signature or certificate is used.

6. Notwithstanding the provisions of paragraphs (2) and (3) of this Article:

    a. Parties to commercial and other transactions may stipulate that a particular Attestation Service Provider, category of Attestation Service Providers, or category of Electronic Attestation Certificates must be used in connection with the Electronic Messages or Electronic Signatures submitted to them.

    b. Where the parties mutually agree to the use of certain types of Electronic Signatures or Electronic Attestation Certificates, that agreement will be deemed sufficient for the purposes of cross-border recognition between various

jurisdictions of countries unless that agreement is illegal under the applicable laws of the Emirate.

Chapter Six
Government Use of Electronic Records and Electronic Signatures

Acceptance of Electronic Filing and Issuance of Documents
Article (27)

1. Notwithstanding any other provision to the contrary in any other law, a Government department or entity may, in the course of performing the duties legally assigned to it:

   a. accept the filing, submission, creation, or retention of documents in the form of Electronic Records;

   b. issue any permits, licences, decisions, or approvals in the form of Electronic Records;

   c. accept fees and other payments in Electronic form; and

   d. invite bids and receive tender bids relating to Government procurement by Electronic means.

2. Where a Government department or entity decides to perform any of the acts set forth in paragraph (1) of this Article, that entity or department may specify:

   a. the manner or format in which the Electronic Records will be created, filed, retained, submitted, or issued;

   b. the manner, method, process, and procedures for inviting bids, receiving tender bids, and conducting Government procurement;

   c. the type of Electronic Signature required, including the requirement that the sender use a digital signature or any other Secure Electronic Signature;

   d. the manner and format in which signature will be affixed to the Electronic Record, and the criteria that must be met by any Attestation Service Provider to whom the document is submitted for filing or retention;

   e. control processes and procedures as appropriate to ensure the validity, security, and confidentiality of Electronic Records, payments, or fees; and

f. any attributes, conditions, or rules currently prescribed for dispatching paper documents, where the dispatch is required in relation to payment and fee Electronic Records.

Chapter Seven
Penalties

Publication of Electronic Attestation Certificates
Article (28)

No person may publish an Electronic Attestation Certificate that refers to an Attestation Service Provider named in the certificate, if that person is aware that:

a. the Attestation Service Provider named in the certificate has not issued it;

b. the Signatory named in the certificate has not accepted it; or

c. the certificate has been revoked or suspended. This does not apply to cases where the purpose of publication is verifying an Electronic Signature or digital signature used prior to the suspension or revocation.

Fraudulent Publication of Electronic Attestation Certificates
Article (29)

Any person who knowingly creates, publishes, or provides a false Electronic Attestation Certificate or incorrect information for any fraudulent or other illegal purpose will be punished by imprisonment, by a fine not exceeding two hundred and fifty thousand dirhams (AED 250,000), or by both penalties.

False or Unauthorised Applications
Article (30)

Without prejudice to any stricter penalty stipulated in any other law, a person who deliberately provides incorrect information about his identity or authorisation to an Attestation Service Provider as part of applying for issuing, revoking, or suspending an Electronic Attestation Certificate will be punished by imprisonment for up to six (6) months, by a fine not exceeding one hundred thousand dirhams (AED 100,000.00), or by both penalties.

Non-Disclosure Obligation
Article (31)

1. Any person who, pursuant to any powers conferred on him under this Law, gains access to information in Electronic Records or documents, or Electronic Communications, and deliberately discloses any such information will be punished by imprisonment, by a fine not exceeding one hundred thousand dirhams (AED 100,000.00), or by both penalties. Where the disclosure of information is caused by the person's negligence, he will be punished by a fine not exceeding one hundred thousand dirhams (AED 100,000.00).

2. The provisions of paragraph (1) of this Article will not apply to any disclosure that is made for the purposes of this Law, of any criminal proceedings relating to a crime committed in violation of any law, or of any orders issued by a judicial authority.

General Penalties
Article (32)

Without prejudice to any stricter penalty stipulated in any other law, a person who commits an act that constitutes a crime under applicable legislation by using Electronic means will be punished by imprisonment for up to six (6) months, by a fine not exceeding one hundred thousand dirhams (AED 100,000.00), or by both penalties. Where the penalty prescribed by the applicable legislation is stricter than the penalty prescribed in this Article, the stricter penalty will apply.

Legal Person Offences
Article (33)

Where a legal person violates the provisions of this Law or the bylaws issued in pursuance hereof, and it is proven that the violation is caused as a result of the act, negligence, consent, or connivance by a member of the board of directors, manager, or other employee of the legal person; or any person who appears to be acting in this capacity, both the violating person and the legal person will be convicted of the violation and punished accordingly.

Confiscation of Tools Used in Committing Offences
Article (34)

Where a court convicts a party pursuant to this Law, it will order the confiscation of the tools used in committing the crime.

Lapse of Penal Claim by Conciliation
Article (35)

Criminal proceedings in respect of the crimes committed for the first time will lapse if settlement is reached after committing the crime but prior to determination of the case by a definitive court judgment. Where the settlement is reached after a definitive court judgment is rendered, the execution of the judgment will be stayed.

Chapter Eight
Miscellaneous Provisions

Exemption Authority
Article (36)

The Chairman may, in accordance with the conditions and rules he deems appropriate, exempt any person or entity from compliance with all or any of the provisions of this Law or the provisions of any bylaws issued in pursuance hereof.

Courts and Special Arbitration Tribunals
Article (37)

The Chairman may form courts or special arbitration tribunals to determine the cases and disputes arising from the implementation of this Law.

Bylaws
Article (38)

The Chairman will issue the bylaws required for the implementation of this Law.

Commencement
Article (39)

This Law will be published in the Official Gazette, and will come into force on the day on which it is published.

Maktoum bin Rashid Al Maktoum

Ruler of Dubai

Issued in Dubai on 12 February 2002

Corresponding to 30 Thu al-Qidah 1422 A.H.