

Electronic Transactions and Commerce Law No. 2 of 2002

We, Maktoum Bin Rashid Al Maktoum, Ruler of Dubai

In accordance with the Government of Dubai's pursuance for the placement of means of modern technology in transactions and commercial exchange,

Do hereby promulgate the following Law:

CHAPTER (I)

Definitions

Article 1

This Law shall be cited as the "**Law of Electronic Transactions and Commerce No.2/2002.**"

Article 2

The following words and terms shall have the respective meaning assigned to each of them, unless the context of the provision requires otherwise:

The Government

The Government of Dubai, including its departments, corporations and public institutions.

The Emirate

The Emirate of Dubai

The Chairman

The Chairman of Dubai Technology, Electronic Commerce and Media Free Zone Authority.

Electronic

Whatever relates to modern technology having electrical, digital, magnetic, wireless, optical, electromagnetic, automated, photonic capabilities or similar to the aforesaid.

Electronic Information

Data that has Electronic features in the form of texts, codes, sounds, graphics, images, Computer Programs or other databases.

Electronic Information System

An Electronic system for creating, generating, sending receiving, storing, displaying or otherwise processing information or Electronic Communications Electronically.

Electronic “Record” or “Document”

A record or document created, stored, generated, copied, sent, communicated, received by Electronic means, on a tangible medium or on any other Electronic medium, and is retrievable in perceivable form.

Computer

An Electronic device that deals with information and data by analysing, programming, presenting, storing, sending, or otherwise receiving them through Electronic Information programs and systems; which might function separately

or in conjunction with other Electronic devices or systems.

Originator

A natural or legal person who sends, or on whose behalf, an Electronic Communication is sent, whichever is the case, though it shall not be considered as originator a party whose task is to supply services in relation to producing, processing, sending, or storing such Electronic Communication and other related services.

Addressee

A natural or legal person to whom the Originator has intended his Electronic Communication to be addressed; it shall not be considered as Addressee the person who carries out the supplying of services in relation to receiving, processing, or storing such Electronic Communication and other related services.

Computer Program

A collection of data or instructions used directly or indirectly in an Electronic Information processing system for the purpose of finding or reaching specific results

Electronic Communications

Electronic Information sent or received by Electronic means, whatever is the method of retrieval in the place where it is received.

Communicating Electronically

The sending and receiving Electronic Communications.

Electronic Signature

A signature consisting of letters, numbers, symbols, voice or processing system in an Electronic form and logically attached or connected to an Electronic Communication and stamped with the intention of authenticating or approving such Communication.

Protected Electronic Signature

An Electronic Signature fulfilling the conditions of Article (20) of this Law.

Signatory

A natural or legal person, holding his own Electronic Signature Device, and who signs or a signature is made on his behalf on an Electronic Communication by using such device.

Signature Device

A device or Electronic Information prepared to operate independently or in conjunction with other devices and Electronic Information Systems to create a unique Electronic Signature attributable to a specific person; such an operation shall include any systems or

devices which generate or capture unique information such as codes, algorithms, letters, numbers, private keys, personal identification numbers, (PINs), or personal attributes.

Automated Electronic Agent

An Electronic program or system to a Computer capable of acting or responding to an act, independently, wholly or partly, without any supervision by any natural person at the time when the act or the response has taken place.

Automated Electronic Transactions

Transactions that are concluded or performed, wholly or partly, through Electronic means or records, where these activities or records are not subject to any follow-up or revision by a natural person, as is the case in the context of the conventional establishment and performance of contracts and transactions.

Supplier of Certification Services

Any confirmed or authorized person or entity that carries out the Issuing of Electronic Authentication Certificates or any other services or tasks relating to them and to Electronic Signatures, as regulated under Chapter V of this Law.

“Electronic Authentication Certificate”

A Certificate issued by a supplier of certification services providing in it an assurance as

to the identity of the person or the party in control of a specific Signature Device, and which may be referred to in this Law as the “Certificate”

“Secure Authentication Procedures”

Procedures which aim at verifying that an Electronic Communication was issued by a specific person, and detecting any error or alteration in the contents of an Electronic Communication or Record or in its transmission or saving, within specific period of time; This will include any procedure using algorithms, codes, identifying words or numbers, encryption, answerback or acknowledgement procedures, or similar information security devices.

“Relying Party”

A person who acts in reliance on an Electronic Certificate or Signature.

“Electronic Transactions”

Any dealing, contract or agreement concluded or performed, wholly or partly, through Electronic Communications.

“Electronic Commerce”

Commercial transactions which are concluded through Electronic Communications

**Construction
Article 3**

This Law shall be construed consistently with what is commercially reasonable in Electronic Transactions and Commerce, and which will lead to the attainment of the following objectives:

1. facilitate Electronic Communications by means of reliable Electronic Records:
2. Facilitate and eliminate any barriers to Electronic Commerce and other Electronic Transactions which may result from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure Electronic Commerce;
3. facilitate the transmission of Electronic Documents to Government agencies and corporations, and to promote efficient delivery of services by such agencies and corporations by means of reliable Electronic Communications;
4. minimise incidences of forgery related to Electronic Communications including their subsequent amendment and chances of fraud in Electronic Commerce and other Electronic Transactions;
5. establish uniform rules, regulations and standards with regard to authentication and integrity of Electronic Communications;
6. promote public confidence in the integrity and validity of Electronic transactions, Communications and records;
7. enhance the development of Electronic Commerce and other transactions on the national and international level through the use of Electronic Signatures.

Article 4

In applying this Law, regard shall be had to the rules of international commercial custom that relate to Electronic Transactions and Commerce and to the level of development in technological communications.

Application Article 5

(1) This Law shall be applicable to Electronic Records and Signatures that relate to Electronic Transactions and Commerce; though the following shall be exempt from the application of this Law:

- (a) Transactions and issues relating to personal law such as marriage, divorce and wills.
 - (b) Documents of title to immovable property.
 - (c) Negotiable instruments.
 - (d) Transactions concerning the sale and purchase of immovable property and the disposition thereof, and their lease for a period longer than ten years and the registration of any rights relating to them.
 - (e) Any document required by law to be notarised before the notary public.
- (2) The Chairman may, by order, add to those mentioned under paragraph (1) above, any transaction or mater, or to delete from them or modify them.

Consenting to Electronic Dealing
Article 6

- (1) Nothing in the Law requires a person to use or accept information in Electronic form, but a person's consent to do so may be inferred from the person's affirmative conduct.
- (2) As between parties involved in generating, sending, receiving, storing or otherwise processing Electronic Records, any of the rules provided in Chapters II to IV of this Law may be varied by agreement.
- (3) As an exception to paragraph (1) above, the consent of the Government to deal Electronically in transactions to which it is a party must be expressed.

CHAPTER (II)

REQUIREMENTS FOR ELECTRONIC TRANSACTIONS

Electronic Communications
Article 7

- (1) An Electronic Communication shall not be denied legal effect or

enforceability solely on the ground that it is Electronic in form.

- (2) An Electronic Communication that refers to information, without providing details of that information, shall not be denied legal effect or enforceability, so far as the viewing of this information is attainable and the way of viewing it was indicated within the Electronic System of the Originator.

Retention of Electronic Records **Article 8**

- (1) Where a rule of law requires that any document, record or information be retained, for whatever reason, that requirement is satisfied by retaining such document, record or information in the form of an Electronic Record, if the following conditions are observed:
 - (a) The Electronic Record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received.
 - (b) The information remains stored in a way that is accessible and usable for subsequent reference.
 - (c) The retention of information, if any, so as to enable the identification of the origin and destination of an Electronic Communication and the date and time when it was sent or received.
- (2) An obligation to retain documents, records or information in accordance with paragraph (1)- (c) shall not be extended to any information necessarily and automatically generated to enable the record to be sent or received.
- (3) A person may satisfy the requirements referred to in paragraph (1) of this Article by using the services of any other person, if the conditions in that paragraph are complied with.

(4) Nothing in this Article shall affect the following:

- (a) Any other law that expressly provides for the retention of documents, records or information in the form of Electronic Records, in accordance with a specific Electronic System or through specified procedures, or their retention or Communication through a specified Electronic Agent.
- (b) The discretion of the Government to specify additional requirements for the retention of Electronic Records that are subject to its jurisdiction.

Writing Article 9

Where a rule of law requires a statement, document, record, transaction or evidence to be in writing or provides for certain consequences if it is not, an Electronic Document or record satisfies that rule provided that the provisions of paragraph (1) of the previous Article are observed.

Electronic Signatures Article 10

- (1) Where a rule of law requires a signature on a document, or provides for certain consequences in the event of the absence of a signature, an Electronic Signature that is reliable within the meaning of Article (21) of this Law, satisfies that requirement.
- (2) Unless otherwise is provided by law, it is permitted for any person to use any form of Electronic Authentication.

Electronic Original Article 11

An Electronic Document or Record is considered as original where a method is used which:

- (a) Provides technically reliable assurance as to the integrity of the information in the Document or Record, from the time when it was first

generated in its final form as an Electronic Document or Record; and

- (b) Allows, when required, the display of the information sought to be presented.

Admissibility and Weight of Electronic Evidence
Article 12

- (1) (1) Nothing shall prevent the acceptance of an Electronic Communication or Electronic Signature as proof:
 - (a) (a) solely on the ground that the Communication or the Signature was Electronic in its form.
 - (b) (b) Solely on the ground that the Communication or the Signature was not original or in its original form, if such Electronic Communication or Signature is the best evidence that the person adducing it could reasonably be expected to obtain.
- (2) (2) electronic information shall be given due evidential weight; And in assessing the evidential weight, regard shall be had to the following:
 - (a) (a) The extent of the reliability of the manner in which one or more of the operations of executing, entering, generating, processing, storing, presenting or communicating was carried out.
 - (b) (b) The reliability of the manner in which the integrity of the information was maintained.
 - (c) (c) The extent of reliability of the source of information, if identifiable.
 - (d) (d) The extent of reliability of the manner in which the identity of the Originator, if relevant, was ascertained.
 - (e) (e) Any other relevant factor.
- (3) (3) In the absence of proof to the contrary, it is presumed that a Protected Electronic Signature:
 - (a) (a) could be relied on
 - (b) (b) was the signature of the person to whom it co-relates
 - (c) (c) was affixed by that person with the intention of signing or

approving the Electronic Communication to which it is affixed or logically associated.

- (4) (4) In the absence of proof to the contrary, a Protected Electronic Record is presumed to be:
 - (a) (a) unaltered since its creation
 - (b) (b) reliable

CHAPTER (III)

ELECTRONIC TRANSACTIONS

Formation and Validity of Contracts

Article 13

- (1) For the purpose of contracting, it is permissible to express offer and acceptance, partly or wholly, by means of Electronic Communication.
- (2) A contract shall not be denied validity or enforceability on the sole ground that it was concluded by means of one or more Electronic Communications.

Automated Electronic Transactions

Article 14

- (1) It is permissible for a contract to take place between automated Electronic mediums that include two Electronic Information Systems or more, set and programmed earlier for carrying out such tasks. A contract shall be valid, effective and legally enforceable despite the fact that there has been no personal or direct involvement by any natural person, in such systems, in the conclusion of the contract.
- (2) It is also permissible for a contract to be concluded between an Automated Electronic Information System belonging to a natural or legal person and a legal person, where the latter knows or ought to have known that such a system will carry out the task of concluding or Performing the contract.

Attribution
Article 15

- (1) (1) An Electronic Communication shall be considered as being issued by the Originator if the Originator itself issued it.
- (2) (2) As between the Originator and the Addressee, an Electronic Communication is deemed to be that of the Originator if it was sent:
 - (a) (a) by a person who had the authority to act behalf of the Originator with respect to the Electronic Communication; or
 - (b) (b) by an automated Information System programmed by or on behalf of the Originator to operate automatically.
- (3) (3) As between the Originator and the Addressee, an Addressee is entitled to regard an Electric Communication as being that of the Originator and to act on that assumption if:
 - (a) (a) in order to ascertain whether the Electronic Communication was that of the Originator, the Addressee properly applied a procedure previously agreed to by the Originator for that purpose; or
 - (b) (b) the Electronic Communication, as received by the Addressee, resulted from the actions of a person whose relationship with the Originator or with any agent of the Originator enabled that person to gain access to a method used by the Originator to identify the Electronic Communication as its own.
- (4) (4) Paragraph (3) above shall not apply:
 - (a) (a) from the time when the Addressee has both received notice from the Originator that the Electronic Communication is not that of the Originator and had reasonable time to act accordingly;
 - (b) (b) where the Addressee knew or ought to have known, had it exercised reasonable care or used any agreed procedure, that the

Electronic Communication was not that of the Originator; or

- (c) (c) if it is unreasonable for the Addressee to regard the Electronic Communication as that of the Originator or to act on that assumption.

(5) Where an Electronic Communication is that of the Originator or is deemed to be that of the Originator, or the Addressee is entitled to act on that assumption in accordance with paragraphs (1), (2) and (3) of this Article, then, as between the Originator and the Addressee, the Addressee is entitled to conclude that the Electronic Communication received is what the Originator intended to send, and to act on that basis.

(6) The Addressee is entitled to regard each Electronic Communication received as a separate Communication and to act on that assumption alone. Paragraph (7) of this Article does not apply where the Addressee knew or should have known, had the Addressee exercised reasonable care or used any agreed procedure, that the Electronic Communication was a duplicate.

(7) The Addressee is not entitled to make the assumptions and conclusions in paragraphs (5) and (6) above when the Addressee knew or should have known, had the Addressee exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the Electronic Communication as received.

Acknowledgement of Receipt Article 16

(1) Paragraphs (2), (3) and (4) of this Article shall apply where, on or before sending an Electronic Communication, or by means of that Electronic Communication, the Originator has requested or has agreed with the Addressee that receipt of the Electronic Communication be acknowledged.

(2) Where the Originator has not agreed with the Addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by:

- (a) any Communication by the Addressee, whether by Electronic means,

automated means or by any other means; or

(b) any conduct of the Addressee; sufficient to indicate to the Originator that the Electronic Communication has been received.

(3) Where the Originator has stated that the Electronic Communication is conditional on receipt of the acknowledgement, then such Communication is treated, in relation to setting legal rights and obligations between the Originator and the Addressee, as though it had never been sent, until the Originator receives the acknowledgement.

(4) Where the Originator has asked for an acknowledgement but has not stated that the Electronic Communication is conditional upon receipt of the acknowledgement within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the Originator:

(a) may give notice to the Addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in paragraph (4)- (a) above, may, upon notice to the Addressee, treat the Electronic Communication as though it has never been sent, or resort to exercising any other rights it may have.

(5) Where the Originator receives the Addressee's acknowledgement of receipt, it is presumed, unless evidence to the contrary is adduced, that the Addressee received the related Electronic Communication, but that presumption does not imply that the content of the Electronic Communication sent by Originator, corresponds to the] content of the Communication delivered to him from the Addressee.

(6) Where the acknowledgement received by the Originator states that the related Electronic Communication met technical requirements, either agreed upon or set forth in applicable standards, it is presumed, unless evidence to the contrary is adduced, that those requirements have been met.

(7) Except in so far as it relates to the sending or receipt of Electronic

Communications, this article is not intended to deal with the legal consequences that may result either from that Electronic Communication or from the acknowledgement of its receipt.

**Time and Place of Despatch and Receipt of
Electronic Communications
Article 17**

- (1) Unless otherwise agreed to between the Originator and the Addressee:
 - (a) The dispatch of an Electronic Communication occurs when the Communication enters an Information System outside the control of the Originator or the person who sent the Communication on behalf of the Originator.
 - (b) The time of the receipt of an Electronic Communication is determined as follows:
 - (1) If the Addressee has designated an information system for the purpose of receiving an Electronic Communication, receipt occurs:
 - (i) at the time when the Electronic Communication enters the designated information system; or
 - (ii) if the Electronic Communication is sent to an Information System of the Addressee that is not the designated Information System for receiving such Communications, at the time when the Communication is retrieved by the Addressee.
 - (2) If the Addressee has not designated an Information System, receipt occurs when the Electronic Communication enters an Information System of the Addressee.
- (2) Paragraph (1)- (b) of this Article shall apply notwithstanding that the place

where the Information System is located may be different from the place where the Electronic Communication is deemed to be received, under paragraph (3) below.

(3) Unless otherwise agreed between the Originator and the Addressee, an Electronic Communication is deemed to be despatched at the place where the Originator has its place of business, and is deemed to be received at the place where the Addressee has its place of business.

(4) For the purposes of this Article:

- (a) If the Originator or the Addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business.
- (b) If the Originator or the Addressee does not have a place of business, reference is to be made to the usual place of residence.
- (c) “Usual place of residence” in relation to a body corporate, means its principal place or otherwise the place where it was incorporated.

Article 18

Articles (15), (16) and (17) of this Law shall not apply to cases that the Chairman may specify by order, by-law or regulation issued by him.

CHAPTER (IV)

PROTECTED ELECTRONIC RECORDS AND SIGNATURES

Protected Electronic Records

Article 19

(1) If a prescribed or commercially reasonable Secure Authentication

Procedures, agreed to by the parties, has been properly applied to an Electronic Record to verify that it has not been altered since a specified point in time, it shall be treated as a Protected Electronic Record from such specified point in time to the time of verification.

(2) For the purposes of this Article and Article (20) of this Law, whether Secure Authentication Procedures are commercially reasonable shall be determined having regard to these procedures and the commercial circumstances at the time these procedures were used, including:

- (a) the nature of the transaction.
- (b) the knowledge and sophistication of the parties.
- (c) the volume of similar transactions engaged in by either or all parties.
- (d) the availability of alternative procedures.
- (e) the cost of alternative procedures.
- (f) the procedures in general use for similar types of transactions.

Protected Electronic Signature Article 20

(1) A Signature shall be treated as a Protected Electronic Signature, if, through the application of a prescribed or commercially reasonable Secure Authentication Procedures agreed to by the parties, it can be verified that an Electronic Signature was, at the time it was made:

- (a) unique to the person using it;
- (b) capable of verifying the identity of that person;

- (c) under that person's full control, whether in relation to its creation or the means of using it at the time of signing; and
 - (d) linked to the Electronic Communication to which it relates, in a manner which provides reliable assurance as to the integrity of the Signature, so that if the Electronic Record is changed, then the Electronic Signature shall become unprotected.
- (2) In the absence of proof to the contrary, and notwithstanding Article (21) of this Law, reliance on a Protected Electronic Signature is presumed to be reasonable.

Reliance on Electronic Signatures and Certificates of Authentication
Article 21

- (1) A person is entitled to rely on an Electronic Signature or an Electronic Certificate to the extent that it is reasonable to do so.
- (2) Where an Electronic Signature is supported by a Certificate, the Relying Party in respect of such signature shall bear the legal consequences of its failure to take reasonable and necessary steps to verify the validity and enforceability of the Certificate, as to whether it is suspended or revoked, and of observing any limitations with respect to the Certificate.
- (3) In determining whether it was reasonable for a person to rely on an Electronic Signature or a Certificate, regard shall be had, if appropriate, to:
 - (a) the nature of the underlying transaction which was intended to be supported by the Electronic Signature;
 - (b) the value or importance of the underlying transaction, if this is known;
 - (c) whether the Relying Party in respect of the Electronic Signature or certificate has taken appropriate steps to

determine the reliability of the Electronic Signature or the Certificate;

- (d) whether the Relying Party in respect of the Electronic Signature or certificate took reasonable steps to verify if the Electronic Signature was supported by a Certificate, or if it should be expected to be so supported;
- (e) whether the Relying Party in respect of the Electronic Signature or Certificate knew or ought to have known that the Electronic Signature or the Certificate had been compromised or revoked;
- (f) any agreement or course of dealing between the Originator and the Relying Party, or any trade usage which may be applicable;
- (g) any other relevant factor.

(4) If reliance on the Electronic Signature or the Certificate is not reasonable in the circumstances, having regard to the factors in paragraph (2) of this Article, the party relying on the Electronic Signature or Certificate assumes the risks of the Electronic Signature or the Certificate not being valid.

Duties of Signatory **Article 22**

(1) A Signatory shall:

- (a) exercise reasonable care to avoid unauthorised use of his Signature Device;
- (b) notify concerned persons without undue delay in the event that:

- 1. the Signatory knows that his Signature Device has been compromised in its level of security.

- ii. the circumstances known to the Signatory substantially indicate that the Signature Device was compromised in its level of security.
 - (c) exercise reasonable care to ensure the accuracy and completeness of all material representations and declarations made by it which are relevant to the life-cycle of the Certificate, in circumstances where the Signature Device requires the use of a Certificate.
- (2) A Signatory shall be liable for its failure to fulfil the requirements of paragraph (1) above.

CHAPTER (V)

PROVISIONS RELATING TO CERTIFICATES AND CERTIFICATION SERVICES

The Controller of Certification Services

Article 23

- (1) For the purposes of this Law, the Chairman, by an order issued by him, shall appoint a Controller of Certification *Services*, in particular, for the purposes of licensing, certifying, controlling and overseeing the activities of Suppliers of Certification Services; such order to be published in the Official Gazete.
- (2) A controller may, in writing, delegate anyone, any of his duties accorded under this Chapter.
- (3) A controller, or anyone delegated by him, shall be deemed to be a public servant.
- (4) In exercising any of the powers of enforcement conferred upon him, and in response to a demand by a person against whom he is acting, a delegated person shall produce proof of his delegation by the controller.

Duties of Supplier of Certification Services

Article 24

- (1) A Supplier of Certification Services shall:

- (a) act in accordance with the representations it makes with respect to its practices;
- (b) exercise reasonable care to ensure the accuracy and completeness of all material representations that are relevant to a Certificate or which are included within the life-cycle of a Certificate;
- (c) provide reasonably accessible means which enable a Relying Party to ascertain:
 - i. the identity of the Supplier of Certification Services;
 - ii. that the person who is identified in the Certificate had control, at the relevant time, over the Signature Device referred to in the Certificate;
 - iii. the method used to identify the Signatory;
 - iv. any limitations on the purposes or value for which the Signature Device may be used;
 - v. whether the Signature Device is valid and has not been compromised;
 - vi. whether means exist for the Signatory to give notice pursuant to Article 22, (1)-(a),(b) of this Law;
 - vii. whether a timely revocation means is offered.
- (d) provide a means for Signatories to give notice that a Signature Device has been compromised and ensure the availability of a timely revocation service which can be used at the appropriate time;
- (e) utilise trustworthy systems, procedures and human resources in performing its services be licensed by the controller of certification services, if it is operating from the Emirate.
- (f) be licensed by the controller of certification services, if it is operating from the Emirate.

(2) In determining whether any systems, procedures or human resources are trustworthy, for the purposes of paragraph (1)- (e) above, regard shall be had to the following factors:

(a) financial and human resources, including existence of assets within the jurisdiction.

(b) trustworthiness of hardware and software of Computer systems.

(c) procedures for processing and issuing of Certificates and applications for Certificates and retention of Records.

(d) availability of information relating to Signatories that are identified in Certificates and providing information to potential Relying Parties on certification services.

(e) regularity and extent of audit by an independent body.

(f) the existence of a declaration by the Government, an accreditation body or the Supplier of Certification Services regarding the existence of or the compliance with the foregoing.

(g) the Supplier of Certification Services' susceptibility to the jurisdiction of the courts of the Emirate.

(h) the degree of discrepancy between the law applicable to the conduct of the Supplier of Certification Services and the law of the Emirate.

(3) A Certificate shall specify the following:

(a) the identity of the Supplier of Certification Services;

(b) that the person who is identified in the Certificate controls, at the relevant time, the Signature Device referred to in the Certificate;

(c) that the Signature Device was effective at or before the date when the Certificate was issued;

- (d) whether there are any limitations on the purposes or value for which the Certificate may be used; and
 - (e) whether there are any limitations on the scope or extent of liability which the Supplier of Certification Services accepts toward any person.
- (4) If damage has been caused as a result of the Certificate being incorrect or defective, a Supplier of Certification Services shall be liable for loss suffered by:
- (a) any party who has contracted with the Supplier of Certification Services for the presentation of a Certificate; and
 - (b) any person who has reasonably relied on the Certificate issued by the Supplier of Certification Services.
- (5) A Supplier of Certification Services shall not be liable for any damage:
- (a) if it included in the Certificate a statement limiting the scope and the extent of its liability towards any relevant person; or
 - (b) if it proves that it did not commit any fault or was not negligent, or that the damage was due to an external cause in which it did not have any part.

Regulation of Suppliers of Certification Services

Article 25

A Controller shall set the rules for the regulation and licensing of Suppliers of Certification Services operating within the Emirate, and shall submit these rules to the Chairman for approval. These rules shall include the following:

- (1) applications for licences or renewal of licences of Suppliers of Certification Services and their authorised representatives and matters incidental thereto.
- (2) the activities of Suppliers of Certification Services including the manner, place and method of soliciting business from the public.

- (3) the standards and rules which Suppliers of Certification Services have to maintain and follow in their business.
- (4) prescribing the appropriate standards with respect to the qualifications and experience of Suppliers of Certification Services and training of their employees.
- (5)(5) prescribing the conditions for the conduct of business by a Supplier of Certification Services.
- (6)(6) specifying the content and distribution of written, printed or visual material and advertisements that may be distributed or used by a person with respect to any Certificate or digital key;
- (7)prescribing the form and content of any Certificate or digital key.
- (8)prescribing the particulars to be recorded in respect of accounts kept by Suppliers of Certification Services.
- (9)the qualifications of auditor of accounts of Suppliers of Certification Services.
- (10) setting the necessary rules for regulating the inspection and control of business activities of Suppliers of Certification Services.
- (11)‘the conditions for the establishment and regulation of any Electronic system by a Supplier of Certification Services, whether by itself or in conjunction with other Suppliers of Certification Services, and for the imposition and variation of such conditions or restrictions, as a controller may see fit.
- (12) the manner in which a holder of a licence conducts its dealings with its customers, including in the event of conflict of interest with them, and its duties towards them with respect to digital Certificates.
- (13) prescribing fees to be paid in respect of any matter required under Chapter (V) of this Law and regulations issued hereunder.
- (14) prescribing any forms for the purposes of this Article.

Recognition of Foreign Certificates and Electronic Signatures
Article 26

(1) In determining whether a Certificate or an Electronic Signature is legally effective, no regard shall be had to the place where the Certificate or the Electronic Signature was issued, nor to the jurisdiction in which the issuer of the Electronic Certificate or Signature had its place of business.

(2) Certificates issued by a foreign Supplier of Certification Services shall be considered as equivalent to Certificates issued by Suppliers of Certification Services operating under this Law, if the practices of the foreign Suppliers of Certificate Services provide a level of reliability at least equivalent to that required of Suppliers of Certification Services operating in accordance with this Law, as provided under Article (24), and taking into consideration recognized international practices.

(3) Signatures complying with the requirement of laws of another state may be recognised as equivalent to Signatures under this Law if the laws of the other state require a level of reliability at least equivalent to that required for such Signatures under this Law.

(4) In relation to the admissions specified in paragraphs (2) and (3) above, regard must be made to factors provided in paragraph (2) of Article (24) of this Law.

(5) In determining whether an Electronic Signature or Certificate is legally effective, regard shall be had to any agreement between the parties in relation to the transaction in which that Signature or Certificate is used.

(6) Notwithstanding paragraphs (2) and (3) above:

- (a) (a) parties to commercial and other transactions may specify that a particular Supplier of Certificate Services, category of Suppliers of Certification Services or class of Certificates must be used in connection with Electronic Communications or Signatures submitted to them.

- (b) (b) Where parties agree, as between themselves, to use of certain types of Electronic Signatures or Certificates, that agreement shall be recognized as sufficient for the purpose of cross-border recognition between the various jurisdictions of states, provided that the agreement would not be invalid under the enforceable laws in the Emirate.

CHAPTER (VI)

GOVERNMENT USE OF ELECTRONIC RECORDS AND SIGNATURES

Acceptance of Electronic Filing and Issuing of Documents

Article 27

- (1) Notwithstanding any contrary provision in any other law, it is permissible for any department or organ of the Government, in performing tasks assigned to it by law, to carryout the following:
 - (a) accepts the filing, submission, creation or retention of documents in the form of Electronic Records;
 - (b) issues any permit, licence, decision or approval in the form of Electronic Records;
 - (c) acceptance of fees or any other payments in Electronic form.
 - (d) submission of tenders and receiving of bids relating to Government purchases by Electronic means.

- (5) (5) Where a department or organ of the Government decides to perform any of the functions in paragraph (1) of this Article, such agency may specify:
 - (a) the manner or format through which such Electronic Records shall be created, filed, retained, submitted or issued
 - (b) the manner, format, method and procedures by which

Government tenders are submitted, bids are received and Government purchases are made.

- (c) the type of Electronic Signature required including a requirement that the sender use a Digital Signature or other Protected Electronic Signature.
- (d) the manner and format in which such Electronic Signature shall be affixed to the Electronic Record, and the criteria that shall be met by Supplier of Certification Services, to whom Records are submitted for saving or retaining.
- (f) the appropriate control processes and procedures to ensure safety, security and confidentiality of Electronic Records or payments or fees.
- (g) any other required specifications, conditions or rules currently specified for sending paper documents, if that was required in relation to Electronic Records pertaining to payments and fees.

CHAPTER (VII)

PENALTIES

Publication of Certificate

Article 28

No person shall publish a Certificate with reference to a Supplier of Certification Services listed in the Certificate, if that person knows that:

- (1) (1) the Supplier of Certification Services named in the Certificate has not issued it.
- (2) (2) the Signatory who's name is listed in the Certificate has not accepted it.
- (3) (3) the Certificate has been revoked or suspended, unless such publication is for the purpose of verifying

an Electronic or Digital Signature created prior to such suspension or revocation.

Publication of Certificate for Fraudulent Purpose
Article 29

Any person who knowingly creates, publishes or otherwise makes available a Certificate or provides false statements for a fraudulent or any other unlawful purpose, shall be punished by confinement and a fine which does not exceed Dhs.250,000.00, or by either of these penalties.

False or Unauthorised Request
Article 30

Without prejudice to any more severe penalty specified in any other law, any person who knowingly misrepresents to a Supplier of Certification Services his identity or authorization for the purpose of requesting a Certificate or for revoking or suspending a Certificate, shall be punished by confinement for a term not exceeding six months and a fine not exceeding Dhs 100,000.00 or by either of these penalties.

Obligation of Confidentiality
Article 31

- (1) (1) Any person who has, pursuant to any powers conferred under this Law, obtained access to any information in Electronic Files, Documents or Communications, and has intentionally disclosed any such information shall be punishable by confinement and a fine not exceeding Dhs. 100,000.00, or either of these penalties. In the event that his negligence has caused the disclosure of such information, the penalty shall be a fine which shall not exceed Dhs. 100,000.00.
- (2) (2) Excluded from the rules of paragraph (1) of this Article, shall be cases of disclosure that are made for the purpose of this Law, or for any criminal procedures relating to a crime committed in violation of any law, or for the purpose of orders issued by any judicial authority.

General Penalties
Article 32

Without prejudice to any severe penalty prescribed by any other law, any person who commits any act which constitutes a crime by virtue of current legislation, through the use of Electronic means, shall be punishable by confinement for a period not exceeding six months and a fine not exceeding Dhs. 100,000.00 or either of these penalties. Where the penalties prescribed in the other legislation exceed those provided under this Article, then the person shall be punishable with the more severe penalty.

Offence by Body Corporate
Article 33

Where a violation of this Law or the regulation issued thereunder is perpetrated by a body corporate, as a result of an act or a default, consented to or made in connivance with any member of a board of Directors, a manager or any other employee of such body corporate or any person who was purporting to act in any such capacity, such person, as well as the body corporate, shall be charged with that violation and punished accordingly.

Confiscation of Tools Used for the Perpetration of the Crime
Article 34

The court, in the event of conviction, by virtue of the rules of this Law, shall order the confiscation of tools used for the perpetration of the crime.

Termination of the Criminal Case and Conciliation
Article 35

A criminal action, in respect of crimes that are committed for the first time, shall be terminated if conciliation is concluded after the commission of the crime, prior to the issuing of a final ruling; and if it was concluded after the final ruling, then that ruling shall be suspended.

CHAPTER (VIII)

MISCELLANEOUS PROVISIONS

Power to Exempt Article 36

The Chairman may exempt, according to such terms and conditions as he thinks fit, any person or a body from all or any of the provisions of this Law or any regulations made thereunder.

Courts and Special Arbitral Committees Article 37

The Chairman may constitute special courts or arbitral committees to settle law suits and resolve disputes resulting from the application of this Law.

Regulations Article 38

The Chairman shall issue the executive regulations necessary for the enforcement of this Law.

Commencement Article 39

This Law shall be published in the Official Gazette and shall come into force on the date of such publication.

**Maktoum Bin Rashid Al Maktoum
Ruler of Dubai**

Issued in Dubai on 12th of February 2002- Corresponding to 30111 of Thi Al-Qedah 1422.