Federal Law No. (1) of 2006

Concerning

Electronic Transactions & Commerce

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

After perusal of the constitution; and

Federal Law No. 1 of 1972 concerning the Functions of Ministries and the Powers of Ministers and the amendments thereto; and

Federal Law No. 5 of 1975 concerning the Commercial Register; and

Federal Law No. 8 of 1980 Regulating the Labor Relations and the amendments thereto; and

Federal Law No. 10 of 1980 concerning the Central Bank and Monetary System and the Regulation of the Banking Profession and the amendments thereto; and

Federal Law No. 8 of 1984 concerning Commercial Companies and the amendments thereto; and

Federal Law No. 9 of 1984 concerning Insurance Companies and Agents and the amendments thereto; and

Civil Transactions Law promulgated by Federal Law No. 5 of 1985 and the amendments thereto; and

The Penal Code promulgated by Federal Law No. 3 of 1987; and

Federal Law No. 22 of 1991 concerning Notaries Public and the amendments thereto; and

The Law of Proof in Civil and Commercial Transactions promulgated by Federal Law No. 10 of 1992; and

The Civil Procedures Law promulgated by Federal Law No. 11 of 1992; and

The Penal Procedures Law promulgated by Federal Law No. 35 of 1992; and

Federal Law No. 37 of 1992 concerning Trademarks and the amendments thereto; and

The Commercial Transactions Law promulgated by Federal Law No. 18 of 1993; and

Federal Law No. 17 of 2002 Regulating and Protecting the Industrial Property of Patents, Drawings and Industrial Forms; and

The Decree promulgating Federal Law No. 3 of 2003 Regulating the Communication Sector; and

Acting on the submissions made by the Minister of Economy and Planning as approved by the Cabinet and ratified by the Federal Supreme Council,

Promulgate the following law:

Chapter I
Definitions

Article (1)

The following words and phrases shall have the meanings respectively assigned to them unless the context requires otherwise:

State : The United Arab Emirates

Government Bodies	:	Federal ministries, local departments and authorities, federal and local corporations and institutions
Ministry	:	The Ministry of Economy and Planning
Minister	:	The Minister of Economy and Planning
Local Competent Authority	:	The local competent authority of each emirate of the State
Electronic	:	Whatever is connected with modern technology that has electrical, digital, magnetic, wireless, optical, electromagnetic, automated, photo or similar capabilities.
Electronic Information	:	Data or information having electronic features in the form of texts, symbols, sounds, drawings, graphics, computer software or other databases.
Electronic Information System	:	A package of programs and systems prepared for processing and managing data and information to create, originate, produce, transmit, receive, save or display messages electronically or otherwise.
Electronic Record Instrument	:	A record or instrument originated, saved, produced, or copied, transmitted, communicated or received by an electronic means, tangible medium or any other electronic medium that can be retrieved in an understandable form.

Information Technology Means	:	Any electromagnetic, optical, electrochemical or any other tool used for processing data, performing logic, arithmetic or storage functions, including any data storage capability, and communications related to or working in conjunction with such tool.
Originator	:	The natural or corporate person by whom or on whose behalf the electronic message is sent whatever the case, but the party providing the service shall not be considered an originator with respect to producing, processing, transmitting or saving such electronic message and any other services service related thereto.
Addressee	:	The natural or corporate person the originator intends to send his message to, but the person providing the service shall not be considered an addresses with respect to receiving, processing or saving electronic correspondence or any other services related thereto.
Informative Program	:	A package of data, instructions and orders that can be run by means of information technology and prepared for accomplishing a particular task.
Electronic Message	:	Electronic data sent or received by electronic means, whatsoever the medium used for its production at the place where it is received.
Electronic Communication	:	Sending and receiving electronic messages.

Electronic Signature	:	A signature consisting of characters, numbers, symbols, sound or a processing system having an electronic form attached to or logically associated with an electronic message, and stamped with the intention of authenticating or approving such message.
Secure Electronic Signature	:	The electronic signature fulfilling the conditions of Article (18) hereof.
Signatory	:	The natural or corporate person who possesses an own electronic signing tool and who signs or on whose behalf the electronic message is signed using such tool.
Signing Tool	:	Electronic equipment or information prepared independently or in conjunction with other electronic equipment and information to affix the electronic signature for a particular person. Such process includes any systems or equipment generating or receiving specific information such as symbols or mathematical methodologies, characters, numbers, special keys, identification numbers or personal features.
Automated Electronic Medium	:	An electronic software or system of an information technology means that automatically operates independently, totally or partially, without supervision by any natural person at the time an action takes place or is responded to.

Automated Electronic Transactions	:	Transactions concluded or executed totally or partially by electronic means or records, in which such works shall not be subject to any follow up or review by a natural person.
Attestation services Provider	:	Any authorized or recognized person or authority that issues electronic certifications, or any services or assignments related thereto and to electronic signatures governed by the provisions hereof
Electronic Certification	:	A certificate issued by the attestation **services** provider that confirms the identity of the person or authority possessing a certain signing tool.
Strict Attestation Procedures	:	Procedures aimed at verifying that an electronic message is issued by a particular person and detecting any mistake or alteration in the contents or in sending or saving an electronic message or electronic record during a specific period, including any procedure which uses mathematical methodology, symbols, words or identification numbers or coding or procedures for response or acknowledgement of receipt and other information protection procedures.
Relying Party	:	The person who acts by relying upon an electronic certificate or signature.
Electronic Transaction	:	Any dealing, contract or agreement concluded or executed, in whole or part, by electronic

		correspondence.
Electronic Commerce	:	Electronic transactions conducted by means of electronic correspondence.

Chapter Two

Application and Objectives of the Law

Article (2)

1. Any matters not specifically provided for herein shall be governed by the rules of intentional trade custom related to electronic transactions and commerce and the general principles of civil and commercial transactions.

2. This law shall apply to electronic records, documents and signatures relating to electronic transactions and commerce, but its provisions shall not apply to the following:

A. Transactions and matters related to personal status such as marriage, divorce and wills.

B. Title deeds of immovable property.

C. Negotiable instruments.

D. Transactions pertaining to the sale, purchase, disposal of, lease for terms over ten years of immovable property, and the registration of any other rights related thereto.

(e) Any document required by the law to be notarized by the notary public.

(f) Any other documents or transactions excluded by a special legal provision.

(2) The Cabinet may by its resolution add any other transactions or matters to those contained in the above sub-clauses of clause 2 of this Article, make deletions therefrom or amend the same.

Article (3)

This Law aims at achieving the following:

1. Protecting the rights and determining the obligations of electronic dealers

2. Encouraging and facilitating electronic transactions and correspondence by means of reliable electronic records.

3. Facilitating electronic commerce, eliminating barriers to electronic commerce and any other electronic transactions that may result from uncertainties over writing and signature requirements, promoting the legal and business development for the implementation of electronic commerce in a secured manner.

4. Facilitating the transfer of electronic documents among government and non-government agencies and institutions, promoting the provision of services for such agencies and institutions efficiently by means of reliable electronic correspondence.

5. Minimizing the forgeries of electronic correspondence, and subsequent alterations of such correspondence, and fraud chances in electronic commerce and other electronic transactions;

6. Establishing unified principles for the rules, regulations and standards regarding the attestation and integrity of electronic correspondence.

7. Promoting confidence in the integrity and validity of electronic transactions, correspondence and records.

8. Enhancing the development of electronic commerce and other transactions at local and international levels through the use of electronic signatures.

Chapter Three

Requirements of Electronic Transactions

Electronic Correspondence

Article (4)

(1) No electronic message shall be denied legal effect or evidential weight solely on the grounds that it is in an electronic form.

(2) No information recorded in an electronic message shall be denied legal evidential weight even if it is received brief if the details of such information is available for review within the electronic system of its originator, and a reference is made to how it can be reviewed.

Retention of Electronic Records

Article (5)

(1) Where the law provides for retaining any document, record or information for any reason, such provision shall be fulfilled if such document, record or information is retained in the form of an electronic record, provided that the following conditions are satisfied:

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 contained therein remains accessible so as to be usable for subsequent reference;

C. Such information, if any, is retained as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received.

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

(3) A person may satisfy the requirements referred to in clause (1) hereof by using the services of any other person, as long as the conditions in such paragraph are complied with.

(4) Nothing in this Article shall affect:

A. Any other law which expressly provides for the retention of documents, records or information in the form of electronic records in accordance with a particular electronic system or by following particular procedures, or retention or correspondence via a particular electronic medium.

B. Freedom of the government authorities to determine additional requirements for retention of electronic records subject to its jurisdiction.

Third: Acceptance of Electronic Dealing

Article (6)

(1) Nothing in this law requires any person to use or accept information in electronic form. However, the person's consent may be concluded from his positive behavior.

(2) The parties concerned about originating, sending, receiving, saving or processing any electronic records may agree to contract in a manner averse to any provisions set forth in chapter three though chapter four of this law.

(3) By way of exception from the provisions of the precedent paragraph (1), the government's consent to deal electronically in transactions to which it is a party shall be express.

Fourth: Writing

Article (7)

Where the law requires any information, document, record, transaction or evidence to be written, or provides for certain consequences if it is not, the electronic document or record shall satisfy such requirement in so far as it complies with the provisions of paragraph (1) Article 5 hereof.

Fifth: Electronic Signature

Article (8)

(1) Where the law requires a signature on a document, or provides for certain consequences if a document is not signed, the electronic signature relied on within the context of Article (18) hereof shall satisfy the requirement.

(2) Any person may use any form of electronic certification, unless otherwise stipulated by the law.

Sixth: Electronic Original

Article (9)

Where the law requires that an electronic message is submitted or retained in its original form, or provides for certain consequences for failure to do so, the electronic message shall be considered original if:

(1) there exists a reliable technical assurance as to the integrity of the information set forth in the electronic message from the time it was first generated in its final form as an electronic document or record. The criterion for assessing the integrity

of information shall be whether such information has remained complete and unchanged with the exception of any addition, endorsement or change that may occur in the normal course of communication, storage or display. The degree of required reliability shall be assessed in the light of the purpose wherefore the information was generated and in the light of all the relevant circumstances.

(2) Where the message allows for displaying such information when required.

Admissibility and Evidential Weight of Electronic Evidence

Article (10)

(1) No electronic message or electronic signature shall be denied admissibility as evidence:

A. On the sole ground that such message or signature is in an electronic form;

B. On the sole ground that the message or signature is not original or in its original form, where such message or signature is the best evidence reasonably expected to be obtained by the person who uses it as evidence.

(2) In assessing the evidential weight of electronic information, the following elements shall be considered:

A- Extent of reliance on the way in which one or more of the processes of entering, generating, setting up, saving, presenting, or sending information are executed.

B-Extent of reliance on the way used to protect the integrity of information.

C- Extent of reliance on the information source if known.

D-Extent of reliance on the way used for verifying the originator's identity.

E-Any other element relevant to the subject matter.

3- In the absence of contradictory evidence, it is assumed that the secure electronic signature is:

reliable.
b. the signature of the relevant person.

c. affixed by such person with the intention to sign or approve the electronic message the issuance of which is attributed to him.

4- In the absence of contradictory evidence, it is assumed that the secure record:

a-has not changed since origination.
b-is reliable.

Chapter Four

First: Formation & Validity of Contracts

Article (11)

1. For contracting purposes, an offer and the acceptance of an offer may be expressed totally or partially by means of electronic correspondence.

2. The contract shall not be denied validity or enforceability on the sole ground that one or more electronic correspondence is used

Second: Automated Electronic Transactions

Article (12)

1. A contract may be formed between automated electronic mediums, including two or more electronic information systems already prepared and programmed for such tasks. The contract shall be proper, valid and legally effective, even if no natural person intervenes personally or directly concluding the contract in such systems.

2. A contract may be also concluded between automated electronic information system related to a natural or corporate person and another natural person if the latter knows or is assumed to know that such system will automatically undertake the concluding or implementing of the contract.

Third: Attribution

Article (15)

1. An electronic message shall be deemed to be that of the originator if it is sent by the originator himself.

2. As between the originator and the addressee, an electronic message shall be deemed to be that of the originator if it was sent: -

a. by a person who has the authority to act on behalf of the originator in respect of that electronic message; or

b. by an information system automated and programmed to operate automatically by or on behalf of the originator.

3. As between the originator and the addressee, the addressee is entitled to regard an electronic message as being that of the originator and to act on the basis of such assumption, if: -

A. in order to ascertain whether the electronic message is that of the originator, the addressee properly applies a procedure previously agreed to by the originator for such purpose; or

B. the electronic message, as received by the addressee, resulted from the actions of a person who based on his relationship with the originator or with any agent of the originator managed to gain access to a method used by the originator to prove that the electronic message is issued by him.

4. The provisions of paragraph (3) shall not apply in the following cases: -

A. From the time when the addressee has received notice from the originator that the electronic message is not that of the originator. In such case, the addressee must be given reasonable time to act according to the notice.

B. If the addressee knows or ought to have known that the electronic message was not issued by the originator, provided that he has exercises reasonable care or used any procedure agreed upon with the originator.

C. If it is unreasonable for the addressee to regard the electronic message as issued by the originator or to act on such assumption.

5. Where an electronic message is issued by or is deemed to be that of the originator, or where the addressee is entitled to act on such assumption pursuant to paragraphs (1), (2) & (3) hereof, then, the addressee within the frame of the relationship between the originator and the addressee shall be entitled to regard the received electronic message as the one the originator intended to send, and to act on such basis.

6. The addressee shall be entitled to regard each electronic message he receives as a separate electronic message and to act on such basis. Paragraph (7) hereof may not be applied when the addressee knows or should have known that the electronic message is a duplicate, provided that the addressee has exercised reasonable care or used any procedure upon with the originator.

7. The addressee shall not be entitled to the presumptions or conclusions set forth in the above paragraphs (5) & (6) of this Article when he knows or should have known that transmission resulted in any error in the electronic message as received, provided that the addressee has exercised reasonable care or used any procedure agreed upon with the originator.

Fourth: Acknowledgment of Receipt

Article (14)

1. The provisions of paragraphs (2), (3) and (4) of this Article shall apply where, on or before sending an electronic message, the originator has requested or has agreed with the addressee that receipt of the electronic message be acknowledged.

2. Where the originator has not agreed with the addressee that the acknowledgment be given in a particular form or by a particular method, an acknowledgment may be given by:

A. any message by the addressee, electronic, automated or otherwise; or

B.any conduct by the addressee to indicate that he has notified the originator that the electronic message has been received.

3. Where the originator has stated that the electronic message is conditional on receipt of the acknowledgment, this message shall not result in any legal effect until the acknowledgment is received by the originator.

4. Where the originator has requested acknowledgement of receipt without stating that the electronic message is conditional on receipt of the acknowledgment within the specified or agreed period or within a reasonable time, or, if no time has been specified or agreed, the originator:

A. may give notice to the addressee stating that no acknowledgment has been received and specifying a reasonable time within which the acknowledgment must be received; and

B. if the acknowledgment is not received within the time specified in paragraph 4 A. above, upon notice to the addressee, may treat the electronic message as though it has not been sent or exercise any other rights he may have.

5. Where the originator receives the addressee's acknowledgment indicating that he has received the message, this shall be evidence for receipt, unless evidence to the contrary is adduced by the addressee. However, such presumption shall not imply that the electronic message sent by the originator corresponds to the content of the message received.

6. Where the acknowledgment of receipt received by the originator states that the related electronic message has met technical requirements, whether agreed upon or set forth in applicable standards, it shall be presumed, unless the reverse is proved, that those requirements have been met.

7. Except in so far as it relates to the sending or receipt of the electronic message, this Article shall not apply to the legal consequences which may result from that electronic message or the acknowledgment of receipt.

Fifth: Time and Place of Transmitting and Receiving Electronic Messages

Article (15)

First: Unless otherwise agreed between the originator and the addressee

1.The transmission of an electronic message occurs when it enters an information system outside the control of the originator or the person who sent the message on behalf of the originator.

2.The time of receipt of an electronic message shall be determined as follows:

A. If the addressee has designated an information system for the purpose of receiving the electronic message, receipt occurs at the time when the electronic message enters the designated information system, or when it is retrieved by the addressee if it has been sent to an information system of the addressee other than the information system designated for receiving the message.

B. If the addressee has not designated an information system, receipt occurs when the electronic message enters an information system of the addressee.

Second: Clause (2) of the first paragraph of this Article shall apply notwithstanding that the place where the information system is located may be different from the place where the electronic message is deemed to be received under paragraph (3) below.

Third: Unless otherwise agreed between the originator and the addressee, an electronic message shall be deemed to be transmitted from the place where the originator has its place of business, and shall be deemed to be received at the place where the addressee has its place of business.

Fourth: In the application of this Article:

a. If the originator or the addressee has more than one place of business, the place of business shall be 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 shall be made to its usual place of residence; and

c. "Usual place of residence", in relation to a body corporate, means the principal place of business or the place where it is incorporated.

Chapter Five

Secure Electronic records and signatures

First: Secure Electronic Records

Article (16)

1. If strict attestation procedures stipulated in law or commercially reasonable or agreed upon between both parties are properly applied on an electronic record to verify that it has not been changed since a particular time, such record shall be treated as a secure electronic record since then until the time in which the verification has occurred.

2. In the application of this Article and Article (20) hereof, and to determine whether the strict attestation procedures are commercially reasonable, such commercial procedures and circumstances shall be considered when used, including: -

A. Nature of transaction;

B. Parties' experience and skill;

C. Size of similar transactions conducted by either of the parties or both;

D. Existence and cost of alternative procedures;

E. Generally used procedures for similar types of transactions.

Second: Secure Electronic Signature

Article (17)

1. Signature shall be treated as a secure electronic signature, if possible to verify through the application of strict attestation procedures, stipulated in this law or commercially reasonable and agreed upon between both parties, that the electronic signature was when executed: -

A. Solely used by the person who used it;

B. Possible to prove the identity of such person;

C. Under his total control, whether in respect of its creation or means of using it at the time of signing.

D. Linked with the relevant electronic message in a manner providing a reliable assurance on the accuracy of signature, so that the electronic signature will become insecure where the electronic record is changed.

E. Reliance on the secure electronic signature shall be reasonable unless the reverse is proved.

Third: Reliance on Electronic Signatures & Authentication Certificates

Article (18)

1. Any person may rely on the electronic signature or electronic certificate to the extent that such reliance is reasonable.

2. When an electronic signature is backed by an electronic authentication certificate, the party relying on such signature shall assume the consequences of his failure in taking the necessary reasonable measures to verify the authenticity and validity of such certificate, and whether suspended or revoked, and to comply with any restrictions with respect to such electronic authentication certificate.

3. To determine whether it is reasonable for a person to rely on electronic signature or certificate, a consideration, if appropriate, shall be given to:

A. The nature of the concerned transaction intended to be backed by the electronic signature.

B. The value or significance of the concerned transaction, if it is known to the partly relying on the electronic signature.

C. Whether the person who relied on the electronic signature or the attestation certificate has taken all necessary measures to determine the extent of reliance on such electronic signature or attestation certificate.

D. Whether the party who relied on the electronic signature or the electronic authentication certificate has taken all necessary measures to verify that the electronic signature is backed by an electronic authentic attestation certificate or expected to be as such.

E. Whether the party who relied on the electronic signature or the electronic authentication certificate has known or should have known that the electronic signature or the electronic authentication certificate were violated or cancelled.

F. Any agreement or previous relationship between the originator and the party who relied on the electronic signature or the electronic authentication certificate, or any prevailing commercial practice in this respect.

(g) Any other relevant factor.

4. If reliance on the electronic signature or electronic authentication certificate is unreasonable in the light of ambient circumstances, given the factors set forth in paragraph (2) of this Article, the party who relied on the electronic signature or electronic authentication certificate shall assume the risks of invalidity of such signature or certificate unless the reverse is proved.

Fourth: Duties of the Signatory

Article (19)

First: The Signatory shall:

1. not use his signing tool illegally

2. exercise reasonable care to avoid any unauthorized use of his signing tool.

3. notify the concerned persons without unjustified delay if:

a) The signatory knows that his signing tool has been compromised.

2) The circumstances known to the signatory give rise to a substantial risk that the signature may have been compromised.

4. Where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the electronic authentication certificate throughout the validity thereof.

Second: A signatory shall be liable for his failure to fulfill the requirements of paragraph (1) above.

Sixth: Provisions related to Electronic Authentication Certificates and Attestation Services

First: Attestation services Controller

Article (20)

For the purposes of this law, a Controller for Attestation services shall be appointed by resolution of the Cabinet for the particular purposes of licensing, certifying, monitoring and supervising the activities of attestation service providers.

Duties of Attestation Service Providers

Article (24)

1. attestation service provider shall:

A. Act in accordance with the data it submits concerning its activity.

B. Exercise reasonable care to ensure the accuracy and completeness of all material data submitted by its which are relevant to the electronic authentication certificate or included in it throughout its validity.

C. Provide reasonably accessible means which enable the party relying upon its services to ascertain the following: -

1. The identity of the attestation services provider;

2. That the person identified in the electronic authentication certificate had control over the signing tool at the time when the certificate was issued;

3. The method used in identifying the signatory;

4. Existence of any limitations on the purpose or value for which the signing tool may be used;

5. That the signing tool is valid and have not been compromised;

6. Whether the signatory has means to give notice pursuant to this law;

7. Whether there is a proper means to give notice about the revocation of signatures.

D. Provide a method for signatories to enable them to give notice that the signing tool has been compromised, and ensure the availability of a signature revocation service to be used on time.

E. Utilize trustworthy systems, procedures and human resources in performing its services.

F. Licensed by the Attestation Services Controller, if operating in the Emirate.

Second: In determining whether the procedures and human resources utilized by the service provider are trustworthy for the purposes of the above para (1)-(e), the following factors shall be considered:

A. Financial and human resources, including existence of assets within the sphere of competence;

B. Extent of confidence in the hardware and software systems;

C. Procedures for processing of certificates and applications for certificates and retention of records;

D. Availability of information to signatories identified in the electronic authentication certificates, and making the information available to the parties relying on the attestation 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 attestation service provider regarding compliance with and existence of the forgoing;

G. The extent to which the attestation service provider is subject to the jurisdiction of the Emirate's courts.

H. Extent of contradiction between the applicable law to the attestation service provider's business and the government laws.

Third: The electronic authentication certificate must set forth the following: -

A. Identity of attestation services provider.

B. The person identified in the electronic authentication certificate has control for the time being over the signing tool referred to in the certificate.

C. The signing tool was valid on or prior to the issuance date of the electronic authentication certificate.

D. Whether there are any limitations on the purpose or value for which the signing tool or the electronic authentication certificate may be used;

E. Whether there are any limitations on the scope or extent of liability assumed by the attestation services provider towards any person.

Fourth: In case of any damages arising due to invalidity of the electronic authentication certificate or any defect thereof, the attestation services provider shall be liable for the losses incurred by:

A. any party who entered into a contract with the attestation services provider for providing the electronic authentication certificate.

B. Any person who has reasonability relied on the electronic authentication certificate issued by the attestation services provider.

Fifth: The attestation services provider shall not be liable for any damage: -

A. If there is mentioned in the electronic authentication certificate a statement limiting the scope and extent of liability towards any related party pursuant to the regulations to be issued in this respect, and

B. If it proved that no mistake or omission has been committed by him, or that the damage has occurred for an alien reason beyond his control.

Regulation of Attestation service providers' Business

Article (22)

The Minister shall upon a proposal by the Controller issue regulations for the regulation and licensing of the business of the **attestation service** providers operating in the Emirate including:

1. The licenses and renewal of licenses of the attestation service providers and their authorized representatives and matters related thereto.

2. The activities of attestation service providers including the manner, method and place of soliciting business and attracting the public thereto.

3. The standards and rules to be maintained and followed by the attestation service providers in performing business.

4. Determining the appropriate standards with respect to the qualifications and experience of attestation service providers and the training of their employees.

5. Determining the conditions for the conduct of the business by the attestation services provider.

6. Determining the content and distribution of written, printed or visual materials and advertisements which may be distributed or used by a person with respect to an electronic authentication certificate or a digital key.

7. Determining the form and content of a digital certificate or key;

8. Determining the particulars to be recorded in the accounts kept by the attestation service providers.

9. Determining the qualifications of the auditor appointed by the attestation service providers.

10. Establishing the necessary rules for organizing the inspection and audit of the attestation service providers.

11. The conditions for the establishment and regulation of any electronic system by the attestation service provider, whether alone or in conjunction with other attestation service providers, and for the imposition and variation of such conditions or restrictions proposed by the Controller in consultation with competent bodies.

12. The manner in which a holder of a license conducts his dealings with his customers, conflict of interest involving the holder of a license and his customers, and his duties towards them with respect to digital electronic authentication certificates.

13. Proposing the fees to be paid in respect of any requirement under the provisions of this Article. A resolution relevant to such fees shall be issued by the Cabinet.

14. Preparing any forms for the purposes of applying this Article.

15. Financial fines and penalties prescribed for violating the rules regulating the business of the attestation service providers.

Recognition of Foreign Electronic Authentication

Certificates & Signatures

Article (23)

1. In determining whether an electronic certificate or an electronic signature is legally effective, no regard shall be given to the location where the certificate is issued or the electronic signature is created, or to the jurisdiction where the place of business of the party which issued the electronic certificate or signature is located.

2. The electronic authentication certificate issued by foreign attestation service providers shall be deemed the same as the certificates issued by attestation service providers operating under this law, if the practices of foreign attestation service providers offer at least an equivalent level of reliability to that required by Article (20) from the attestation service providers operating under this law, taking into consideration the recognized international standards.

3. Electronic signatures fulfilling the laws of another country may be recognized and considered as at the level of signatures created pursuant to the provisions of this law, if the laws of the other country stipulated a level of reliability at least equivalent to the level prescribed by this law for such signatures.

4. Concerning the recognition of foreign electronic authentication certificates and signatures stipulated in paragraphs (2), (3) above, regard shall be given to the factors set forth in paragraph (2), Article (21) of this law.

5. In determining whether an electronic signature or an electronic authentication certificate is legally effective, regard shall be given to any agreement between both parties on the transaction in which such signature or certificate is used.

6. Notwithstanding the provisions of paragraphs (2) & (3) above:

A. Parties to commercial and other transactions may agree on using certain attestation service providers or a certain category thereof, or certain category of electronic authentication certificates with respect to the electronic messages and signatures submitted to them.

B. In cases where the parties agree among themselves on using certain types of electronic signatures or electronic authentication certificates, such agreement shall be sufficient for the purposes of mutual recognition of the various jurisdictions of the states to which the parties belong, provided that such agreement is not illegal under the provisions of the applicable laws in the Emirate.

Chapter Eight

Use by the Government of Electronic Records and Signatures

Article (24)

1. In performing the functions assigned to them, governmental authorities may:

A. Accept the filing or submittal of documents, or the creation or retention of such documents in the form of electronic records.

B. Issue such permit, license, approval or consent in the form of electronic records.

C. Accept the fees or any other payments in an electronic form.

D. Offer tenders and receive bids related to governmental purchases in an electronic manner.

2. If the government decides to perform any of the functions mentioned in paragraph (1) hereof, then, it may specify:

3. A. The manner or form in which such electronic records shall be created, filed, saved or issued;

B. The manner, method and procedures by which such tenders shall be offered and such bids shall be received, and perform the governmental purchases.

C. The type of electronic signature required, including the condition that the sender uses a digital signature or another secure electronic signature.

D. The manner and form in which such signature shall be affixed to the electronic record, and the criteria that shall be met by the attestation services provider to whom the document is submitted for saving or filing.

E. The appropriate control processes and procedures to ensure the integrity, security and confidentiality of electronic records, payments and fees.

F. Any other attributes, conditions or provisions currently specified for sending paper records, if the same are required in respect of the electronic records of payments and fees.

Article (25)

No person may publish any electronic authentication certificate referring to an attestation services provider named in the certificate, if such person knows that:

A. The attestation services provider named in the certificate has not issued such certificate.

B. The signatory named in the certificate has not accepted it.

C. The certificate was cancelled or suspended, unless such publication is for verifying an electronic or digital signature used prior to suspension or cancellation

Chapter Nine

Penalties

Article (26)

There shall be punished by confinement for a term of not less than one year and a fine of not less than fifty thousand Dirhams or more than two hundred and fifty thousand Dirhams or either punishment any person who knowingly originates, publishes or provides or presents any false electronic authentication containing or referring to any incorrect data.

Article (27)

There shall be punished by confinement for a term not exceeding six months and a fine not exceeding one hundred thousand Dirhams or either punishment any person who intentionally presents incorrect data to an attestation service provider for the purpose of obtaining, canceling, suspending an electronic authentication certificate.

Article (28)

1. There shall be punished by confinement for a term not exceeding six months and a fine of not less than twenty thousand or more than two hundred thousand Dirhams or either punishment any person who by virtue of any powers conferred

to him herein obtains access to any information in electronic records, documents or correspondence or discloses any of such information.

2. The provisions of paragraph (1) of this Article shall exclude the cases of disclosure of information for the purposes of implementing this law, or any other judicial procedures.

Article (29)

There shall be punished by confinement for a term not exceeding six months and a fine not exceeding one hundred thousand Dirhams or either punishment any person who commits an act tantamount to a crime under the legislations in force using an electronic means.

Article (30)

1. There shall be punished by confinement or a fine of not less than ten thousand Dirhams or more than one hundred thousand Dirhams the heads, board chairmen and directors of a corporate body if they by their consent, connivance or any other act cause any provision of this law to be violated.

2. The employee of the corporate body shall be punished by confinement or a fine of not less than ten thousand Dirhams or more than one hundred thousand Dirhams if he commits an infraction of the provisions of this law or the regulations issued for the implementation thereof if it proved that the infraction resulted from his act, default, consent or connivance.

3. In case of conviction of the infractions in any of clause 1 or 2 above of this Article, the corporate body to which the convicts are dependent shall suffer a fine equal to that imposed on any of them.

Article (31)

Without prejudice to the rights of others acting in good faith, the Court may, in case of conviction under the provisions of this law, order the confiscation of the tools used for committing the crime.

Article (32)

The court shall order the repatriation of any foreigner in case of being sentenced to confinement under the provisions of this law.

Article (33)

The application of the penalties provided for in this law shall not prejudice any severer penalty that may be stipulated in any other law.

Chapter Ten

Final Provisions

The personnel of the ministry and local authority appointed by a resolution of the Minister of Justice, Islamic Affairs and Waqfs shall have the capacity of judicial officers to record any infraction of the provisions of this law or any executive regulations thereof.

Article (35)

The Minister shall issue the necessary regulations for implementation of the provisions of this law.

Article (36)

Any provision contradicting or conflicting with the provisions hereof shall be repealed.

Article (37)

This law shall be published in the official gazette and shall come into force as from the date of publication.

Khalifa bin Zayed Al Nahyan

President of the United Arab Emirates

Issued by us at the Presidential Palace, Abu Dhabi

On: 30 Dhul Hijjah 1426 AH

Corresponding to: 30 January 2006 AD