Federal Law No. (1) of 2006
On Electronic Commerce and Transactions

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

In cognisance of the Constitution, and

The Federal Law No. (1) of 1972 Regarding the Functions of Ministries and the Powers of Ministers and the amending laws thereof, and

The Federal Law No. (5) of 1975 Regarding the Commercial Register, and

The Federal Law No. (8) of 1980 on the Regulating Working Relationship and the amending laws thereof, and

The Federal Law No. (10) of 1980 on the Central Bank and the Monetary system and regulating the banking profession and the amending laws thereof, and

The Federal Law No. (8) of 1984 on Commercial Companies and the amending laws thereof, and

The Federal Law No. (9) of 1984 on Insurance Companies and Agencies and the amending laws thereof, and

The Civil Transaction Law issued by the Federal Law No. (5) of 1985, and

The Penal Law issued by the Federal Law No. (3) of 1987, and

The Federal Law No. (22) of 1991 on the Justice Registrar and the amending laws thereof, and

The Civil and Commercial Transactions Evidence Law issued by the Federal Law No. (10) of 1992, and

The Civil Procedure Law issued by the Federal Law No. (11) of 1992, and

The Penal Procedure Law issued by the Federal Law No. (35) of 1992, and

The Federal Law No. (37) of 1992 on the Trademarks and the amending laws thereof, and

The Commercial Transactions Law issued by the Federal Law No. (18) of 1993, and

The Federal Law No. (17) of 2002 on Regulating and Protecting the Industrial rights of Patents, and

The Federal Law by Decree No. (3) of 2003 on the Organization of the Telecommunications Sector, and

On the basis of the proposal of the Minister of Commerce and Planning, and the agreement of the Council of Ministers, and the approval of the High Federal Council, have issued the following Law:

Article (1)

The following words and expressions shall have meaning set out opposite unless the context shall require otherwise:

UAE:	United Arab Emirates
Government Departments:	Federal ministries, local departments and authorities and local and federal public entities and corporations
Ministry:	Ministry of Economy & Planning
Minister:	Minister of Economy & Planning
Competent Local Authority:	Competent local authority in each of the Emirates of the UAE
Electronic:	Relating to modern technology having electrical, digital, magnetic, wireless, optical, electromagnetic, automated, photonic or similar capabilities
Electronic Information:	Electronic data and information in the form of text, codes, sounds, graphics, images, computer programs or otherwise
Electronic Information System:	A group of software and systems for creating, generating, sending, receiving, storing, displaying or otherwise processing and managing messages electronically
Electronic Record or Document:	A record or document that is created, stored, generated, copied, sent, communicated or received by electronic means, on a tangible medium or any other Electronic medium and is retrievable in perceivable form
Computer:	An electronic, magnetic, optical, electrochemical or other device used to process information and perform logical and arithmetic operations or storage functions, including any connected or directly related facility which enables the computer to store information or communication
Originator:	A natural or legal person by whom, or on whose behalf, a Data Message is sent, whichever the case, but does not include a person who provides services in relation to producing, processing, sending or storing such Data Message and other related services

Addressee:	A natural or legal person who is intended by the Originator to receive the Data Message, but not a person who provides services in relation to receiving, processing or storing such Data Message and other related services
Computer Program:	A set of computer executable information, instructions and orders designed to accomplish a specific task
Data Message:	Electronic Information sent or received by Electronic means, whatever the method of retrieval at the place of receipt
Electronic Communication:	The sending and receipt of Data Messages
Electronic Signature:	Any letters, numbers, symbols, voice or processing system in Electronic form applied to, incorporated in, or logically associated with a Data Message with the intention of authenticating or approving the same
Secure Electronic Signature:	An Electronic Signature which meets the requirements set out in Article (18) 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 a Data Message by use of the device
Signature Creation Device:	A uniquely configured device or Electronic Information that is required, alone or in conjunction with other devices or Electronic Information, in order to create an Electronic Signature attributable to a specific person including 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 program or Electronic means used independently to initiate an action or response in whole or in part without review or action by an individual at the time of the action or response
Automated Electronic Transactions:	Transactions concluded or performed, in whole or in part, by Electronic means or Electronic records, in which the acts or records are not monitored or reviewed by an individual
Certification Service Provider:	An accredited or authorized person or organization that issues Electronic Attestation Certificates or provides other services in this connection and in relation to Electronic Signatures regulated by this Law
Electronic Attestation Certificate:	A certificate issued by a Certification Service Provider confirming the identity of the person or entity holding an Electronic Signature Creation Device
Secure Authentication Procedures:	Procedures aimed at verifying that a Data Message is that of a specific person and detecting error or alteration in the communication, content or storage of a Data Message or Electronic Record since a specific point in time, which may require the use of algorithms or codes, identifying words or numbers, encryption, answerback or acknowledgement procedures, or similar information security devices
Relying Party:	A party that acts in reliance on an Electronic Signature or Electronic Attestation Certificate
Electronic Transaction:	Any deal, contract or agreement concluded or performed, in whole or in part, through Electronic Communication
Electronic Commerce:	Commercial activities conducted through Electronic Communication

Chapter Two
Application and Object of the Law

Article (2)

1- Matters for which no specific provision is laid down in this Law shall be governed by the international commercial laws affecting Electronic Transactions and Commerce and the general principles of civil and commercial practice

2- This Law applies to Electronic Records, Documents and Signatures that relate to Electronic Transactions and Commerce but does not apply to:

   a) Transactions and issues relating to personal law such as marriage, divorce and wills;

   b) Deeds of title to immoveable property;

   c) Negotiable instruments;

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

   e) Any document legally required to be attested before a notary public; and

   f) Any other documents or transactions exempted by special provision of law

3- The Cabinet may decide upon an addition, deletion or modification to the list of transactions and matters appearing in subsection (2) of this article

Article (3)

The objects of this Law are as follows:

1- To protect the rights of persons doing business electronically and determine their obligations

2- To encourage and facilitate Electronic Transactions and Communications by means of reliable Electronic Records

3- To facilitate and eliminate barriers to Electronic Commerce and other Electronic Transactions resulting from uncertainties over writing and signature requirements, and promote the development of the legal and business infrastructure necessary to implement secure Electronic Commerce

4- To facilitate the electronic filing of documents with governmental and non-governmental agencies and departments and promote efficient delivery of the services of such agencies and departments by means of reliable Electronic Communications

5- Minimize the incidence of forged Electronic Communications, alteration of Communications and fraud in Electronic Commerce and other Electronic Transactions

6- Establish uniform rules, regulations and standards for the authentication and validity of Electronic Communications

7- Promote public confidence in the validity, integrity and reliability of Electronic Transactions, Communications and Records

8- Promote the growth of Electronic Commerce and other transactions on the national and international level through the use of Electronic Signatures

Chapter Three
Requirements for Electronic Transactions

One: Electronic Communications

Article (4)

1- A Data Message is not without legal force and effect merely on the grounds that it is in Electronic form

2- A Data Message that refers to information, without providing details of that information, is not without legal force, so far as this information is accessible within the context of the Electronic System of the Originator and the Message indicates the method of access

Two: Retention of Electronic Records

Article (5)

1- Where the law requires that certain documents, records or information be retained for any reason, that requirement is met by retaining Electronic Records, provided that the following conditions are satisfied:

a) the Electronic Record is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received;
b) the information contained therein is accessible so as to be usable for subsequent reference; and
c) such information, if any, is retained as enables the identification of the origin and destination of the Data Message and the date and time when it was sent or received

2- An obligation to retain documents, records or information in accordance with paragraph (c) of subsection (1) does not extend to any information necessarily or automatically generated solely for the purpose of enabling a message to be sent or received

3- A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions in that subsection are complied with

4- Nothing in this section shall:

a) apply to any rule of law which expressly provides for the retention of documents, records or information in the form of Electronic Records in accordance with a specific Electronic Information System or through specific procedures, or their retention or communication through a specific Electronic Agent

b) preclude any department of the Government from specifying additional requirements for the retention of Electronic Records that are subject to the jurisdiction of such department

Three: Admissibility of Electronic Transactions

Article (6)

1- Nothing in this Law shall require any person or employee to use or accept information in Electronic format, but a person's consent to do so may be inferred from his affirmative conduct

2- As between persons involved in generating, sending, receiving, storing or otherwise processing Electronic Records, the provisions of Chapters Two-Four of this Law may be varied by agreement

3- Notwithstanding the provisions of subsection (1), the Government must give explicit consent to dealing electronically in transactions to which it is a party

Four: Writing

Article (7)

If 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 the requirement if the provisions of subsection (1) of Article (5) of this Law are complied with

Five: Electronic Signature

Article (8)

1- Where a rule of law requires a signature on a document, or provides for certain consequences in the absence of a signature, that rule is satisfied if the document contains a reliable Electronic Signature within the meaning of Article (18) of this Law

2- Absent contrary statutory provision, a person may use any form of Electronic authentication

Six: Electronic Original

Article (9)

Where a rule of law requires a Data Message to be presented or retained in its original form, or provides for certain consequences if not so presented or retained, that requirement is met by a Data Message if:

1- there exists reliable assurance as to the integrity of the information contained in the Data Message from the time when it was first generated in its final form, as an Electronic Document or Record. The criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

2- if the message allows, when required, the display of the information sought to be presented

Seven: Admissibility and Evidential Weight of Electronic Records

Article (10)

1- In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to prevent the admission of a Data Message or Electronic Signature in evidence:

a) on the grounds that the message or signature is in Electronic format; or
b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that the message or signature is not original or in its original form

2- In assessing the evidential weight of Electronic Information, regard shall be given to:

a) the reliability of the manner in which one or more of the operations of executing, entering, generating, processing, storing, presenting or communicating was performed;
b) the reliability of the manner in which the integrity of the information was maintained;
c) the reliability of the source of information, if identifiable;
d) the reliability of the manner in which the Originator was identified;
e) any other factor that may be relevant

3- Absent proof to the contrary, it shall be presumed that a Secure Electronic Signature:

a) is reliable;
b) is the signature of the person to whom it correlates; and
c) was affixed by that person with the intention of signing or approving the Data Message attributed to him

4- Absent proof to the contrary, it shall be presumed that a Secure Electronic Record:

a) remained unaltered since creation; and
b) is reliable

Chapter Four
Electronic Transactions

One: Formation and Operation of Contracts

Article (11)

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 is not invalid or unenforceable solely by reason that Electronic Communication was used in its formation

Two: Automated Electronic Transactions

Article (12)

1- A contract may be formed by the interaction of Automated Electronic Agents that include two or more Electronic Information Systems preset and preprogrammed to carry out these tasks. Such contract would be valid and enforceable even if no individual was directly involved in the conclusion of the contract within such systems

2- A contract may be formed between an Automated Electronic Information System in the possession of a natural or legal person and another natural person, where the latter knows or has reason to know that the such a system will automatically conclude or perform the contract

Three: Attribution

Article (13)

1- A Data Message is that of the Originator if it was sent by the Originator himself

2- As between the Originator and the Addressee, a Data Message is deemed to be that of the Originator if it was sent:

   a) by a person who had the authority to act on behalf of the Originator in respect of the Data Message;
   b) by an Automated Information System programmed by or on behalf of the Originator to operate automatically

Four: Acknowledgement of Receipt

Article (14)

1- The provisions of subsections (2), (3) and (4) of this Article shall apply where, on or before sending a Data Message, or by means of that Data Message, the Originator has requested or has agreed with the Addressee that receipt of the Data Message 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, electronic, automated or otherwise; or

   b) any conduct of the addressee, sufficient to indicate to the Originator that the Data Message has been received

3- Where the Originator has stated that the Data Message is conditional on receipt of the acknowledgment, the Data Message is treated as though it had never been sent until the acknowledgment is received

4- Where the Originator has asked for an acknowledgement but has not stated that the Data Message is conditional on receipt of the acknowledgment 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 acknowledgment has been received and specifying a reasonable time by which the acknowledgment must be received; and

   b) if the acknowledgement is not received within the time specified in para (a) of this subsection, may treat the Data Message as though it has never been sent, or exercise any other rights it may have

5- Where the Originator receives the Addressee's acknowledgment of receipt, it is presumed, unless evidence to the contrary is adduced, that the related Data Message was received by the Addressee, but that presumption does not imply that the content of the Data Message sent by the Originator corresponds to the content of the message received from the Addressee

6- Where the acknowledgment received by the Originator states that the related Data Message 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 as it relates to the sending or receipt of the Data Message, this Article is not intended to address the legal consequences that may flow either from that Data Message or from the acknowledgment of its receipt

Article (15)

One: Unless otherwise agreed by the Originator and the Addressee:

1- The dispatch of a Data 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 a Data Message is determined as follows:

a) if the Addressee has designated an information system for the purpose of receiving Data Messages, receipt occurs at the time when the Data Message enters the designated Information System; or if the Data Message is sent to an Information System of the Addressee that is not the designated Information System, at the time when the Data Message is retrieved by the Addressee;

b) if the Addressee has not designated an Information System, receipt occurs when the Data Message enters an Information System of the Addressee

Two: Clause (2) of Section One of this Article shall apply notwithstanding that the place where the Information System is located may be different from the place where the Data Message is deemed to be received under Section Three of this Article

Three: Unless otherwise agreed between the Originator and the Addressee, a Data Message is deemed to be dispatched 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

Four: 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; and

c) "usual place of residence" in relation to a body corporate, means the place where it is incorporated or otherwise legally constituted

Chapter Five
Secure Electronic Records and Signatures

One: Secure Electronic Records

Article (16)

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

2- For the purposes of this Article and Article 17 of this Law, the determination of whether Secure Authentication Procedures are commercially reasonable shall take into account these procedures in the light of the commercial circumstances existing at the time the procedures were used, including:

a) the nature of the transaction;

b) the experience 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 and their cost; and

e) the procedure generally used for similar types of transactions

Two: Secure Electronic Signature

Article (17)

1- A signature shall be treated as a Secure Electronic Signature if, through the application of a prescribed Secure Authentication Procedure or a commercially reasonable Secure Authentication Procedure agreed to by the parties involved, 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 identifying such person;

c) was, at the time of signing, under the sole control of the Signatory in terms of the creation data and the means used; and

d) linked to the Electronic Record to which it relates in a manner which provides reliable assurance as to the integrity of the signature such that if the record was changed the Electronic Signature would be invalidated

2- Absent proof to the contrary, reliance on a Secure Electronic Signature is deemed reasonable

Three: Reliance on Electronic Signatures and Electronic Attestation Certificates
Article (18)

1- A person may rely on an Electronic Signature or Electronic Attestation Certificate to the extent that such reliance is reasonable

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 have relied on an Electronic Signature or Certificate, regard shall be had, if appropriate, to

a) the nature of the underlying transaction that Electronic Signature was intended to support;

b) the value or importance of the underlying transaction, if this 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 had 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 had taken appropriate steps to ascertain whether the Electronic Signature was supported or was 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 knew or ought to have known that the Electronic Signature or the Electronic Attestation Certificate had been compromised or revoked;

f) any agreement or course of dealing which the Originator has with the Relying Party in respect of the Electronic Signature or the Electronic Attestation Certificate, or any trade usage or practice which may be applicable;

g) any other relevant factor

4- Absent proof to the contrary, the party relying on an Electronic Signature or Electronic Attestation Certificate assumes the risk that the Electronic Signature or the Electronic Attestation Certificate is forged, if reliance on the Electronic Signature or the Electronic Attestation Certificate is not reasonable under the circumstances, having regard to the factors in subsection (2) of this Article

Four: Duties of Signatory

Article (19)

One: A Signatory shall:

1- not unlawfully use its Signature Creation Device;

2- exercise reasonable care to avoid the unauthorized use of its Signature Creation Device;

3- without undue delay, notify concerned persons if:

a) the Signatory becomes aware that the security of its Signature Creation Device has been compromised;

b) the circumstances known to the Signatory give rise to a substantial risk that the security of the Signature Creation Device may have been compromised; and

4- where an Electronic Attestation Certificate is used to support a Signature Creation Device, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the Signatory which are relevant to the Electronic Attestation Certificate throughout its life cycle

Two: A Signatory shall bear the legal consequences of its failure to satisfy the requirements of Section One of this Article

Chapter Six
Provisions Relating to Electronic Attestation Certificates and Certification Services

One: Certification Services Controller

Article (20)

For the purpose of this Law, the Cabinet shall appoint an authority to oversee certification services particularly in relation to the licensing, approval, monitoring and overseeing of the activities of Certification Service Providers

Two: Duties of the Certification Service Provider

Article (21)

One: A Certification Service Provider shall:

a) act in accordance with representations made by it with respect to its policies and practices;

b) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the Electronic Attestation Certificate throughout its life cycle or that are included in the certificate;

c) provide reasonably accessible means which enable a Relying Party to ascertain:

1) the identity of the Certification Service Provider;

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

3) the method used to identify the Signatory;

4) any limitation on the purpose or value for which the Signature Creation Device may be used;

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

6) whether means exist for the Signatory to give notice pursuant to this Law;

7) whether a timely signature revocation service is offered;

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

e) utilize trustworthy systems, procedures and human resources in performing its services;

f) be licensed by the Certification Services Controller if operating in the UAE

Two: For the purposes of para (e) under Section One above, in determining whether any systems, procedures and human resources are trustworthy, regard shall be had to the following factors:

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

b) quality of hardware and software systems;

c) procedures for processing and issuing Electronic Attestation Certificates and applications for certificates and retention of records;

d) availability of information to Signatories identified in Electronic Attestation Certificates and parties relying on certification services;

e) regularity and extent of audit by an independent body;

f) the existence of a declaration by the UAE, an accreditation body, or the Certification Service Provider regarding compliance with or existence of the foregoing;

g) certification Service Provider's susceptibility to the jurisdiction of the courts of the UAE;

h) the degree of discrepancy between the law applicable to the conduct of the Certification Service Provider and the law of the UAE;

Three: An Electronic Attestation Certificate shall state:

a) the identity of the Certification Service Provider;

b) that the person identified in the Electronic Attestation Certificate holds, at the relevant time, the Signature Creation Device referred to in the certificate;

c) that the Signature Creation Device was effective at or before the date when the certificate was issued;

d) any limitations on the purposes or value for which the Signature Creation Device or the Electronic Attestation Certificate may be used;

e) any limitation on the scope or extent of liability which the Certification Service Provider accepts to any person

Four: If damage has been caused as a result of the Electronic Attestation Certificate being incorrect or defective, a Certification Service Provider shall be liable for damage suffered by either:

a) a party who has contracted with the Certification 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 Certification Service Provider

Five: A Certification Service Provider shall not be liable for any damage if:

a) it included in the Electronic Attestation Certificate a statement limiting the scope or extent of its liability to any relevant person according to the regulations issued in this regard; or

b) it proves that it was not at fault or negligent or that the damage occurred for reasons beyond its control

Three: Regulation of the Conduct of Certification Service Providers

Article (22)

The Minister shall, at the recommendation of the Controller, issue rules for the regulation and licensing of Certification Service Providers operating in the UAE. These rules shall include:

a) applications for licenses or renewal of licenses of Certification Service Providers and their authorized representatives and matters incidental thereto;

b) specifying the activities of Certification Service Providers including the manner, place and method of soliciting business from the public;

c) specifying the standards and rules which Certification Service Providers have to maintain and follow in their business;

d) specifying appropriate standards with respect to the qualifications and experience which Certification Service Providers should possess and the training of their employees;

e) specifying the conditions subject to which Certification Service Providers shall conduct their business;

f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of an Electronic Attestation Certificate and the digital key;

g) specifying the form and content of an Electronic Attestation Certificate and the digital key;

h) specifying the form and manner in which accounts shall be maintained by Certification Service Providers;

i) specifying the qualification which auditors and Certification Service Providers should possess;

j) laying down regulations governing the inspection and auditing of the activities of Certification Service Providers;

k) specifying the terms and conditions for the establishment of any electronic system by a Certification Service Provider either solely or jointly with other Certification Service Providers and enforcing and revising those terms and conditions pursuant to the recommendation of the Controller and in coordination with the relevant authorities;

l) specifying the manner in which the licensee shall conduct its dealings with the subscribers including its conflict of interest policy and duties towards subscribers with respect to digital signature certificates;

m) specifying the fees to be paid in respect of any matter required under this Article based on a decision from the Cabinet;

n) prescribing any forms for the purpose of this Article;

o) specifying the fines and penalties applicable to breach of the rules governing the activities of Certification Service Providers;

Recognition of Foreign Certificates and Electronic Signatures

Article (23)

1- In determining whether an Electronic Attestation 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 Attestation Certificate or Signature had its place of business

2- Electronic Attestation Certificates issued by a foreign Certification Service Provider are recognized as legally equivalent to Certificates issued by Certification Service Providers operating under this Law, if the practices of the foreign Certification Service Provider provide a level of reliability at least equivalent to that required of Certification Service Providers operating in accordance with this Law, as provided under Article (21), and taking into consideration recognized international standards

3- Signatures complying with the requirements of laws of another state may be recognized as legally 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 subsections 2 and 3 above, regard must be had to the factors stated in Section Two of Article (21) of this Law

5- In determining whether an Electronic Signature or Electronic Attestation 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 was used

6- Notwithstanding subsections (2) and (3) above:

a) Parties to commercial and other transactions may specify that a particular Certification Service Provider, class of Certification Service Providers or class of certificates must be used in connection with Data Messages or signatures submitted to them

b) Where parties agree, as between themselves, to the use of certain types of Electronic Signatures or Electronic Attestation Certificates, that agreement shall be recognized as sufficient for the purpose of cross-border recognition between the various jurisdictions of states, unless that agreement would not be valid or effective under applicable law of the UAE

Chapter Eight
Government Use of Electronic Records and Signatures

Article (24)

1- Government Departments may, within the scope of their legal duties:

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

b) issue any permit, license, decision or approval in the form of Electronic Records;

c) accept fees and other payments in Electronic form;

d) put out tenders and receive bids relating to Government procurement by Electronic means

2- In any case where the Government decides to perform any of the functions in subsection (1), the Government may specify:

a) the manner and format in which such Electronic Records shall be created, filed, retained, submitted or issued;

b) the manner, method and process by which Government tenders are put out , bids are received, and Government procurement is made;

c) the type of Electronic Signature required (including, if applicable, the requirement that the sender use a digital signature or other Secure Electronic Signature);

d) the manner and format in which such signature shall be affixed to the Electronic Record, and the criteria that shall be met by any Certification Service Provider to whom the document is submitted for filing and retention;

e) control processes and procedures as appropriate to ensure adequate integrity, safety, security and confidentiality of Electronic Records, payments or fees; and

f) any other required attributes, conditions or rules for Electronic Records of payments and fees that are currently specified for corresponding paper documents

Article (25)

No person shall publish a certificate with reference to a Certification Service Provider listed in the certificate, with the knowledge that:

a) the Certification Service Provider listed in the certificate has not issued it;

b) the subscriber listed in the certificate has not accepted it; or

c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying an Electronic Signature or digital signature used prior to such suspension or revocation

Chapter Nine
Penalties

Article (26)

The penalty shall be imprisonment for a period of not less than 1 year and a fine of not less than AED 50,000 and not more than AED 250,000 or either for anyone who knowingly creates, publishes, offers or provides any Electronic Attestation Certificate containing or referring to incorrect information

Article (27)

The penalty shall be imprisonment for a period not exceeding 6 months and a fine not exceeding AED 100,000 or either for anyone who deliberately provides incorrect information to a Certification Service Provider when requesting an Electronic Attestation Certificate or requesting the revocation or suspension of an Electronic Attestation Certificate

Article (28)

1- The penalty shall be imprisonment for a period of not less than 6 months and a fine of the not less than AED 20,000 and not more than AED 200,000 or either for anyone who, pursuant to any powers conferred under this Law, obtains access to information in Electronic Records, Documents or Communications and discloses the same

2- Excluded from subsection (1) of this Article shall be cases of disclosure that are made for the purpose of this Law or judicial proceedings

Article (29)

The penalty shall be imprisonment for a period not exceeding 6 months and a fine not exceeding AED 100,000 or either for anyone who, through the use of Electronic means, commits an act which constitutes an offence under the laws in force

Article (30)

1- The penalty shall be imprisonment or a fine of not less than AED 10,000 and not more than AED 100,000 where an offence under this Law has been committed with the consent, or connivance of, or is attributable to any act of a chairman or member of board of directors or manager of a body corporate

2- The penalty shall be imprisonment or a fine of not less than AED 10,000 and not more than AED 100,000 where an offence under this Law or any of its implementing regulations has been committed by an employee of a body corporate, and it is proved that the offence has been committed with his consent or connivance, or is attributable to any negligence on his part

3- In case of conviction per subsections (1) or (2) of this Article, the body corporate employing the convicted parties shall be ordered to pay a fine equivalent to the fine ordered against any of them

Article (31)

A court convicting per this Law shall direct the confiscation of the tools and devices used in the commission of the offence without prejudice to the rights of bona fide third parties

Article (32)

A court sentencing a foreign national to imprisonment per this Law shall also order him deported

Article (33)

The penalties prescribed under this Law shall be enforced without prejudice to any severer penalty provided for by any other law

Chapter Ten
Closing Provisions

Article (34)

Employees of the Ministry and the Competent Local Authority appointed by the Minister of Justice, Islamic Affairs & Awqaf shall act as law enforcement officers for the purpose of detecting and establishing offences which are committed in violation of this Law and its implementing regulations

Article (35)

The Minister shall issue the regulations and decisions necessary to enforce this Law

Article (36)

All provisions contravening the provisions of this Law are hereby repealed

Article (37)

This Law shall be published in the Official Gazette and shall take effect from the date of publication

HH SH. Khalifa bin Zayed Al Nahyan
President of the State of the United Arab Emirates

Issued at the Presidential Palace in Abu Dhabi
Dated: 30 Dhul-Hijjah 1426H
Corresponding to: January 30, 2006