

## **FEDERAL LAW NO . 1**

Issued on 30/01/2006

Corresponding to 30 Dhu al - Hijjah 1426 H .

### **CONCERNING ELECTRONIC TRANSACTIONS AND COMMERCE**

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

Pursuant to the perusal of the Constitution ; and

Federal Law no . 1 of 1972 regarding the Jurisdiction of Ministries and the Powers of Ministers and the amending laws thereof ; and

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

Federal Law no . 8 of 1980 regarding the Regulation of Labor Relations and the amending laws thereof ; and

Federal Law no . 10 of 1980 regarding the Central Bank , the Monetary System and Regulation of Labor Relations and the amending laws thereof ; and

Federal Law no . 8 of 1984 regarding the Commercial Companies and the amending laws thereof ; and

Federal Law no . 9 of 1984 concerning the Insurance Partners and Agents and the amending laws thereof ; and

Civil Transactions Law issued by Federal Law no . 5 of 1985 and the amending laws thereof ; and

Penal Code issued by Federal Law no . 3 of 1987 ; and

Federal Law no . 22 of 1991 regarding the Notary public and Federal Law no . 10 of year 1992 ; and

Law of Substantiation of Commercial and Civil Transactions issued by Federal Law no . 10 of 1992 ; and

Civil Procedure Law issued by Federal Law no . 11 of 1992 ; and

Penal Procedure Law issued by Federal Law no . 35 of 1992 ; and

Federal Law no . 37 of 1992 concerning Trademarks and the amending laws thereof ; and

Commercial Transactions Law issued by Federal Law no . 18 of 1992 ; and

Federal Law no . 17 of 2002 regarding Regulation and Protection of Industrial Property of Patents , Drawings and Industrial Designs ; and

Federal Decree - Law no . 3 of 2003 regarding the Regulation of Telecommunications Sector ; and

Acting upon the proposal of the Minister of Economy and Planning and the approval of the Council of Ministers , and the ratification of the Federal Supreme Council ,

Have promulgated the following Law :

## **CHAPTER ONE**

### **DEFINITIONS**

#### **Article 1**

The following words and terms shall have the meanings assigned to them below unless the context indicates otherwise :

The State : The United Arab Emirates State .

Government Authorities : Federal Ministries , local departments and authorities , organizations , and general , Federal and local establishments .

The Ministry : The Ministry of Economy and Planning .

The Minister : The Minister of Economy and Planning .

The competent local authority : the competent local authority in each Emirate member of the state .

Electronic : whatever relates to modern technology having electrical , digital , magnetic , confidential , luminous powers or the like .

Electronic information : data and information of electronic features in the form of texts , symbols , sounds , drawings , images , computer programs or other .

Electronic information system : group of programs and systems designed for processing and administering data and information to create , retrieve , send , receive , store , electronic mail displaying and others .

Electronic record or document : a record or document to be established , stored , retrieved , copied , sent , notified , or received by electronic means

through tangible medium or any other electronic medium and shall be retrievable in perceivable form .

Information means : electronic management , magnetic , optical , electrochemistry or any other tools used to process data , perform logic and arithmetic or storage functions , and it includes any storage capability of data and communications relate or function in conjunction with a similar tool .

The originator : Physical or juristic person who himself or through his representative , send an electronic message of whatever instance . Shall not be considered originator , any party carries out the duty of services provider concerning production , processing , sending or saving this electronic message and any other services related to it .

The addressee : Physical or juristic person whom the originator has intended to send him his message . Shall not be considered an addressee , the person who provides the services concerning receiving , processing or saving the electronic messages and other related services .

Computer program : Group of data , instructions and orders enforceable through information means designed for a specific task .

Electronic message : electronic information sent or received by electronic means whatever retrieving means used at the place of receipt .

Electronic Messenger : Sending and receipt of electronic messages .

Electronic signature : Signature composed of letters , numbers , symbols , sound or electronic processing system attached or logically connected to an electronic message imprinted with intent of ratification or adoption of that message .

Protected Electronic Signature : Electronic signature observing the conditions of Article 18 of the present Law .

Signer : Physical or juristic person acquiring an electronic signature tool of his own , and who signs or the signing shall be performed on his behalf on the electronic message by using the mentioned tool .

Signature tool : a system or electronic information designed independently or in participation with other electronic systems and information to set down an electronic signature to a definite person , these operations comprehend any systems or tools that produce or receive certain information like symbols , mathematical methods , letters , numbers or personal private keys .

Confidential Electronic agent : A program or an electronic system of an automated information tool that works independently , in whole or in part , without supervision of any physical person at the time of action or response .

Confidential Electronic transactions : Transactions to be concluded or performed , in whole or in part by electronic means or records , and where these activities or records are not followed up or reviewed by a physical person .

Authentication Services Provider : any person or duly accredited party issues electronic authentication certificates or any services or tasks related to it and to electronic signatures regulated by the provisions of the present Law .

Electronic authentication certificate : A certificate issued by authentication services provider in which he indicates the identity of the person or the party acquiring a specified signature tool .

Protected Authentication Procedures : procedures aiming to ascertain that an electronic message is initiated by or to a certain person , and to discover any error or modification in contents , sending or saving an electronic message or an electronic record within a fixed period , this shall include any procedure uses mathematical methods , symbols , words , identification letters , codes , procedures of reply or acknowledgment of receipt and other means of information security procedures .

Accredited party : the person who acts depending on an electronic signature or an electronic authentication certificate .

Electronic transaction : Any dealing , contract or agreement concluded or enforced in whole or in part by electronic messages .

Electronic commerce : Commercial transactions carried out by electronic messages.

## **CHAPTER TWO**

### **APPLICABILITY OF THE LAW AND ITS OBJECTIVES**

#### **Article 2**

1 - The rules of international commercial customs concerning electronic transactions and commerce and the general rules of civil and commercial transactions shall apply on all matters not provided for in this Law .

2 - This Law shall apply to electronic records , documents and signatures related to electronic transactions and commerce , the following instances shall be excluded from the provisions of this Law :

a - Transactions and matters concerning civil status like marriage , divorce and wills .

b - Title deeds of real estates .

c - Bonds in circulation .

d - Transactions concerning the sale and purchase of real estates , its disposition and rental for periods in excess of ten years and the registration of any other rights related to it .

e - Any document required by Law before Notary Public .

f - Any other documents or transactions to be excluded by a special legal term .

3 - The Council of Ministers may decide to add any other transactions or matters to whatever is mentioned in previous sections of paragraph two of this Article , or to cancel or modify it .

### **Article 3**

Purposes of this Law are :

1 - To protect the rights of electronic users and determine their obligations .

2 - To promote and facilitate electronic transactions and communications through reliable electronic records .

3 - Facilitate and eliminate any obstacles to the electronic commerce and other electronic transactions resulting from ambiguity relating to writing and signature requirements , and to enhance legal and commercial development to ensure the implementation of electronic commerce .

4 - To Facilitate the transferring of electronic documents between governmental authorities and establishments and non - governmental in addition to enhance supplying the services of these authorities and establishments efficiently and through reliable electronic messages .

5 - To Decrease forgery of electronic messages and changes to these messages and to decrease fraud opportunities in electronic commerce and other electronic transactions .

6 - To set uniformed principles of the rules , bylaws and the standards concerning ratification and reliability of electronic messages .

7 - To enhance confidence in the validity and reliability of electronic transactions , messages and records .

8 - To enhance the development of electronic commerce and other transactions locally and globally through using electronic signatures .

## **CHAPTER THREE**

### **REQUIREMENTS OF ELECTRONIC TRANSACTIONS**

#### **FIRST : ELECTRONIC MESSAGES**

##### **Article 4**

1 - Electronic message shall not be denied legal effect and enforceability solely because it is in electronic form .

2 - Information proven in the electronic message shall not be denied legal conclusiveness , even if is briefly mentioned , if review of the details of these information is available within the electronic system of its originator , and that review directions are indicated in the message .

#### **SECOND : RETENTION OF ELECTRONIC RECORDS**

##### **Article 5**

1 - If the law requires retention of document , record or information for whatever reason , this condition is satisfied by retention of this document , record or information in electronic record form , provided that the following conditions are observed :

a - Retention of the electronic record in its original form , in which it was generated , sent or received , or in form accurately reflects the information as it was originally generated , sent or received .

b - Retention of information be accessible for later usage and reference .

c - Retention of information – if existing - which enables to determine the electronic message origin , destination , date and time of its sending and receipt .

2 - The obligation concerning retention of documents , records or information pursuant to section ( c ) of paragraph ( 1 ) of this Article shall not be extended to any information generates necessarily and spontaneously solely to enable record sending and receipt .

3 - Any person may satisfy the requirements specified in paragraph ( 1 ) of this Article by resorting to the services of another person provided that the conditions specified in the mentioned paragraph are observed .

4 - Nothing in this Article precludes the following :

a - Existence of a term in another law decides to retain documents , records or information in the form of electronic records pursuant to a specified electronic information system or to adopt certain procedures , retention or communication through determined electronic agent .

b - The right of the governmental authorities to determine additional requirements for the retention of electronic records subject to its jurisdiction .

### **THIRD : ACCEPTANCE OF ELECTRONIC DEALING**

#### **Article 6**

1 - This Law does not demand any person to use or accept information in electronic form , but the consent of this person is concluded from his positive conduct .

2 - All parties relating to generating , sending , receiving , storing or processing any electronic record are allowed to conclude agreements contrary to any of the provisions mentioned in Chapter 2 to Chapter 4 of this Law .

3 - As an exclusion of the provisions of paragraph ( 1 ) previously mentioned , the Government's acceptance of electronic dealing in transactions to which it is a party must be explicit .

### **FOURTH : WRITING**

#### **Article 7**

If the law requires any statement , document , record , transaction or evidence to be written , or if determines specific results upon non - writing , the electronic document or record shall satisfy this condition if the provisions of paragraph ( 1 ) of Article 5 of this Law is observed .

### **FIFTH : ELECTRONIC SIGNATURE**

#### **Article 8**

1 - If the law requires the existence of signature on a document , or if determines any specific results upon this signature , eventually ; the electronic signature reliable within the meaning mentioned in Article 18 of this Law is satisfying this condition .

2 - Any person may use any form of electronic ratification forms unless the law otherwise provides .

## **SIXTH : ELECTRONIC ORIGINAL**

### **Article 9**

If the law requires submission of the electronic message or its retention in its original form , or decided specific consequences for non - observance , the electronic message shall be considered original if the following conditions are satisfied :

1 - If any technical evidence confirms the reliability of the information mentioned in the electronic message after it was first generated in its final form as electronic document or record . The standard for evaluating the reliability of information is determination of whether it is complete and unchanged , excluding any addition , endorsement , changing that may occur during the normal situation of notification , storage and display .

The degree of reliability demanded must be evaluated in the light of the purpose for which the information is generated , and in the light of the related circumstances .

2 - If the message allows to display the information to be submitted on demand .

## **SEVENTH : ACCEPTANCE AND CONCLUSIVENESS OF ELECTRONIC EVIDENCE**

### **Article 10**

1 - Shall not preclude from accepting the electronic message or electronic signature as an evidence :

a - That the message or signature is in electronic form .

b - That the message or signature be not original or in its original form , when this electronic message or signature is the best acceptable evidence obtainable by the person using it as a proof .

2 - For the evaluation of the conclusiveness of the electronic information evidence , the following factors must be observed :

a - The extent of reliability of the method by which one or several transactions of information entry , establishment , preparation , storage , submission or sending are carried out .

b - The extent of reliability of the method used to preserve the information validity .

c - The extent of reliability of information source if known .

d - The extent of reliability of the method by which the identity of the originator is ascertained .

e - Any other element related to the subject .

3 - Unless otherwise is established , the protected electronic signature must be :

a - Reliable .

b - The signature of the person attributed to him .

c - Set by that person with the intent to sign or ratify the electronic message attributed to him .

4 - Unless otherwise is established , the protected electronic record must be :

a - Unchanged since it was generated .

b - Recognized .

## **CHAPTER FOUR**

### **ELECTRONIC TRANSACTIONS**

#### **FIRST : SETTING UP CONTRACTS AND ITS VALIDITY**

##### **Article 11**

1 - For contracts purposes , it is allowed to express the offer and acceptance in whole or in part through the electronic message .

2 - The contract may not be denied its validity or enforceability solely because it is concluded in one or several electronic messages .

#### **SECOND : CONFIDENTIAL ELECTRONIC TRANSACTIONS**

##### **Article 12**

1 - It is allowed to conclude contracts between confidential electronic mediums that include two or several electronic information systems , designed and programmed in advance to perform so , the agreement shall be deemed valid , enforceable and giving its legal effects even in the instance of no personal or direct interference of any physical person in the contract conclusion in the systems .

2 - It is allowed to conclude contracts between a confidential electronic information system in the possession of physical or juristic person and another physical person , should this latter knows or supposed to know that the system shall conclude the contract automatically .

### **THIRD : REFERENCE**

#### **Article 13**

1 - The electronic message shall be attributed to the originator should he issue it himself .

2 - Concerning the relation between the originator and the addressee , the electronic message shall be attributed to the originator should it be sent :

a - From a person competent to act on behalf of the originator concerning the electronic message .

b - From a confidential information system automated by the originator or on his behalf .

3 - Concerning the relation between the originator and the addressee , the addressee is entitled to consider the electronic message as issued by the originator and act on the basis of this presumption :

a - If the message is correctly implemented , a procedure previously agreed upon by the originator to verify that the electronic message is issued by this originator for this purpose .

b - If the electronic message as received by the addressee , resultant from the acts of a person enabled by virtue of his relation with the creator or by his deputy to access the method used by the creator to prove that the electronic message is issued by him .

4 - The provisions of the paragraph ( 3 ) of this Article shall not be applicable :

a - From date of receipt of notification by the addressee sent by the originator in which he states that the electronic message is not issued by him , provided that the addressee was enabled enough time to react on the basis of the notification .

b - If the addressee knew or should have known that the electronic message was not issued by the originator , should he exerts reasonable efforts or uses any procedure agreed upon with the originator .

c - Should it be impossible for the addressee to consider the electronic message as issued by originator or act on the basis of this presumption .

d - When the electronic message is issued or deemed as issued by the originator or when the addressee is entitled to act due to this presumption pursuant to paragraphs ( 1 ), ( 2 ), ( 4 ) of the provisions of this Article , the addressee is entitled within the framework of the relation between him and the originator to consider that the electronic message received , is the message intended to be sent by the originator , and to act on this basis .

5 - The addressee is entitled to consider every electronic message received by him as independent message and act on this basis , paragraph ( 7 ) of this Article shall not be enforceable if the addressee knew or should have known - should he exerts reasonable efforts or uses any procedure agreed upon with the originator – that the electronic message is a second copy .

6 - The addressee shall not be entitled to presumptions and conclusions mentioned in paragraphs ( 5 ), ( 6 ) of this Article if he knew or should have known should he exerts reasonable efforts or uses any procedure agreed upon , that transmission has attributed to an error in the electronic message as received by him .

#### **FOURTH : ACKNOWLEDGMENT OF RECEIPT**

##### **Article 14**

1 - The provisions of paragraphs ( 2 ), ( 3 ) and ( 4 ) of this Article shall be applicable when the originator demand the recipient or agree with him , before or at the time of sending the electronic message , to send an acknowledgment of receipt .

2 - Should there is no agreement between the originator and the recipient that the acknowledgment of receipt must be in specific form or method , the acknowledgment of receipt may be performed through :

a - Any message from the recipient whether by electronic means , confidential or any other means .

b - Any conduct of the recipient indicates that he has notified the originator of receiving the electronic message .

3 - If the originator mentioned that the electronic message is conditioned upon receiving an acknowledgment of receipt , accordingly it shall have no legal effect until the originator receives the acknowledgment .

4 - If the originator demands an acknowledgment of receipt without mentioning that the electronic message is conditioned upon receiving an acknowledgment of receipt during the determined time limit or agreed upon or within a reasonable time limit , if a specific time is not determined or agreed upon , the originator may :

a - Notify the recipient that he has not received any acknowledgment of receipt and determine a reasonable time in which he should receive this acknowledgment .

b - If the acknowledgment of receipt is not received within the time limit specified in section ( a ) of this paragraph , the originator is allowed to consider the electronic transaction as not sent , or exercise other rights .

5 - If the originator receives an acknowledgment from the recipient indicating that he has received the electronic message , this shall be considered as proof of delivery unless the recipient submits a proof to the contrary , this presumption shall not impliedly include that the electronic message sent from the originator conform to the content of the message received by the recipient .

6 - If the acknowledgment of receipt received by the originator provides that the related message has observed all the technical conditions , whether agreed upon , or determined by the standards in effect , it is supposed that these conditions were satisfied unless proven otherwise .

7 - Excluding any matter related to sending or receiving the electronic message , this Article shall not apply to legal effect resultant from electronic message or acknowledgment of receipt .

## **FIFTH : TIME AND PLACE OF SENDING ELECTRONIC MESSAGES**

### **Article 15**

First : Unless otherwise agreed between the originator and the addressee :

1 - The electronic message is sent when using information system not subject to the control of the originator or the person who sent the message on his behalf .

2 - Time of receipt of 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 shall be at the time of entering the electronic message into the designated electronic system or when retrieving the message by the recipient should it be sent to an information system subject to it other than the information system designated to receive the message .

b - If there is no information system designated by the addressee , time of receipt shall be when the electronic message enters an information system subject to the addressee .

Second : Section ( 2 ) of ( First ) of this Article shall apply even if the place wherein the information system is located differs from the place wherein the electronic message is deemed to be received under paragraph ( Third ) of this Article .

Third : unless otherwise agreed between the originator and the recipient , the electronic message is deemed to be sent from the originator's place of business and to be received at the recipient's place of business .

Fourth : For the enforcement of the provisions of this Article :

a - If the originator or recipient has more than one place of business , the place of business shall be the place having the closest relationship to the underlying transaction , or the principal place of business if there is no underlying transaction .

b - If the originator or recipient does not have a place of business , the place of business is the habitual residence .

c - The habitual residence concerning juristic person , is the head office or place of establishment .

## **CHAPTER FIVE**

### **PROTECTED ELECTRONIC RECORDS AND SIGNATURES**

#### **FIRST : PROTECTED ELECTRONIC RECORDS**

##### **Article 16**

1 - If precise authentication procedures whether specified in the law or commercially acceptable and agreed upon between the parties , were properly implemented on an electronic record to verify that it is unchanged since a specified period , this record shall be treated as protected electronic record from that time until verification time .

2 - For the enforcement of the provisions of this Article and Article 17 of this Law , and within the field of determination whether the precise authentication procedures are commercially acceptable , for those procedures commercial circumstances at time of its usage shall be reviewed in addition to :

a - Nature of Transaction .

b - Expertise and skills of parties .

c - Volume of similar transactions performed by one party or by both of them .

d - Existence of substitute procedures and its cost .

e - Procedures used generally in similar types of transactions .

## **SECOND : PROTECTED ELECTRONIC SIGNATURE**

### **Article 17**

1 - Signature shall be deemed protected electronic signature if it is possible to verify through the implementation of precise authentication procedures designated in this Law or commercially acceptable and agreed upon between the parties that the electronic signature at the time of its execution :

a - Is attributed only to the person who used it .

b - It is possible to prove the identity of that person .

c - It is fully controlled by him whether concerning its creation or usage at time of signing .

d - It is connected to the concerned electronic message by a link that provides reliable proof as regards the signature validity , accordingly if the electronic record is changed , the electronic signature will no longer be protected .

2 - The electronic signature shall be accepted as a proof unless otherwise established .

## **THIRD : RELYING ON ELECTRONIC SIGNATURES AND AUTHENTICATION CERTIFICATES**

### **Article 18**

1 - The person is entitled to rely on electronic signature or electronic authentication certificate to the extent of which such reliable is acceptable .

2 - When electronic signature is enhanced with electronic authentication certificate , the party relying on that signature shall be responsible for the consequences of his failure to adopt necessary reasonable steps to verify the validity and applicability of such certificate , and whether it is suspended or canceled , and observance of any restrictions concerning the electronic authentication certificate .

3 - To determine whether it is possible for a person to rely on an electronic signature or electronic authentication certificate , the following factors must be considered :

a - Nature of the concerned transaction intended to be enhanced by the electronic signature .

b - Value or importance of the concerned transaction if acknowledged by the party relying on the electronic signature .

c - If the person relying on the electronic signature or electronic authentication certificate , has adopted appropriate steps to determine the extent of reliability of electronic signature or electronic authentication certificate .

d - If the party relying on the electronic signature has adopted appropriate steps to verify that the electronic signature is enhanced by electronic authentication certificate or supposed to be so .

e - If the party relying on the electronic signature or electronic authentication certificate , has known or should have known that the electronic signature or electronic authentication certificate was violated or canceled .

f - Agreement or previous dealing between the originator and the party relying on the electronic signature or electronic authentication certificate or any other commercial custom common in this matter .

g - Any other related factor .

4 - If relying on this electronic signature or electronic authentication certificate is impossible in the light of the surrounding circumstances due to the factors mentioned in paragraph 2 of this Article , the party relying on the electronic signature or electronic authentication certificate shall be responsible for all the risks resultant from the non - validity of that signature or certificate unless otherwise established .

#### **FOURTH : THE SIGNERS' DUTIES**

##### **Article 19**

First : The signer must :

1 - Not use his signature tool unlawfully .

2 - Exert reasonable effort to preclude using his signature tools by unlicensed usage .

3 - Notify the concerned person without any unjustifiable delay , in the instance of :

a - The signer's knowledge that his signature tool is exposed to what indicates doubts in its safety .

b - If established due to the circumstance acknowledged by him that his signature tool is exposed to what evoke doubts .

4 - Exert reasonable efforts to ensure precise and perfection of whatever he submit of statements and essential declarations related to the electronic authentication certificate at its effectiveness period , these are the instances in which the signature tool requires the use of this certificate .

Second : The signer is responsible for his failure to comply with requirements of paragraph ( First ) of this Article .

## **CHAPTER SIX**

### **PROVISIONS RELATED TO ELECTRONIC AUTHENTICATION CERTIFICATES AND AUTHENTICATION SERVICES**

#### **FIRST : AUTHENTICATION SERVICES CONTROLLER :**

##### **Article 20**

For the purposes of this Law , the Council of Ministers shall designate an authority to control over authentication services and particularly for the purposes of licensing , authentication and controlling the activities of authentication services providers and its supervision .

#### **SECOND : THE DUTIES OF THE AUTHENTICATION SERVICES PROVIDER**

##### **Article 21**

First : The authentication services provider must :

a - Act according to the information submitted concerning the exercise of his activity .

b - Exert reasonable effort to ensure submitting precise and complete essential data related to the electronic authentication services or mentioned in it during its applicability .

c - Provide accessible means which enable the party relying on his services to ascertain from the following :

1 - The identity of the authentication services provider .

2 - That the person whose identity is determined in the electronic authentication certificate is controlling the signature tool indicated in this certificate at the concerned time .

3 - The method used to determine the signer's identity .

4 - Whether any restrictions on the purpose or value to which the signature tool is allowed to be used .

5 - That the signature tool is valid and is not exposed to what evoke doubts .

6 - Whether the signer has a notification means pursuant to this Law .

7 - Whether there is appropriate means to notify about signature cancellation .

d - Provide means to the handicapped enabling them to submit a notification indicates that the signature tool is doubtful and ensure the availability of signature cancellation service usable at the appropriate time .

e - Use while carrying out his services reliable regulations , procedures and human resources .

f - Be licensed by the authentication services controller if working in the State .

Second : To determine the reliability of regulations , procedures or human resources for the purposes of paragraph ( 1 / e ) above - mentioned , the following must be taken into consideration :

a - Financial and human resources including the availability of assets within the jurisdiction area .

b - Extent of trust in computer programs and systems .

c - Processing procedures , issuance of electronic authentication certificates , applications for obtaining these certificates and retention of records .

d - Availability of the information concerning the signers designated in the electronic authentication certificates , in addition to providing the information to the parties relying on authentication services .

e - Regularity and the extent of accounts reviewing by an independent authority .

f - Existence of announcement from the State , accredited authority or the authentication services provider concerning the existence of whatever he mentioned or committed to .

g - Extent of compliance of the authentication services provider to the judicial jurisdiction of the States' court .

h - Extent of incompatibility between the law enforced on the activities of the authentication services provider and the States' laws .

Third : The electronic authentication certificate must determine the following :

a - Identity of the authentication services provider .

b - That the person whose identity is specified in the electronic authentication certificate is controlling the signature tool indicated in this certificate at the concerned time .

c - That the signature tool was valid during or before the date of issuing the electronic authentication certificate .

d - If there are any restrictions on the purpose or value to which the signature tool or the electronic authentication certificate is allowed to be used .

e - If there are any restrictions on the scope or extent of responsibility accepted by the authentication services provider towards any person .

Fourth : Should any damages resultant from the invalidity of the electronic authentication certificate or existence of any default , the authentication services provider shall be responsible for the losses sustained :

a - If inscribed in the electronic authentication certificate , a statement restricting the scope and extent of his responsibility towards any concerned person in compliance with the regulation issued in this matter .

b - If he establishes that he has not committed any mistake or negligence , or that the damage is resultant from a foreign cause .

Third : Regulating the Work of the Authentication Services Provider :

## **Article 22**

The Minister shall issue ; on the proposal of the controller , the regulations concerning regulating and licensing the work of the authentication services providers working in the State including the following :

1 - Licensing and license renewal of the authentication services providers , their authorized representatives and renewal of these licenses and matters related to it .

2 - Activities of the authentication services providers including the method and place where they obtain their works and public attraction .

3 - Standards and rules to be observed and adopted by the authentication services providers in their works .

4 - Determination of the appropriate standards concerning the qualifications and expertise of the authentication services providers and training regarding their works .

5 - Determination of the conditions of business administration carried by the authentication services providers .

6 - Determination of contents and distribution of written , printed and visual items and announcements which are allowed to be distributed or used by any person concerning any electronic authentication certificate or digital key .

7 - Determination of the form and content of any electronic authentication certificate or digital key .

8 - Determination of the details to be set down in the accounts retained by the authentication services provider .

9 - Qualifications to be observed by the auditors of the authentication services providers .

10 - Setting down the rules necessary to regulate searching and examining the acts of the authentication services providers .

11 - Conditions of setting up and regulating any electronic system by the authentication services provider , whether solely or in participation with other authentication services providers , impose and change these conditions or restrictions according to the proposal of the controller and in coordination with the competent authorities .

12 - The method adopted by the license beneficiary to administer his transactions with the clients , also in case of contradiction between his interests and their interests and his duties towards them concerning the digital electronic authentication certificates .

13 - Proposition of duties to be collected concerning any order requested pursuant to the provisions of this Article . These duties shall be determined by a decision given by the Council of Ministers .

14 - Setting down any forms for the purposes of the enforcement of this Article .

15 - Financial fines and penalties decided for the violation of the rules concerning licensing and regulating the activities of the authentication services providers .

## CHAPTER SEVEN

### RECOGNITION OF ELECTRONIC AUTHENTICATION CERTIFICATES AND FOREIGN ELECTRONIC SIGNATURES

#### Article 23

1 - To determine whether the electronic authentication certificate or the electronic signature is in effect , shall not be taken into consideration either the place where the certificate or electronic signature is issued or the judicial jurisdiction wherein the place of business of the party that issued this certificate or the electronic signature is located .

2 - The electronic authentication certificate issued by foreign authentication services provider , shall be deemed as an electronic authentication certificate issued by the authentication services providers working pursuant to this Law , if the acts of the foreign authentication services providers are reliable at least in a standard equivalent to the standard required by Article 20 concerning the authentication services providers working pursuant to this Law , taking into consideration the accredited international standards .

3 - It is allowed to recognize signatures satisfying the conditions of the laws of another State , and consider it in the same level of the signatures issued in compliance with the provisions of this Law , if the laws of other countries set down conditions standard of credit to signatures equivalent at least to the standard required by this Law to these signatures .

4 - For the recognition of electronic authentication certificates and foreign electronic signatures specified in paragraphs ( 2 ), ( 3 ) previously mentioned , it is necessary to review the factors mentioned in paragraph ( 2 ) of Article 21 of this Law .

5 - To determine whether the electronic signature or electronic authentication certificate is in effect , it is necessary to take into consideration any agreement between the parties as regards the transaction using that signature or certificate .

6 - As an exclusion from the provisions of paragraphs ( 2 ), ( 3 ) previously mentioned :

a - The parties of commercial transactions and other transactions are allowed to agree to employ specific authentication services providers or group of them or a specific category of the electronic authentication certificates concerning the letters and electronic signatures submitted to them .

b - In the instances in which the parties agree to use specific types of signatures or electronic authentication certificates , this agreement shall be sufficient for purposes of mutual recognition to judicial jurisdiction of the countries to which the parties are subject , provided that this agreement be not unlawful according to the provisions of the laws enforced in the State .

## CHAPTER EIGHT

### GOVERNMENTAL USE OF ELECTRONIC RECORDS AND SIGNATURES

#### Article 24

1 - Governmental authorities within the scope of its duties assigned to them by law are allowed to perform the following acts :

a - Acceptance of deposit or submission of documents or its generation , or retention in the form of electronic records .

b - Issuance of any permission , license , decision or approval in the form of electronic records .

c - Acceptance of duties or any other payments in electronic form .

d - Putting forth bids and receiving auctions concerning governmental purchases by electronic means .

2 - If the Government decides to execute any of the acts mentioned in paragraph 1 of this Article , it shall be allowed thereupon to determine :

a - The manner or form in which the electronic records must be created , deposited , retained , submitted or issued .

b - The manner , means , method and procedures carried out to put forth bids , receive auctions , and fulfill governmental purchases .

c - The type of the electronic signature required including stipulating that the sender uses a digital signature or another protected electronic signature .

d - The manner and form to be adopted to affix the signature to the electronic record and the standard to be met by the authentication services provider to whom the document is submitted for retention and deposit .

e - Control processes and procedures as appropriate to ensure the safety , security and secrecy of the electronic records , payments or duties .

f - Any other features , conditions or provisions currently determined for sending paper documents , if requested so concerning the electronic records related to payments and duties .

### **Article 25**

It is not allowed to any person to publish an electronic authentication certificate which refers to the authentication services provider whose name is mentioned in this certificate , if this person acknowledges that :

a - The authentication services provider whose name is mentioned in the certificate has not issued it .

b - The signer whose name is mentioned in this certificate has not accepted it .

c - This certificate is cancelled or stopped unless the publishing is aiming to ascertain from electronic or digital signature used before stoppage or cancellation .

## **CHAPTER NINE**

### **PENALTIES**

#### **Article 26**

Shall be sentenced to imprisonment of at least one year and by a fine that may range between fifty thousand Dirhams and two hundred and fifty thousand Dirhams or either of these two penalties whoever creates , publishes , provides or submits any electronic authentication certificate which includes or refers to incorrect data with his knowledge of this .

#### **Article 27**

Shall be sentenced to imprisonment of six months at most and by a fine not in excess of one hundred thousand Dirhams or either of these two penalties whoever submits to the authentication services provider an application using incorrect information aiming for the issuance , cancellation , stoppage of electronic authentication certificate .

#### **Article 28**

1 - Shall be sentenced to imprisonment for at least six months and by a fine that may range between twenty thousand Dirhams and two hundred thousand Dirhams or either of these two penalties any person , due to any powers

granted to him managed to review information in electronic records , documents or messages , and discloses any of this information .

2 - Shall be excluded from the provisions of paragraph ( 1 ) of this Article the instances where declaration of information is carried out for purposes related to the enforcement of this Law or execution of any judicial procedures .

### **Article 29**

Shall be sentenced to imprisonment for six months at most and by a fine not in excess of one hundred thousand Dirhams or either of these two penalties whoever commits an act that forms a crime according to legislations in effect , by using electronic means .

### **Article 30**

1 - Shall be sentenced to imprisonment or by a fine that may range between ten thousand Dirhams and one hundred thousand Dirhams , the presidents and members of general assemblies and the directors of the juristic person should they cause due to their consent or concealment or any conduct incurred to a violation of any provision of the provisions of this Law .

2 - The employees of the juristic person shall be sentenced to imprisonment or by a fine that may range between ten thousand Dirhams and one hundred thousand Dirhams should they contravene the provisions of this Law or its implementing regulations in case it is established that the violation is a result of his conduct , negligence , consent or concealment .

3 - In the instance of conviction regarding any of the two sections 1 and 2 of this Article , the juristic person to whom the convicted individuals are subject shall be penalized by a fine equivalent to the fine rendered against any of them .

### **Article 31**

Without prejudice to the rights of a third party of good faith , and in the instances of conviction according to the provisions of this Law , the court may decide to confiscate machines and tools used in committing the crime .

### **Article 32**

The court shall decide to expatriate the foreigner if a judgment of imprisonment is rendered against him pursuant to the provisions of this Law .

### **Article 33**

Enforcement of the penalties specified in the present Law shall not affect any greater penalties specified in another law .

## CHAPTER TEN

### FINAL PROVISIONS

#### Article 34

The employees of the Ministry and the competent local authority who are designated by a decision given by the Minister of Justice , Islamic Affairs and Endowments by agreement with the Minister shall have the capacity of judicial officers to investigate any violation to this Law and its implementing regulations .

#### Article 35

The Minister shall issue regulations and decisions necessary for the implementation of the provisions of this Law .

#### Article 36

Any provision contrary or inconsistent with the provisions of this Law is abrogated .

#### Article 37

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

Presidential

Promulgated by Us at the

Palace in Abu Dhabi

On 30 Dhu al - Hijjah 1426 H .

Corresponding to 30/01/2006

**Khalifah Bin Zayed Al Nahyan**

**President of the United Arab Emirates  
State**

This Federal Law has been published in the Official Gazette , issue no . 442 , page 31 .