Electronic Transactions Law
Chapter One
Definitions and General Provisions

Article (1)

In the application of this Law, The following words and expressions shall have the meaning assigned to them, unless the context otherwise provides:

Government	:	The units of the state Administrative Apparatus and ex officio units.
Minister	:	The Minister of National Economy.
Competent Authority	:	The Information Technology Authority.
Electronic Transaction	:	Any action or contract concluded or to be partially or wholly executed by electronic messages.
Electronic	:	Any kind of means of modern technology with electric or digital or magnetic or wireless or optical or electromagnetic or photic or any other means of equivalent nature.
Electronic Message	:	Electronic information to be sent by electronic means whatever the method of its extraction at the location of receiving.
Electronic Mailing	:	Sending and receiving electronic messages.
Electronic Record	:	A contract or register or data message originated or stored or extracted or copied or sent or being informed or received by electronic means through a tangible intermediary or any other intermediary and should be receivable and understandable.
Electronic Data	:	Information or data to be interchanged electronically in the form of texts or symbols or sounds or pictures or photos or charts or computer programs or any other database.
Electronic Data Interchange	:	Transfer of information from person to person using an agreed standard to structure the information.
Electronic Intermediary	:	A computer program or system or any other electronic means used for processing or responding to any process with the intention of originating or sending or receiving data message without interference of natural person.
Computer Program	:	A collection of electronic information or instructions used directly or indirectly for processing electronic information with the purpose of obtaining specific results.
Intermediary	:	The natural or juristic person who, on behalf of another, sends or receives or adopt or store an electronic transaction or performs services related to such a transaction.
Processing System	:	An electronic system for treating and processing data and information automatically for the purpose of

		originating or sending or receiving or storing or presenting or programming or analyzing such data and information.
Originator	:	Any person sends an electronic message or to be sent on his behalf upon a proper power of attorney.
Addressee	:	The natural or juristic person whom the originator of the electronic message intends to receive his message.
Signatory	:	The person who possesses, from the competent authority, electronic signature and he signs on behalf of himself or on behalf of his appointee or those who represent them legally.
Signature Originating tool	:	A tool used for originating an electronic signature such as a software electronic device
Electronic Signature	:	Signing an electronic message or transaction in the form of letters or digits or symbols or signs or others and should be unique capable of determining the character of the person signed and identifying him from others.
Authentication Procedure	:	The procedure aimed to verifying that an electronic message has been issued by a certain person and detection of any mistake or amendment in the contents of or sending or storing electronic message or electronic record within a certain period of time. This includes any action in which logarithm or symbols or defining words and numbers or ciphering or reply procedure are admitting receipt or any other means of similar information protection.
Certification Service Provider	:	Any person or approved licensed authority authorized to issue electronic certificates or any other services related to such certification and electronic signatories.
Certificate	:	An electronic certification issued by the certification service provider confirming the link between the signatory and the data of the electronic signature.
Approved Party	:	A person who acts pursuant to a certificate or electronic signature.
Processing Personal Data	:	Any process or series of processes conducted on the personal data through automatical means or other, or collecting or recording or organizing or storing or amending or modifying or retrieving or reviewing or disclosing such data through sending or distribution or making it accessible by other means or coordinating or joining to each other or concealing or deleting or cancelling such data.
Ciphering	:	The process of changing a text or document or electronic message into unknown or scattered symbols impossible to be read or known without being retrieved to its original text.

Article (2)

This Law aims to:

1. Facilitate electronic transactions by using reliable electronic messages or records.
2. Remove any obstacles or challenges encountering electronic transactions resulting from ambiguities associated with writing and signature and enhancing the basic legal structure for secured electronic transactions.
3. Facilitate the transfer of electronic documents and subsequent amendments.
4. Minimize cases of forgery on electronic correspondences and subsequent amendments and committing frauds on electronic transactions
5. Set up unified principles for rules and regulations and standards relating to authentication and safety of electronic correspondences and records.
6. Consolidate the public trust in the safety and authenticity of electronic transactions, correspondences and records.
7. Develop the electronic transactions at the national Gulf and Arabic domain by using the electronic signature.

Article (3)

The provisions of this Law shall apply to electronic transactions, records, signatures and to any electronic messages.

This law shall not apply to:

a. Transactions and matters related to Personal Status Law such as marriage, divorce, wills and endowments.
b. Court procedures, judicial summons, proclamations, summons, search orders, arrest orders and judicial decrees.
c. Any document required by Law to be authenticated by the Notary Public.

Article (4)

1. The provisions of this law shall apply to transaction between the parties who agree on conducting their transactions by electronical means and the consent of each party may be inferred from his conduct. As to the Government, its consent to electronical dealing shall be given expressly.
2. The parties involved in originating or sending or receiving or storing or processing electronic records may agree on dealing in a way different to any of the rules provided for in Chapter 2 up to 4 of this Law.
3. Any agreement between the parties to conduct any transaction by electronical means shall not be obligatory on either party to conduct other transactions by the same means.

Article 5

The competent Authority shall determine the system of electronical payments after agreement with the Central Bank of Oman.

Article 6

The intermediary and the Certification Service provider shall, on their own cost, provide all technical components such as equipments, devices, systems and programs that allow the security authorities to enter their systems to achieve national security requirements provided that the provisions of such service shall be in line with the provisions of the technical components according to the state of the art techniques. The Ministry of Finance shall provide all requirements needed for connecting all hardwares of used by these security authorities to

achieving the objectives of National Security with those hardwares used by the intermediary and the Certification Service provider as the National Securities council may decides. The intermediary and the certification service provider shall bear all costs of updating and connections to hardwares used by these security authorities in case of changes in their systems according to the decisions to be issued by the competent Authority and the Laws into force.

Chapter two
Legal Consequences Ensuing from Electronic Messages and Electronic Transactions Requirements

Article (7)

The electronic message shall have legal effect and shall be deemed true and enforceable like the written document if the conditions provided for in this law and the executive regulations are observed in its origination and approval.

Article (8)

(1) Where any law requires the retention of any document or record or information or data for any reason, then such retention shall be ascertained by retaining that document or record or information or data in electronical form if the following conditions are satisfied:

(a) The document or record or information or data are retained electronically in the form they were originated or sent or received or in a form capable of proving accurately that the document or record or information or data originated or sent or received in its original form

(b) The document or record or information or data shall remain retained in a way to render it accessible, usable and retrievable for subsequent reference.

(c) The document or record or information or data shall be retained in a way to enable the identification of their origin and destination and the date and time when they were sent or received.

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

(a) Any other Law providing expressly for retention of a document or record or information or data in electronical form pursuant to any established electronic system or by following certain procedures or their retention or sending them through a certain electronic intermediary.

(b) Any other additional requirements to be determined by the Government for the retention of its electronic records under its possession.

Article (9)

Where the Law requires the writing of any document or record or transaction or information or statement or provides for consequences otherwise, then that requirement of writing is met by submission of any of the above in electronical form if the conditions provided for in the previous article are observed.

Article (10)
Where the Law requires the provision of a message or record or document in its original form and provides for consequences otherwise, then the electronic message or electronic record or electronic document will be regarded as original if there exist a reliable assurance or means allowing display of the information intended to be provided in an understandable way and to verify the integrity of the information contained in any of the above documents.

Article (11)
1- In the application of the rules of evidence in any legal proceedings, nothing shall apply so as to deny the admissibility of the electronic message on the ground that it is not in its original form if the message is the best evidence that the person adducing it could reasonably be expected to obtain.

   Such a message shall have evidential weight with regard to be had to the following:

   (a) The reliability of the manner in which the message was performed or entered or generated or processed or stored or presented or sent.
   (b) The reliability of the manner in which the integrity of the information was maintained.
   (c) The reliability of the source of information if such source is well known.
   (d) The reliability of the manner in which its originator was identified
   (e) Any other relevant factor.

2- Unless the contrary is proved, the electronic signature shall be deemed protected if the conditions stipulated in Article (22) of this Law are satisfied and it intends to signing or authenticating the electronic message on which it was put or related and it has not being changed since being originated, and it is a reliable signature.

Chapter Three
Electronic Transactions and Contract Formation

Article (12)
1- For the purposes of contracting, any offer and the acceptance may be expressed by means of electronic messages. Such expression shall be considered as binding on all parties whenever it is given in accordance with the provisions of this Law.
2- The contract shall not be denied validity or its enforceability for the reason that it was concluded by one or more electronic messages.

Article (13)
1- The contract may be concluded between auto-electronic media having electronic information system or more already prepared and programmed to do such tasks, and the contracting shall be valid and enforceable irrespective of any personal or direct interference of any natural person in the process of concluding the contract.
2- The contract may be concluded between any information system owned by a natural or Juristic person and another natural or juristic person if he knows or should have known that the contract will be concluded by that system. The electronic contracts shall have the same legal effects associated with contracts concluded in the normal ways whether in its validity or evidential value or enforceability and any other rules.

Article (14)
The responsibility of the Intermediary:

1- The Intermediary shall not be held responsible civilly or criminally for any informations received in the form of electronic records concerning a third party, if the Intermediary is not the originator of such information and his role is restricted to providing access to such information, if such responsibility arises on:
   (a) Originating or publishing or distributing such information or any data included therein.
   (b) Trespassing on any of the personal rights related to such information.
2- For absolving the intermediary from responsibility based on the provisions of this Article the following shall be ascertained:
   (a) He has no knowledge of any facts or circumstances, in the ordinary course of things, capable of creating criminal or civil responsibility.
   (b) In case of his knowledge of any of the above, he has immediately removed all informations, from any information system under his control and stopped access to or display of such information.
3- The provisions of this Article will not impose any legal obligation on the intermediary with regard to monitoring any informations in the form of electronic records relating to a third party if his sole role is only to provide access to such records.
4- The provisions of this Article will not affect the following:
   (a) Any obligations arising out of any contract.
   (b) The obligations imposed by any legislation in respect of providing communication services.
   (c) The obligations imposed by other legislation or enforceable Judicial decree related to restricting or preventing or removal of any informations in the form of electronic records or blocking such informations.
5- In the application of this Article, providing access to any information of third party, shall mean the availability of technical means that facilitate access to informations in the form or electronic records concerning a third party or disseminate or even increase efficacy of dissemination and this shall include auto or provisional saving of information with the purpose of accessing it. In the application of this Article, the third party shall mean any person upon whom the intermediary has no actual control.

Article (15)

1- The electronic message shall be considered issued by the originator in the following situations:
   (a) If the originator has generated it himself.
   (b) As between the Originator and the addressee, the electronic message shall be considered as generated by the originator if it was sent:
      i. By a person who has authority to act on behalf of the originator in respect of the said electronic message.
      ii. In accordance with an information system programmed by or on behalf of the originator, to operate automatically.
2- The addressee shall consider the electronic message as being transmitted by the originator and shall act on that assumption in the following two cases:
   (a) If the addressee has applied properly a procedure previously agreed to by the originator for the ascertainment whether the electronic message was that of the originator.
   (b) If the electronic message as received by the addressee resulted from the acts of a person whose relationship with the originator or any agent of the originator will enable that person to gain access to a method used by the originator to identify to the addressee that the electronic message was that of the originator.

This sub-article shall cease to be effective as from:

1- The time when the addressee has received notice from the originator that the electronic message is not that of the originator and the addressee had been given reasonable time to act accordingly.
2- The time when the addressee came to know or ought to have known had he exercised reasonable care or used an agreed procedure that the electronic message is not that of the originator.

This sub-article is also ineffective if it is not acceptable for the addressee to consider that the electronic message is that of the originator or to act in accordance with this assumption and the addressee is entitled to consider each electronic message received by him as an independent correspondence and to act on that assumption only unless he knows or ought to have known if he exercises reasonable care or uses an agreed procedure that the electronic message was a mere duplicate.

Article (16)

Where the originator has requested the addressee or agreed with him on or before sending the electronic message or through that message, that the acknowledgement of receiving that message shall be admitted, then the provisions of Article (15) of this law shall be applied subject to the followings:

1) Where the originator has stated that the electronic message is conditional on receipt of the acknowledgement, the electronic message is to be treated, with regard to the rights and obligations as between the originator and the addressee, as though it has never been sent until the acknowledgement is received by the originator.
2) Where the originator has requested an acknowledgement of receipt of the electronic message but he has not stated that the electronic message is conditional on receipt of the acknowledgement within the time specified or agreed upon, or that such time is not agreed or specified, then the originator shall give to the addressee notice stating that no acknowledgement has been received and specifying a reasonable time within which the acknowledgement shall be received. If the acknowledgement is not received within the time specified or agreed upon, the originator may, upon notice to the addressee, treat the message as though it had never been sent.
3) Where the originator received the addressee's acknowledgement of receipt, it is presumed that the related electronic message was received by the addressee unless the contrary is proved. That presumption does not imply that the contents of the electronic message sent by the originator corresponds to the message received by the addressee.
4) Where the originator has not agreed with addressee that the acknowledgement be given in a particular form or by a particular method, then an acknowledgement may be communicated by mean of any correspondence from the side of the addressee electronically or otherwise or any conduct of the addressee capable of confirming to the originator that the electronic message has been received.
5) Where the acknowledgement received by the originator states that the related electronic message met the technical requirements whether those agreed upon or stated in the applicable standards, it is presumed that those requirements were met until the contrary is proved.

Article (17)

Unless otherwise agreed between the originator and the addressee:

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

(2) The time of receipt of the electronic message is determined as follows:
   (a) If the addressee has designated an information system for the purpose of receiving electronic messages, then receipt occurs at the time when the message enters the designated information system and if the message is sent to an informations system the time of receipt will be the time when the message is retrieved by the addressee.
   (b) If the addressee has not designated an information system, then receipt occurs when the message enters an information system of the addressee.

(3) The electronic 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 even if the place where the information system is located differ from the place where the message is presumed to be received.

(4) 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 and if the originator or the addressee does not have a place of business, then reference is to be made to its habitual residence.

Chapter Four
Methods of Protecting Electronic Transactions

Article (18):

Ciphering is to be used as a mean of protecting electronic transactions in order to keep the information and the data of the message confidential and to verify the person of the originator and to prevent others from getting information or electronic messages so as not to reach the addressee or to corrupt them.

Article (19)

One of the following means shall be used to protect information systems:

(a) Public key Ciphering.
(b) Firewalls.
(c) Information Filters.
(d) Non-repudiation means.
(e) File and Message Ciphering Technology.
(f) Protecting of backup Data.
(g) Anti Worms and Anti Virus Programs.
(h) Any other means authorized by competent Authority.

Article (20)

Save the ciphering keys determined by the National Security Council, the employee designated by the competent authority may request from any owner of ciphering key to allow him checking the necessary informations pertinent to that key and the owner of the key shall handover the key to that employee.

Article (21)

1- Where specific authentication procedure were applied as agreed upon between the parties on electronic record to verify that it has not been changed since a certain time, then such a record shall be treated as a protected electronic record since that time up to the time of verification.

2- Where no agreement exists between the parties, the authentication procedure shall be deemed acceptable according to sub-article (1) of this Article and Article (22) of this law taking into consideration the circumstances relating to the parties especially:
   (a) The nature of the transaction.
   (b) The knowledge and experience of the parties.
   (c) The volume of similar transaction to which any or all of the parties is a party.
   (d) The existence of alternative procedures.
   (e) The cost of the alternative procedures
   (f) The deployed procedures in similar transactions

Article (22)

The electronic signature shall be considered protected and reliable on the ascertainment of the followings:

(a) The signature originating tool, in the course of its usage is limited to the signatory and no other person.
(b) The signature originating tool, was at the time of signing under the control of the signatory and no other person.
(c) That any alteration to the electronic signature after the time of signing is discoverable.
(d) That any alteration in the information related to the signature after the time of signing is discoverable. However, any concerned person may adduce evidence to prove that the electronic signature is reliable or not.

Article (23)

1- A person may rely on the electronic signature or the certificate to the extent that such reliance is reasonable.
2- Where the approved party receives an electronic signature confirmed by certificate, it is presumed that this party has verified the accuracy of the certificate and its enforceability and that he relies only on the certificate as issued according to its conditions.
3- For deciding whether the electronic signature or the certificate is reliable, the following shall be observed:
   (a) The nature of the transaction intended to be confirmed by the electronic signature or the certificate.
   (b) The value or the importance of the transaction if this is available.
   (c) That the party relying on the electronic signature or the certificate has taken appropriate steps to decide whether such electronic signature or the certificate is reliable.
   (d) Any previous agreement or transaction between the originator and the approved party
   (e) Any other relevant factor.

Article (24)

The signatory, when using a signature originating tool, to have a signature of legal effect shall:-

(a) Exercise reasonable care to avoid unauthorized use of his signature originating tool.
(b) Without undue delay, use all means made available to him by the certification service provider or use reasonable efforts to notify any person expected to rely

on or provide services with reference to the electronic signature in the following cases:

1- Where the signatory knows that the signature originating tool was misused.
2- Where the circumstances known to the signatory will give rise to great doubts that the signature originating tool will be misused.

(c) Exercise reasonable care when using a certificate for confirming an electronic signature to ensure the accuracy and completeness of all material data made by the signatory which so related to the certificate throughout its effectiveness period or those data supposed to be included in certificate.

Chapter Five
Competent Authority

Article (25)

The competent Authority shall undertake the following functions:

(a) Issuing licenses for affording authentication services according to the provisions and conditions provided for in this law and its executive regulations and decisions.
(b) Determining the licenses fees.
(c) Importing or giving licenses for importing ciphering tools necessary for authentication services or that used by the Government units except the security authorities.
(d) Exercising control, supervision and inspection over the activities of the authentication service providers to ensure that they use hardwares, softwares and secured procedures against intervention and misusing and that they are committed to the approved performance standards to ensure confidentiality and security of electronic signatures and certificates.
(e) Specifying the standards of the authentication service providers.
(f) Specifying the qualifications and experiences that should be possessed by the authentication service providers.
(g) Stipulating the conditions that the authentication service providers are subjected to.
(h) Facilitating the institution of any electronic systems by the authentication service provider individually or with other providers

Article (26)

The competent authority may apply procedure deems to be appropriate for controlling and supervising the extent of compliance by the authentication services providers with the provisions of this law and the authority may access any computer system or hardware or data or any material connected to that system with the purpose of inspection and control. It may issue orders to any concerned person to afford reasonable technical assistance and other kind of assistance as it may thinks necessary and that person shall obligate himself to execute such an order.

Article (27)

The Minister may ask the Minister of Justice to confer quasi-Judicial power on the employees of the Competent Authority in accordance with the provisions of the Law of Criminal Procedure.

Article (28)

1- The application for the license of providing authentication services shall be submitted to the competent authority on the form prepared for this purpose.
2- It is not permitted to issue the license of providing authentication service unless the applicant fulfills the conditions specified by the competent authority and has been approved by a Ministerial Decision.
3- The license shall be personal and non-transferable and valid for five renewable years.

Article (29)

The competent authority shall have the right to revoke the license after conducting the required investigation with the authentication service provider in the following cases:

(a) If he submits false statement when applying for issuing or renewing the license.
(b) If he does not abide by the conditions and instructions specified for granting license.
(c) If he violates any of the obligations provided for in Article (34) of this law or the executive regulations and decisions.

The authentication service provider whose license has been revoked shall give it back to the competent authority immediately after the issuance of the revocation decision.

Article (30)

The competent authority may, if it has reasonable ground for revoking the license, issue an order suspending its validity till the completion of the investigation ordered by it provided that the period of suspension shall not exceed ten (10) days.

Where necessity so demands, the suspension period may be renewed for not more than ten days provided that the authentication service provider has been notified before renewal in order to introduce his reasons for not renewing and the authentication service provider should not issue any certificates during the period of suspension.

Article (31)

1- When suspending or revoking a license of an authentication service provider, the competent authority shall publicize this in its maintained database.
2- The abovementioned database containing the suspension or revocation shall be 24 hours accessible through the web.
3- The competent authority may publicize the contents of the database through another electronic means as appropriate and if necessary.

Article (32)

The concerned persons may appeal the decisions of refusal or suspension or revocation of the license to the Minister and he shall have the right to revoke or amend the decision so appealed if there are reasons for such revocation or amendment and the executive regulations shall determine the dates and procedures of submitting the appeal and its settlement.

Chapter Six
Provisions Related to Certificates and Authentication Services

Article (33)

The certificate shall explain the following:

(a) The identity of the authentication service provider
(b) That the signatory in the meantime is controlling the signature originating tools mentioned in the certificate.
(c) The signature originating tool was valid and true at the date of issuing the certificate.
(d) Any restriction on the scope or extent and value within which the certificate may be used.
(e) Any restrictions on the scope or the extent of the responsibility that the authentication service provider shall accept toward any person.
(f) Any other informations to be determined by the competent authority.

Article (34)

The authentication service provider shall have obtained the license from the competent authority and shall be obliged to:

(a) Act in accordance with the data provided by him in respect of his practices.
(b) Verify the accuracy and completeness of all material data contained in the certificate throughout the duration of its validity.
(c) Provide reasonably accessible means that enable the party who relies on his services to ascertain of:
    (1) The identity of the authentication service provider.
    (2) That the identified person in the certificate has control in the meantime over the signature originating tool mentioned in the certificate.
    (3) The method used in identifying the signatory
    (4) The existence of any restrictions on the purpose or value that the signature originating tool will be used for.
    (5) The validity of the signature originating tool and that it has not been subject to suspicions.
    (6) The appropriate mean for notifying revocation.
(d) Provide a mean for the signatory to enable him in giving notice in case the signature originating tool is misused and should ensure the availability of a service for revocation of the signature to be used in the appropriate time.
(e) Using trustworthy systems, procedures and human resources in the performance of his services while taking into consideration the following factors:
    (1) The financial and human resources.
    (2) Trustworthy hardware and software.
    (3) The procedure for obtaining certificates and applications for such certificates and retention of records.
    (4) Providing informations related to signatories identified in the certificates and render informations to parties who probably rely on the authentication services.

Article (35)

(1) If damage occurs due to inaccuracy of the certificate or because it is defective due to error or negligence committed by the authentication service provider, then he will be held responsible for that damage ensued whether to the party who contracted with him to give him the certificate or any person who reasonably relies on the certificate.
(2) The authentication service provider shall not be responsible for any damage if he proves that he didn't commit any mistake or negligence or that the damage ensued for a reason out of his control.

Article (36)

The authentication service provider shall:

1- Immediately suspend the operation of the certificate upon its owner's request if it appears to him or genuinely believe that:
   (a) The certificate was provided upon false or forged informations.
   (b) The signature originating tools was counterfeited
   (c) The certificate was used for fraudulent purposes.
   (d) The informations included in the certificate were changed.
2- Immediately notify the owner of the certificate on suspension of the certificate and the reasons therefor.
3- Immediately stop the suspension if the owner of the certificate retracted his request for suspension or on prove of the validity of informations included in the certificate and the validity of its usage.
4- The owner of the certificate or any other interested third party shall have the right to object to the suspension decision issued by the authentication service provider.

Article (37)

The authentication service provider shall revoke the certificate immediately in the following cases:

(a) If the owner of the certificate so requests.
(b) If he knows the death of the owner or the dissolution or liquidation of the juristic person who possess the certificate.
(c) If he ensures, after thorough examination, of the accuracy of the reasons on which he relies on suspending the certificate.

Article (38)

The authentication service provider shall be responsible for the damage ensued as a result of his failure to take an action to suspend or revoke the certificate in accordance with Article (36) and (37) of this Law.

Article (39)

The authentication service provider shall undertake the responsibility of depositing all public keys authorized in accordance with this law and shall keep a database in a computer containing all public keys in a way to render such a database and the public key available to the public.

Article (40)

No person is permitted to publicize a certificate referring to an authentication service provider whose name is appearing on the certificate if that person knows that:

1) The authentication service provider appeared in the certificate has not issued it.
2) The Signatory whose name appeared in the certificate has refused it.
3) The certificate has been suspended or revoked.

However, publication may be allowed for the purpose of ascertaining that the electronic signature is effected before suspension or revocation.

Article (41)

1- The authentication service provider who desires to stop his activity shall notify the competent authority (3) three months prior to stoppage.

2- The authentication service provider may transfer part of his activity to another authentication service provider provided that:
   (a) He notifies the owners of the valid certificates of his intention to transfer the certificates to another provider at least one month prior to the expected date of transfer.
   (b) He notifies the owners of the certificates of their rights in refusing such transfer and the deadline for refusal and the method thereof. The certificates whose owners expressed their refusal shall be revoked in writing or electronically on the stated deadline.
3- In case of the death or bankruptcy or dissolution of the authentication service provider, his heirs or liquidators shall be subjected to sub-article (2) of this article provided that the whole activity shall be transferred within three months.
4- In all cases of stopping the activity, the personal informations that remain under the control of the authentication service provider shall be destroyed in the presence of the competent authority representative.

Article (42)

1- In determining the accuracy and validity of the certificate or electronic signature no regard should be had to the place where the certificate is issued or the electronic signature is effected or the jurisdiction within which the place of business of the certificate issuer is located or the electronic signature is effected.
2- The certificates issued by foreign authentication service providers shall be the same as those issued by authentication service providers who act pursuant to this law if the practices of the foreign authentication service provider has got that level of credibility not less than the level required from the authentication service providers who have been subjected to the provisions of this law taking into consideration the recognized international practices.
3- The certificates issued by foreign authentication service provider shall not be recognized unless by a ministerial decision.
4- To decide the validity of a certificate or electronic signature, any agreement between the parties in respect of the transaction in which that signature is used or the certificate is issued, or in respect of the obligation of a specific authentication service provider or specific group of authentication service providers to use a specific type of certificates in relation to electronic messages or signatures introduced to them, shall be considered, provided that such agreement shall not be contrary to the laws of the Sultanate of Oman.

Chapter Seven
Protection of Private Data

Article (43)

Any government body or authentication service provider may collect personal data directly from the concerned person or from others after his explicit approval, only for the purpose of issuing a certificate or keeping it or facilitating such issuing or keeping. It is not permitted to collect or process or use such data for any other purpose without the explicit consent of the person from whom such data is collected.

As an exception from the above paragraph, the collection or disclosing or providing or processing of personal data shall be legal in the following cases:-

(a) If these data are necessary to prevent or discover a crime on official request from the investigation authorities.
(b) If these data are required or authorized by any law or by a court decision.
(c) If these data are necessary for the estimation or collection of any taxes or fees.
(d) If the processing is necessary for the protection of the person from whom data is collected.

Article (44)
Subject to the second paragraph of the above article, the authentication service provider shall follow the appropriate procedure to ensure confidentiality of the personal data in his possession in the course of his business and he shall not be allowed to disclose or transfer or declare or publicize these data for any purpose.

Article (45)
Any person who controls any personal data by virtue of his job in electronic transactions shall, before processing such data, notify the person from whom it is collected by a designated notice of the procedure he is following to protect those data. These procedures shall include an identification of the person responsible for processing the data, the nature of the data, and the purpose, methods and locations of processing and all informations necessary to ensure secured data processing.

Article (46)
The authentication service provider shall, upon the request of the person from whom data is collected, enable that person to have access to or update those personal data. Such right shall include the right of accessing all personal databases related to the person from whom it is collected, and shall make available to him all the appropriate technical means for this purpose.

Article (47)
The users of the personal data collected pursuant to Article (43) of this law, shall not be allowed to send electronic documents to the person from whom such data is collected if he explicitly refuses to accept them.

Article (48)
Any person controlling personal data is not allowed to process these data if the processing will cause damage to persons from whom such data is collected or will prejudice their rights and freedoms.

Article (49)
When the personal data are supposed to be transferred outside Oman, regard shall be had to the security of such information, in particular:
(a) Nature of personal data.
(b) Source of information and data.
(c) Purpose for which the data are to be processed and duration of process.
(d) The country of destination where the data were transferred, its international obligation, and the law applicable.
(e) Any related rules applied in that country.
(f) The security measures taken to secure that data in that country.

Chapter Eight

Government Use of Electronic Records and Signatures

Article (50)

The government may use electronic records and signatures to carry out the following tasks:

(a) Accept depositing or presenting or originating or maintaining documents.
(b) Issue any permission or license or decision or approval.
(c) Accept fees or any payments.
(d) Issue tenders and receive bids related to government purchases.

Article (51)

The government may, if so decided to carry out any of the abovementioned tasks electronically, determine:

(a) The form and method by which the records are to be originated or deposited or maintained or presented or issued.
(b) The form, method, shape and procedure of tendering and receiving bids and procurement of government purchases.
(c) The type of electronic signature required including the condition that the originator shall use another protected electronic signature.
(d) The form and method by which the electronic signature is to be fixed on the record and the standard to be met by the authentication service provider to whom the records are presented for depositing and maintaining.
(e) The appropriate operations and procedures of control required to ensuring safety, security and confidentiality of electronic records, payment of fees.
(f) Any other specifications or conditions or other provisions for sending paper based documents if so is required in relation to the electronic records of payment and fees.

Chapter Nine
Penalties

Article (52)

Without prejudice to any hard penalty provided for by the Omani Penal Law or any other Law, a person shall be punished by imprisonment for a period not exceeding two years and a fine not exceeding RO 5000 (Five thousands Omani Riyals) or both, if he:

1- Causes intentionally unauthorized amendment in the contents of any computer with the intention of weakening its efficacy or preventing or hindering access to any program or data maintained therein or weakening the efficacy of that program or diminishing the reliability of those data if the so called amendment takes place in any of the following ways:
   (a) Deleting any program or data maintained in the computer.
   (b) Adding any program or data to the contents of the computer.
   (c) Any act contributing in effecting that amendment.

2- Penetrates a computer or a series of computers or a web site or an internet site which resulted in:
   (a) Breaking down the operating systems of the computer or the series of computers.

(b) Damaging the computer programs or the computers and the informations contained therein.
(c) Stealing informations.
(d) Using the informations contained in the computers for illegal purpose.
(e) Entering incorrect informations.

3- Fraudulently breaks through the information system or the database with the purpose of misusing the electronic signatures.
4- Illegally discloses the deciphering keys or to deciphering informations deposited with him.
5- Illegally uses personal deciphering components related to signatures of other persons.
6- Penetrates or intercepts encrypted information or data, or intentionally deciphers them without a legal justification. The penalty shall be doubled if the information or data are related to the state confidentiality.
7- Intentionally unlock encrypted information or data by any means in legally unauthorized situations.
8- Intentionally creates or publicizes a certificate or provides incorrect electronic information for illegal purposes.
9- Presents incorrect data about his identity, or he mandates the authentication service provider so as to issue, cancel, or suspend a certificate.
10- Intentionally, without authorization, discloses confidential data that he is able to access using his authorities stipulated by this or any other law.
11- Exercises the activity of authentication service provider without being licensed.
12- Illegally uses a signature originating tool related to another person's signature.
13- Illegally accesses a computer so as to commit or make it easy for committing a crime by himself or by another person.
14- Counterfeits an electronic record or a signature or used it though he knows it is counterfeited.
15- Intentionally and illegally publicizes, makes it easy to publicize, or uses an electronic record or signature, or decipher it. The penalty shall be doubled if the perpetrator is a custodian to that record or signature by virtue of his profession or employment.

Article (53)
Without prejudice to any hard punishment provided for by the Omani Penal Law, or any other Law a person shall be punished with imprisonment for a period not exceeding one year and with a fine not exceeding RO 1500 (one thousand and five hundred Oman Riyals) or with one of the two punishments:

1. Any person who makes or possesses or obtains informations system or program for originating an electronic signature without the explicit consent of the owner of the signature.
2. Any owner of a ciphering key who refuses to hand it over to the employee specified by the competent authority after disclosing his identity.
3. Any authentication service provider or any one of his staff who refuses to provide assistance to the competent authority or to any of its employees in controlling or supervising or inspecting a computer system or data system or any other materials related to the computer at the office of the authentication service provider.

Article (54)
In case of conviction under this law, the court shall decree, in addition to any punishment, the confiscation of tools used in the commission of the crime.