Sultanate Decree
No. 2008/69
For the issuance of the Electronic Transactions Law

We Qaboos bin Said, the Sultan of Oman

After having reviewed the Basic Statute of the State issued under the Sultanate Decree No. 96/101.
And the Omani Penal Law issued under the Sultanate Decree No. 74/7.
And Penal Procedures Law issued under the Sultanate Decree No. 99/97.
And Banking Law issued under the Sultanate Decree No. 2000/114.
And Telecommunication Regulatory Law issued under the Sultanate Decree No. 2002/30.
And the Money Laundering Law issued under the Sultanate Decree No. 2002/34.
And the Executive Regulation of the Money Laundering Law issued under the Sultanate Decree No. 2004/72.
And the Sultanate Decree No. 2006/52 to establish the Information Technology Authority,
And as required by the public interest:

We Resolved the Following:

Article (One)

The attached Electronic Transactions Law shall be applied.

Article (Two)

The Minister of National Economy shall issue the Regulations and Decisions necessary to implement the Provisions of this Law.

Article (Three)

Anything contrary to this Law shall be null and void.

Article (Four):

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

Qaboos bin Said
Sultan of Oman

Issued on: Jumada Al-Awal 11, 1429 H
Corresponding to: May 17th, 2008 G

Electronic Transactions Law

Chapter One

Definitions and General Provisions

Article (1)

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

Government:
It is the units of the State Administrative Apparatus and the like.

Minister:
The Minister of National Economy.

Competent Authority:
The Information Technology Authority.

Electronic Transaction:
Any act or contract partially or wholly concluded and executed by way of electronic messages.

Electronic:
Any method related to the modern technology of electric, digital, magnetic, wireless, optical, electromagnetic, photic or any other similar capabilities.

Electronic Message:
Electronic information sent by electronic means whatever the means of extraction at the place where it received is.

Electronic Correspondence:
Sending or receiving electronic messages.

Electronic Record:
The contract or record or message of information generated, stored, extracted, copied, sent, informed or received by electronic means via a tangible intermediary or any other intermediary, provided to be deliverable and understandable.

Electronic Information:
Information or data electronically exchanged in a form of texts, symbols, sounds, images, photos, maps, computer programs or any other databases.

Exchange of the Electronic Data:
To transfer information from a person to another using an agreed standard to form the information.

Automated Electronic Intermediary:
An electronic program or system for a computer or any other electronic means used to implement any procedure or response to any procedure with the purpose of creating, sending or receiving an information message without intervention of any natural person.

Computer Programs:
A set of electronic information or instructions which are used directly or indirectly in an electronic information processing system for the purpose of obtaining specific results.

Network Intermediary:
A natural or legal person who, on behalf of another person who sends, receives, approves or stores an electronic transaction or renders services relating to such transaction.

Information Processing System:
An electronic system for the purpose of the automatic treating and processing of data and information for the purpose of originating or sending or receiving or storing or presenting or programming or analyzing such data and information.

Originator:
Any person who sends an electronic message, or to be sent on his behalf, pursuant to a valid authorization.

Addressee:
A natural or legal person whom the originator of the electronic message intends to direct his message to.

Signatory:
The person who has been granted from the competent authority the right of the electronic signature and who signs on behalf of himself or on behalf of his appointee to legally represents him.

Signature Originating Tool:
A tool that is used to create an electronic signature such as a software electronic device.

Electronic Signature:
Signing an electronic message or transaction in the form of letters, digits, symbols, signs or otherwise, and having a unique and capable way of determining the character that allows the identification of the signatory.

Procedures of Authentication:
The procedures aimed at verifying that an electronic message was issued by a particular person, and disclosing any error or amendment in the contents, sending, storing an electronic message or electronic record within a specific period of time. Including any action that uses mathematical equations, symbols, words and defining numbers, ciphering, procedures for reply or acknowledgment of receipt or any other means of protection of similar parameters.

Provider of Certification Services:
Any approved or licensed person/ body authorized to issue electronic authentication certificates or any other services related to them and the electronic signatures.

Certificate:
An electronic certification certificate issued by the certification service provider stating the link between the signatory and the data of the electronic signature.

Approved Party:
A person acting based on a certificate or electronic signature.

Processing of Personal Data:
Any process or set of processes which is performed on the personal data via automatic means or otherwise, collecting, recording, organizing, storing, modifying, retrieving, reviewing or disclosing it through sending, distributing, making it available by other means, coordinating or combining each other, concealing, deleting or cancelling it.

Encryption:
It is the process of changing a simple text or electronic message into unknown or scattered symbols that are impossible to be read or known without returning them to the original form.

Article (2)

This Law aims to:

1. Facilitate electronic transactions by using reliable electronic messages or records.
2. Remove any obstacles or challenges that face the electronic transactions resulting from

ambiguity relating to the requirements of writing and signature, and enhancing the development of the basic legal structure for the performance of the electronic transactions in a secure manner.

3. Facilitate the transfer of the electronic documents and the subsequent amendments.
4. Reduce cases of fraudulent electronic correspondence, subsequent amendments and opportunities of committing fraud on electronic transactions.
5. Establish unified principles for the rules, regulations and standards relating to authentication and integrity of electronic correspondence and records.
6. Enhance the public trust in the integrity and validity of the electronic transactions, correspondence and records.
7. Develop the electronic transactions at the National, Gulf and Arab levels through the use of the electronic signature.

Chapter (3)

The provisions of this Law shall apply to the electronic transactions, records, signatures as well as any electronic information message.

This Law shall not apply to:

a. Transactions and matters relating to the Personal Status Law such as marriage, divorce, wills and grants.
b. Court proceedings, judicial declarations, proclamations, summons, inspection orders, arrest warrants and judicial judgements.
c. Any document required by Law to be authenticated by the Notary Public.

Article (4)

1. The provisions of this Law shall apply to the transactions conducted among the parties who have agreed to conduct their transactions by electronic means, and the consent of each person to that effect may be inferred from his conduct. As for the government, its consent to electronic dealing must be expressly given.
2. The parties involved in establishing, sending, receiving, storing or processing electronic records may agree to deal in a way different from any of the rules provided for in Chapter Second up to Fourth of this Law.
3. No agreement among the parties to conduct a particular transaction by electronic means shall commit any of them to conduct other transactions by the same means.

Article (5)

The competent authority shall establish, operate and develop the electronic payment gateway, and determine its operating system in coordination with the Central Bank of Oman.

Article (6)

Both the network intermediary and the certification service provider shall provide on their own expense all technical elements such as equipment, devices, systems and programs that allow the security authorities to access their systems in order to meet the national security requirements, provided that the provisions of such service shall coincide with the provision of the technical elements according to the latest techniques, the Ministry of Finance shall provide all requirements needed for connecting all hardware sets used by these security authorities to achieve the objectives of National Security with those hardware sets used by the intermediary and the certification service provider as decided by the National Security Council. Both the network intermediary and the certification service provider shall bear all costs of certification service in case of changing their systems, and the costs of updating and connections to hardware sets used by these authorities if affected by the changes in their systems in

accordance with the decisions issued by the competent authority and the applied Laws.

Chapter Two
Legal Consequences Resulting from Electronic Messages and the Requirements of the Electronic Transactions

Article (7)

The electronic message shall have its legal effect and shall be deemed valid and enforceable like the written document, in case of considering the conditions provided for in this Law and the executive regulations upon its establishment and adoption.

Article (8)

1. Should any law require the retention of any document, record, information or data for any reason, then such retention shall be achieved by retaining such document, record, information or data in an electronic form if the following conditions are observed:
    a. The retention of the document, record, information or data electronically in the form they were originally created, sent or received, or in a form that can prove proving accurately that the document, record, information or data created, sent or received in its original form.
    b. The continued retention of the document, record, information or data in a way make available, usable and retrievable for subsequent reference.
    c. The document, record, information or data is retained in a way which enables the identification of their origin, destination, the date and time of its transmission or receipt.
2. Nothing in this Article shall affect the following:
    a. Any other law expressly provides for the retention of a document, record, information or data in an electronical form according to any particular electronic system or by following particular procedures or their retention or sending them through a particular electronic intermediary.
    b. Any additional requirements determined by the government for the retention of the electronic records subject to its competences.

Article (9)

If the law requires the writing of any document, record, transaction, information, statement or arrangement of particular results if it is not done, then the receipt of any of the above in an electronic form shall satisfy the requirement of writing if the conditions provided for in the preceding Article are observed.

Article (10)

If the Law requires that a message, record or document shall be provided in its original form and provides for certain results in case of noncompliance, then the electronic message, electronic record or electronic document will be deemed as original if a means is used to allow the 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.

Article (11)

1. When applying the rules of evidence in any legal proceedings, nothing shall apply to prevent the admissibility of the electronic message due to the fact that it is not in its original form if the message is the best evidence that the person submitting it could reasonably be expected to obtain.
    Such a message shall have evidential weight, considering the following:
    a. The extent of reliability of the manner in which the message was conducted,

entered, generated, processed, stored, submitted or sent.

b. The extent of reliability of the manner in which the safety of the information was maintained.
c. The extent of reliability of the source of information if it is known.
d. The extent of reliability of the manner in which its originator was identified, if relevant.
e. Any other relevant factor.

2. Unless the contrary is proved, the electronic signature shall be considered protected if the conditions stipulated in Article (22) of this Law are satisfied and signing or authenticating the electronic message on which it was placed or related is intended, and it has not been changed since its establishment, and that the signature is reliable.

Chapter Three
Electronic Transactions and Contract Conclusion

Article (12)

1. For the purposes of contracting, the offer and acceptance may be expressed through the electronic messages, and such expression shall be binding on all parties if given in accordance with the provisions of this Law.
2. The validity or enforceability of the contract shall not be denied because it was concluded by one or more electronic messages.

Article (13)

1. Contracting may be made between automated electronic media containing an electronic information system or more that was already prepared and programmed for doing such duties, and the contracting shall be valid and enforceable regardless the absence of any natural person in the process of concluding the contract directly or indirectly.
2. A contract may be concluded between an automated information system owned by a natural or legal person and another natural or legal person if the latter knows or should have known that the contract will be concluded using such a system.

   The electronic contracts shall have the same legal effects of the contracts concluded in the normal manners in terms of their validity, evidential value or enforceability in addition to any other provisions.

Article (14)

The responsibility of the Network Intermediary:

1. The network intermediary shall not be responsible civilly or criminally for any information included in a form of electronic records related to a third party, if the network intermediary is not the originator of such information and its role was only limited to providing access to such information, if that responsibility is based on:
   a. Creating, publishing or disseminating or distributing such information or any data contained therein.
   b. Trespassing on any personal rights related to such information.
2. The following is required to absolve the network intermediary from responsibility based on the provisions of this Article:
   a. He does not know about the facts or circumstances which in the ordinary course of matters, may create criminal or civil liability.
   b. In case of knowledge of the above, he removed immediately all information from any information system that is fallen under its control and stopped access to or offering such information.

3. The provisions of this Article do not impose any legal obligation on the network intermediary in respect of monitoring any information received in the form of electronic records relating to third parties if its role is limited only to providing access to such records.
4. The provisions of this Article do not prejudice 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 court judgment related to restricting, preventing or removing any information in the form of electronic records or preventing access to it.
5. In the application of this Article, provision of access to any information of third parties means, the availability of the technical means that enable access to information in the form of electronic records relating a third party or disseminate or only increase effectiveness of dissemination. This includes automatic provisional or temporary saving of information with the purpose of accessing it. In the application of this Article, the third party means any person upon whom the network intermediary has no actual control.

Article (15)

1. The electronic message shall be deemed issued by the originator in the following cases:
    a. If the originator is the person who issued it himself.
    b. As between the originator and the addressee, the electronic message shall be deemed issued by the originator if it was sent:
        1. By the person who has the authority to act on behalf of the originator in respect of the electronic message.
        2. In accordance with an automated system programmed by or on behalf of the originator, to automatically operate.
2. The addressee may consider that the electronic message was issued by the originator and may act on that assumption in the following two cases:
    a. If the addressee has accurately applied a procedure previously agreed to by the originator verify that the electronic message was issued by the originator.
    b. If the electronic message as received by the addressee is resulted from the acts of a person whose relationship with the originator or any agent of the originator legally enabled that person to have access to a method used by the originator to identify that the electronic message belongs to it.

    This Article shall not apply as of:
    1. The time at which the addressee received a notice from the originator that the electronic message is not that of the originator and the addressee had a reasonable time to act accordingly.
    2. The time at which the addressee knew or ought to have known if it exercises reasonable care or used an agreed procedure that the electronic message was not from the originator.

    This Article shall not apply if it is not acceptable for the addressee to consider that the electronic message is of the originator or to act in accordance with this assumption.

    The addressee may consider each electronic message he receives as an independent message and to act on that assumption only, unless he knew or ought to have known if it exercises reasonable care or uses an agreed procedure that the electronic message was a

duplicate.

Article (16)

Should the originator have requested the addressee or agreed with it when or before sending an electronic message or through that electronic message, that the receiving of that electronic message shall be acknowledged, then the provisions of Article (15) of this Law apply subject to the following:

1. Should the originator have stated that the electronic message is conditional on receipt of acknowledgement, the electronic message is to be treated, with regard to the rights and obligations as between the originator and the addressee, as if it has not been sent until the originator receives the acknowledgement of receipt.
2. Should the originator have 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 if that such time is not agreed upon or specified, then the originator may give to the addressee a 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 if it had not been sent.
3. When the originator receives the addressee's acknowledgement of receipt, it is assumed, unless the contrary is proven, that the related electronic message was received by the addressee. But, that assumption does not imply that the content of the electronic message sent by the originator corresponds the content of the message received by the addressee.
4. If 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 disclosed by any communication from the addressee electronically or otherwise or any conduct of the addressee sufficient to confirm to the originator that the electronic message has been received.
5. If the acknowledgement received by the originator states that the related electronic message has satisfied the technical requirements, whether those agreed upon or stated in the applicable standards, it is assumed that those requirements have been met, unless the contrary is proven.

Article (17)

Unless otherwise agreed by the originator and the addressee:

a. The electronic message is deemed to be sent when it enters an information system beyond the control of the originator or the person who sent the electronic message on his behalf .
b. The time of receiving the electronic message shall be determined as follows:
    1. If the addressee designated an information system for the purpose of receiving an electronic message, then receipt occurs at the time when the message enters the designated information system, and if the message is sent to an information system related to the addressee other than the designated one, the time of receipt will be the time when the message is retrieved by the addressee.
    2. If the addressee did not designate an information system, then receipt occurs when the message enters an information system related to the addressee.
c. The electronic message is deemed to be sent at the place where the originator has its place of work, and is deemed to be received at the place where the addressee has its place

of work even if the place where the information system is located is different from the place where the message is assumed to be received.

d. If the originator or the addressee has more than one place of business, it shall be the nearest place to the concerned transaction, or the headquarters, where there is no concerned transaction, the principal place of work, and if the originator or the addressee does not have a place of work, then it will be the habitual residence.

Chapter Four
Methods of Protection of Electronic Transactions

Article (18)

Ciphering is to be used as a means of protecting electronic transactions in order to maintain the confidentiality of the information or data of the message, and to verify the personality of the originator and to prevent third parties from capturing information or electronic messages so as not to reach the addressee or to distort it.

Article (19)

One of the following means is used for the protection of the information systems:

(a) Ciphering through Public key.
(b) Firewalls.
(c) Information Filters.
(d) Set of means related to prevention of denial.
(e) File and message ciphering technology.
(f) Protecting procedures for backup data.
(g) Anti-worms and anti-virus programs.
(h) Any other method approved by the competent authority.

Article (20)

Except for ciphering keys determined by the National Security Council, the employee designated by the competent authority may request from any holder of ciphering key to enable him to examine the necessary information related to that key and the holder of the key shall handover the key to that employee.

Article (21)

1. If specific authentication procedures were applied as agreed upon between the parties on electronic record to verify that it has not been changed since a certain time, then this record shall be treated as a protected electronic record since that time up to the time of verification.
2. If there is no agreement between the parties, the authentication procedures shall be deemed acceptable according to clause (1) of this Article and Article (22) of this Law taking into account the circumstances relating to the parties, particularly:
    a. The nature of the transaction.
    b. The knowledge and experience of the parties.
    c. The volume of similar transactions to which any or all of the parties are associated.
    d. The existence of alternative procedures.
    e. The cost of the alternative procedures.
    f. The procedures used in similar types of transactions in common.

Article (22)

The electronic signature shall be deemed protected and relied upon if the following are achieved:

a. The signature creation tool, in the course of its usage is exclusively limited to the signatory.
b. The signature creation tool, was at the time of signing under the control of the signatory only.
c. That any change to the electronic signature occurring after the time of signing is discoverable.
d. That any change in the information related to the signature occurring after the time of signing is discoverable.

However, any concerned party may prove in whatever manner that the electronic signature is reliable or not.

Article (23)

1. A person shall have the right to rely on the electronic signature or the certificate as long as such reliance is reasonable.
2. When an authorized party receives an electronic signature confirmed by a certificate, it is assumed that this party has verified the authenticity of the certificate and its enforceability and that he relies only on the certificate as issued according to its terms and conditions.
3. To determine 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 known.
   c. Whether the party relying on the electronic signature or the certificate has taken appropriate steps to determine the reliability of such electronic signature or the certificate.
   d. Any prior agreement or transaction made between the originator and the authorized party.
   e. Any other relevant factor.

Article (24)

1. The signatory shall, when using a signature creation tool, to create a signature of a legal effect observe the following:
   a. Exercise reasonable care to avoid unauthorized use of his signature creation tool.
   b. To use without undue delay, all means made available to him by the authentication service provider or use reasonable efforts to notify any person expected to rely on or provides services based on the electronic signature in the following cases:
      1. If the signatory knows that the signature creation tool was misused.
      2. If the circumstances known by the signatory give rise to great doubts that the signature creation tool will be misused.
   c. Exert reasonable care when using a certificate to confirm an electronic signature in order to ensure the accuracy and completeness of all material data provided by the signatory which relates closely to the certificate throughout the period of its effectiveness or such data supposed to be contained in the certificate.

Chapter Five
Competent Authority
Article (25)

The competent Authority shall be responsible for the following functions:

a. Issuing licenses for the practice of authentication services in accordance with the terms and conditions provided for in this Law and decisions executed thereof.
b. Determining the licensing fees.
c. Importing or issuing licenses for importing ciphering tools necessary for the purposes of authentication services or those used by the government bodies except the security authorities.
d. Controlling, supervising and inspecting the activities of the authentication service providers to ensure that they use hardware components, software and secured procedures against unauthorized intervention and misuse, and that they comply with the established standards of performance to ensure confidentiality and security of the electronic signatures and certificates.
e. Specify the levels of the authentication service providers.
f. Specify the qualifications and experience that should be obtained by the authentication service providers.
g. Determine the conditions that the authentication service providers are subjected to.
h. Facilitate the establishment of any electronic systems by an authentication service provider individually or together with other providers.

Article (26)

The competent authority may take the procedures it deems appropriate for controlling and supervising the compliance of the authentication services providers with the provisions of this Law, and the authority may access any computer system, hardware, data or any other material connected to that system for the purpose of conducting inspection and control. It may also issue orders to any competent person to provide reasonable technical assistance and other types of assistance as it deems necessary and that person shall be obligated to implement such orders.

Article (27)

The Minister may request the Minister of Justice to confer the power of judicial control 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 that purpose.
2. A license for providing authentication service may not be issued unless the applicant fulfills the conditions specified by the competent authority and has been approved by the Minister.
3. The license shall be personal, non-transferable and valid for five renewable years.

Article (29)

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

a. If he submits an incorrect statement upon applying for issuing or renewing the license.
b. If he does not comply with the conditions and controls specified for granting the license.
c. If he violates any of the obligations provided for in Article (34) of this Law or the executive regulations issued in implementation of its provisions.

The authentication service provider whose license is cancelled shall submit the license to the competent authority immediately upon the issuance of the cancelation decision.

Commented [u1]: The Service provider or the signatory?

Article (30)

The competent authority may, if it has acceptable grounds for canceling the license, issue an order to suspense its validity until the completion of the investigation ordered by it provided that the period of suspension shall not be more than ten (10) days. And in case of necessity, the period may be renewed for not more than another ten days provided that the authentication service provider to be notified before the renewal in order to submit the reasons he may have to prevent the same, and the authentication service provider shall not issue any certificates during the period of suspension.

Article (31)

1. Upon suspending or cancelling a license of an authentication service provider, the competent authority shall announce this in its maintained database.
2. The database that contain the suspension or cancelation shall be available for 24 hours on the web.
3. The competent authority may announce the contents of the database by another electronic means as appropriate and if necessary.

Article (32)

The concerned parties may appeal the decisions of refusal, suspension or cancelation of the license to the Minister and the Minister shall have the right to cancel or amend the decision appealed if there are justifications for that, and the executive regulation shall determine the dates and procedures for submitting the appeal and the decision thereof.

Chapter Six

Provisions Related to Certificates and Authentication Services

Article (33)

The certificate shall indicate the following:

a. The identity of the authentication service provider.
b. That the signatory at that time is controlling the signature creation tool mentioned in the certificate.
c. The signature creation tool was valid and true at the certificate issuing date.
d. Any restrictions on the scope or the value within which the certificate may be used.
e. Any restrictions on the scope or the extent of the liability that the authentication service provider shall accept against any person.
f. Any other data to be specified by the competent authority.

Article (34)

The authentication service provider shall have obtained the license from the competent authority and shall comply with the following:

a. Act in accordance with the data he provides in respect of his practices.
b. Verify the accuracy and completeness of all material data contained in the certificate during the period of its validity.
c. Provide accessible means that enable the party who relies on his services to ascertain the following:
    1. The identity of the authentication service provider.
    2. That the person identified in the certificate has control at that time over the signature creation tool referred to 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 creation tool will be used for.
5. The authenticity of the signature creation tool and that it has never been subject to suspicions.
6. The appropriate mean for reporting cancelation.

d. To provide a method for the signatory to enable him to give notice in case the signature creation tool is breached and shall ensure the availability of a service for cancelation of the signature that can be used in in a timely manner.

e. To use trustworthy systems, procedures and human resources in the performance of his services, taking into consideration the following factors:
   1. The financial and human resources.
   2. Reliable computer systems and software.
   3. The procedure for certificates and obtaining applications for such certificates and retention of records.
   4. Providing information related to signatories identified in the certificates and provide the information to parties who may rely on the authentication services.
   5. Regularity and the extent of accounting auditing conducted by and independent entity.

Article (35)

1. If damage occurs as a result of the invalidity of the certificate or because it is defective as a result of an error or negligence committed by the authentication service provider, then he will be held liable for that damage whether to the party who contracted with to give him the certificate or any person who reasonably relied on the certificate.
2. The authentication service provider shall not be liable for any damage if he proves that he has not committed any error or negligence or that the damage was caused for a reason beyond his control.

Article (36)

The authentication service provider shall:

1. Immediately suspend the operation of the certificate upon its holder's request if it was found that, or there was something to make him believe that:
   a. The certificate was delivered to him based on false or forged information.
   b. The signature creating tool was violated.
   c. The certificate has been used for fraudulent purposes.
   d. The information included in the certificate was changed.
2. Immediately notify the holder of the certificate when the certificate is suspended and the reasons of that procedure.
3. To immediately stop the suspension if the holder of the certificate retracted his request for suspension or upon proving the validity of the information contained in the certificate and the legality of its usage.
4. The holder of the certificate or any other interested third party may object to the suspension decision issued by the authentication service provider.

Article (37)

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

a. If the holder of the certificate so requested.
b. If he knows of the death of the holder or the dissolution or liquidation of the legal

person who holds 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 liable for the damage resulting from his failure to take an action to suspend or cancel the certificate in accordance with Article (36) and (37) of this Law.

Article (39)

The authentication service provider shall be responsible for the deposit of all public keys issued in accordance with this Law and shall retain a database in a computer containing all public keys in a way to make such a database and the public key available to the public.

Article (40)

No person is allowed to publicize a certificate indicating to an authentication service provider included in the certificate if that person knows that:

a. The authentication service provider indicated in the certificate has not issued it.
b. The signatory whose name is indicated in the certificate has not accepted it.
c. The certificate has been suspended or canceled.

Publication may be made for the purpose of ascertaining that an electronic signature is affected before suspension or cancelation.

Article (41)

1. The authentication service provider who desires to suspend his activity shall notify the competent authority three months at least before suspension.
2. The authentication service provider shall have the right to transfer a part of his activity to another authentication service provider provided that:
   a. To notify the holders of the valid certificates of his intention to transfer the certificates to another service provider one month at least before the expected date of transfer.
   b. To notify the holders of the certificates of their rights to refuse such transfer and the dates and methods of refusal. The certificates whose holders expressed their refusal shall be canceled in writing or electronically within the specified period.
3. In case of the death, bankruptcy, liquidation of the authentication service provider, his heirs or liquidators shall be subject to clause (2) of this Article provided that the whole activity shall be transferred within three months at most.
4. In all cases of suspension of the activity, the personal information that remain under the control of the authentication service provider must be destroyed in the presence of the representative of the competent authority.

Article (42)

1. For the purpose of determining the validity and effectiveness of the certificate or electronic signature, the place where the certificate or the electronic signature is issued shall not be considered, nor the department of the jurisdiction in which the issuer of the certificate or electronic signature is located.
2. The certificates issued by a foreign authentication service provider shall be the same as the certificates issued by authentication service providers who act under this Law if the practices of the foreign authentication service provider are of that level of credibility and not less than the level required from the authentication service providers who are subject to the provisions of this Law taking into consideration the recognized global practices.

3. The certificates issued by a foreign authentication service provider shall be recognized only by the Minister's decisions.
4. For the purpose of determining the effectiveness of a certificate or electronic signature, any agreement between the parties with respect to the transaction in which that signature or certificate is issued, or with respect to the obligation of a specific authentication service provider or group of authentication service providers to use a specific type of certificates with relation to electronic messages or signatures provided to them shall be considered, provided that such agreement is not in violation of the laws in force in the Sultanate.

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 obtaining the explicit consent of that person, this only for the purpose of issuing a certificate, maintaining it, facilitating such issuance or maintenance. Data may not be collected, processed or used for any other purpose without the explicit consent of the person from whom such data is collected.

To be excluded from the above paragraph, the collecting, disclosing, providing or processing of personal data shall be legal in the following cases:

a. If this data is necessary to prevent or detect a crime at an official request from the investigation authorities.
b. If this data is required or authorized by any law or by a decision of a court.
c. If this data is 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 preceding Article, the authentication service provider shall follow the appropriate procedure to ensure confidentiality of the personal data in his custody in the course of implementing his duties, and he shall not disclose, transfer, declare or publicize such data for any purpose without obtaining the prior written consent of the person about whom the data was collected.

Article (45)

Any person who controls any personal data by virtue of his job in electronic transactions must, before processing such data, inform the person from whom it was collected under a particular notice of the procedure followed by him to protect such data. These procedures must identify the person responsible for processing the data, nature of the data, and the purpose of its processing, methods and locations of processing in addition to all information necessary to ensure secured processing of data.

Article (46)

The authentication service provider, upon the request of the person from whom data is collected, must enable that person to have access to the personal data or update it. Such right includes the right of access to all personal databases related to the person from whom it was collected, and shall provide him with all the appropriate technical means that electronically enable him to do this.

Article (47)

The users of the personal data collected in accordance with Article (43) of this Law, shall not

send electronic documents to the person from whom such data was collected if he expressly refuses to accept them.

Article (48)

No person controlling personal data is allowed to process such data if the processing will cause damage to persons from whom such data was collected or will prejudice their rights and freedoms.

Article (49)

When personal data is determined to be transferred outside the Sultanate, adequate protection level of that data must be considered, in particular:

a. Nature of personal data.
b. Source of information included in the data.
c. Purpose for which the data is to be processed and its duration.
d. The country to which the data will be transferred, its international obligation, and the law applicable thereon.
e. The Related rules applied in that country.
f. The security measures taken to protect such data in that country.

Chapter Eight
Governmental Use of Electronic Records and Signatures

Article (50)

The government may carry out the following tasks with the usage of electronic records and signatures:

a. Accept filing, submitting, creating or retaining documents.
b. Issue any permission, license, decision or consent.
c. Accept fees or any payments.
d. Offer tenders and receive bids related to governmental purchases.

Article (51)

The government may, where deciding to carry out any of the duties mentioned in the preceding Article electronically, determine:

a. The method and form by which such records are created, filed, retained, submitted or issued.
b. The method, form, manner and procedures of offering tenders, receiving bids and carrying out government purchases.
c. The type of the required electronic signature including the condition that the sender must use another protected electronic signature.
d. The method and form by which the electronic signature is fixed on the record and the standard to be satisfied by the authentication service provider to whom the records are submitted for filing and retaining.
e. The appropriate processes and procedures of control required to ensure safety, security and confidentiality of electronic records, payment or fees.
f. Any other specifications, conditions or provisions for sending paper documents if the same is required in respect of the electronic records of payment and fees.

Chapter Nine
Penalties

Article (52)

Without prejudice to any tougher penalty provided for in 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 OR 5000 (Five thousand Omani Riyals) or one of these two penalties, if he:

1. Intentionally caused unauthorized amendment in the contents of any computer with the intention to weaken its effectiveness, prevent or hinder access to any program or data saved in it or to weaken the effectiveness of that program or to reduce the reliability of such data if such amendments were made in any of the following ways:
   a. Deleting any program or data saved in the computer.
   b. Adding any program or data to the contents of the computer.
   c. Any act contributing to that amendment.
2. Hacked a computer, a computer system, a website or an internet site and resulted in:
   a. Breaking down the operating systems of the computer or the computer systems.
   b. Destroying the computer programs or the computers as well as the information contained therein.
   c. Stealing of information.
   d. Using the information saved in the computers for illegal purpose.
   c. Entry of incorrect information.
3. Fraudulently hacked the information system or the database with the purpose of misusing the electronic signatures.
4. Disclosed illegally the deciphering keys or to deciphering information deposited with him.
5. Used illegally personal deciphering components of the signatures of other persons.
6. Hacked encrypted information or data, intentionally deciphered them without any legitimate justification, the penalty shall be doubled if the information or data is related to the secrets of the State.
7. Unlock intentionally encrypted information or data by any means in situation not legally authorized.
8. Creates intentionally or published a certificate or provided incorrect electronic information for illegal purposes.
9. Provided incorrect identification data about his identity or authorization to the authentication service provider in order to issue, cancel, or suspend a certificate.
10. Intentionally, without a legal permission, disclosed confidential data that he has access to using his powers under this Law or any other law.
11. Exercised the activity of authentication service provider without a license.
12. Uses illegally a signature creation tool of another person.
13. Accessed illegally to a computer in order to commit a crime or to facilitate committing a crime whether by himself or by another person.
14. Forged an electronic record, a signature or used it while he knows that it is forged.
15. Deliberately and illegally published, facilitated the publish, or uses an electronic record or signature, or decipher it, the penalty shall be doubled if the violator is the trustee of that record or signature under his profession or job.

Article (53)

Without prejudice to any tougher 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 OR 1500 (one thousand and five hundred Oman Riyals) or with one of these two penalties:

1. Anyone who made, possessed or obtained an information system or a program for creating an electronic signature without the express consent of the owner of the signature.
2. Any holder of a ciphering key who refused to deliver it to the employee specified by the competent authority after the disclosure of his identity.
3. Each authentication service provider or any of his employees has refused to provide facilities

to the competent authority or to any of its employees in monitoring, supervising or inspecting a computer system, data device or any other materials relating to the computer at the premises of the authentication service provider.

Article (54)

In case of conviction under this law, the court shall confiscate the tools used in committing the crime, in addition to any other penalty.