Electronic Transactions Law

Royal Decree No. (M/8)
8 *Rabi' I*- 1428H – 26 March 2007

Chapter One

General Provisions
Definitions

Article (1):

The following words and phrases, wherever mentioned in this Law, shall have the meanings assigned to them, unless the context requires otherwise:

1. **Ministry:** Ministry of Communications and Information Technology.
2. **Minister:** Minister of Communications and Information Technology.
3. **Commission:** Communications and Information Technology Commission.
4. **Governor:** Governor of the Communications and Information Technology Commission.
5. **Regulations:** Implementing Regulations of this Law.
6. **Center:** National Center for Digital Certification.
7. **Computer:** Any stationary or portable, wired or wireless, electronic device with a system for processing, storing, sending, receiving or browsing data, performing specific functions according to programs and given commands.
8. **Person:** Any natural or corporate person, whether public or private.
9. **Electronic:** Technology based on using electrical, electromagnetic, optical or similar capabilities.
10. **Electronic Transactions:** Any exchange, communication, contracting or other procedure, performed or executed, wholly or partially, by electronic means.

11. **Electronic Data:** Data with electronic features in the form of texts, codes, images, graphics, sounds or any other electronic form, either collective or separate.
12. **Electronic Data System**: One or more electronic devices or programs used to generate, retrieve, send, transmit, receive, store, display or process electronic data.
13. **Electronic Record:** Data generated, communicated, received, or stored by electronic means, and retrievable in perceivable form.
14. **Electronic Signature:** Electronic data included in, attached to or logically associated with an electronic transaction used to verify the identity and approval of the person signing it and to detect any change to said transaction after signature**.**
15. **Electronic Signature System:** An electronic data system specially designed to work independently or with another electronic data system, to generate electronic signature.
16. **Signatory:** A person making an electronic signature in an electronic transaction using an electronic signature system.
17. **Digital Certificate:** An electronic document issued by a certification service provider to verify the identity of the person having an electronic signature system, including signature verification data.
18. **Intermediary:** A person who receives an electronic transaction from an originator and delivers it to another person or performs other relevant services.
19. **Originator:** A person, other than an intermediary, initiating an electronic transaction.

20. **Addressee:** A person - other than an intermediary**-** to whom an electronic transaction is directed by an originator.
21. **Certification Service Provider:** A person licensed to issue digital certificates or perform any other service or task related thereto and to electronic signatures in accordance with this Law.

Objectives and Scope

Article (2):

This Law aims at controlling, regulating and providing a legal framework for electronic transactions and signatures so as to achieve the following:

1. Setting uniform legal standards for using electronic transactions and signatures and facilitating the implementation thereof in both private and public sectors by means of reliable electronic records.
2. Ensuring the credibility and integrity of electronic transactions, signatures and records.
3. Facilitating electronic transactions and signatures, domestically and internationally, in all sectors, including government procedures, commerce, medicine, education and electronic payments.
4. Removing obstacles facing use of electronic transactions and signatures.
5. Preventing misuse and fraud in electronic transactions and signatures.

Article (3):

This Law shall apply to electronic transactions and signatures, excluding the following:

1. Transactions pertaining to personal status law. Status.
2. Issuance of deeds of legal actions pertaining to real property.

Unless the authorities responsible for such transactions approve of making them electronically according to conditions set by said authorities in coordination with the Ministry.

Article (4):

1. Nothing in this Law shall compel any person to use electronic transactions without his implicit or explicit consent.
2. In exception to paragraph (1) of this Article, the consent of government agency to electronic transactions shall be explicit, taking into consideration the conditions set by the government agency for electronic transactions.
3. A person may set additional conditions for accepting electronic transactions and signatures, provided that such conditions do not conflict with the provisions of this Law.

Chapter Two

Legal Effects of Electronic Transactions, Records and Signatures

Article (5):

1. Electronic transactions, records and signatures shall have full effect and their validity and enforceability may not be contested, nor may the execution thereof be stayed on the ground that they were wholly or partially conducted by electronic means; provided that such electronic transactions, records or signatures are carried out in compliance with the conditions provided for in this Law.
2. Information resulting from electronic transactions shall remain in effect and enforceable as long as access to the details thereof is allowed within the electronic data system of the originator thereof and the manner of accessing them is indicated.

Article (6):

1. Without prejudice to Article (3) of this Law, if a law in the Kingdom requires for certain documents or information to be stored for any reason, such requirement shall be deemed satisfied provided that said documents or information is stored or sent in the form of an electronic record, subject to the following:
    a. Storing the electronic record in the form it was generated, sent, or received, or in such form that the contents thereof may be verified as being identical to the contents in which it was generated, sent or received.

b. Storing an electronic record in a manner allowing for future use and reference.
c. Storing information, together with electronic records, indicating the originator, addressee as well as the date and time of sending and receiving.

2. Any person may, at his own responsibility, assign another person to satisfy the requirements set forth in paragraph (1) of this Article.
3. The Regulations shall set forth the procedures for storing electronic records and data, and the conditions required to produce them in electronic format and the conditions and restrictions for accessing them.

Article (7):

Without prejudice to Article (3) of this Law, if a law in the Kingdom requires that documents, records or information provided to others be written, said requirement shall be deemed satisfied, provided that they were provided in an electronic form in accordance with the provisions of paragraph (1) of Article (6).

Article (8):

An electronic record shall be deemed an original in its own right when technical means and conditions are observed to ensure the integrity of information included therein from the time said record was created in its final form as an electronic record, and allow for required information to be provided upon request. The Regulations shall set forth such technical means and conditions.

Article (9):

1. Electronic transactions or signatures shall be admissible as evidence if their electronic records satisfy the requirements set forth in Article (8) of this Law.
2. Electronic transactions or signatures may be admissible as presumptive evidence even if their electronic records do not satisfy the requirements set forth in Article (8) of this Law.
3. Electronic transactions, signatures and records shall be deemed reliable evidence in transactions, and shall be deemed intact unless proven otherwise.
4. When assessing the reliability of an electronic transaction the following shall be considered:
    a. The method of creating, storing or communicating an electronic record and the possibility of tampering therewith.
    b. The method of maintaining the integrity of information.
    c. The method of identifying the originator.

Chapter Three
Concluding Electronic Transactions

Article (10):

1. Offer and acceptance of contracts may be expressed by electronic means, and such contracts shall be deemed valid and enforceable if concluded in accordance with the provisions of this Law.
2. The validity or enforceability of a contract shall not be denied if concluded through one or more electronic records.

Article (11):

1. Contracts may be concluded through automated electronic data systems or directly between two or more electronic data systems previously designed and programmed to carry out such tasks on behalf of the two contracting parties. Such contracts shall be deemed valid and legally effective, notwithstanding the absence of direct intervention of any natural person in conclusion thereof.
2. Contracts may be concluded between an automated electronic data system and a natural person, only if said person is aware, or presumed aware, that said contract is being concluded and executed by an automated system.

Article (12):

An originator shall be deemed to have issued an electronic record if the record was sent by the originator personally, another person acting on his behalf, or an automated system programmed by him to do so on his behalf. Intermediaries shall not be deemed originators. The Regulations shall specify procedures and provisions related thereto.

Article (13):

1. An electronic record shall be deemed sent upon entry to a data system that is not controlled by the originator. The Regulations shall set the technical standards for data systems and method of determining the time and place of sending or receiving a given electronic record.

2. Acknowledgement of receipt shall take any form specified in the Regulations, unless the originator and the addressee agree on a specific form.

Chapter Four
Electronic Signature

Article (14):

1. If a signature is required for any document or contract or the like, such requirement shall be deemed satisfied by an electronic signature generated in accordance with this Law. The electronic signature shall be equal to a hand-written signature, having the same legal effects.
2. Any person generating an electronic signature shall do so in accordance with the provisions of this Law and the conditions, requirements and specifications set by the Regulations, and shall take into consideration the following:
    a. Take necessary precautions to prevent unlawful use of signature generating data or the personal equipment related thereto. The Regulations shall specify such precautions.
    b. Notify the certification service provider of any unauthorized use of his signature in accordance with the procedures specified in the Regulations.
3. If an electronic signature is provided in any legal procedure, the following shall be deemed valid, unless proven otherwise or the concerned parties agree to the contrary:
    a. The electronic signature is the signature of the person identified in the relevant digital certificate.

b. The electronic signature was provided by the person identified in the relevant digital certificate for the purpose specified therein.
c. The electronic transaction has not been altered since the electronic signature was affixed thereto.

4. If an electronic signature does not satisfy the conditions and requirements set forth in this Law and the Regulations, the presumed validity established in paragraph (3) of this Article shall not apply to said signature nor to the electronic transaction associated therewith.
5. Any person relying on an electronic signature of another person shall exercise due diligence in verifying the authenticity of the signature, using relevant electronic signature verification data in accordance with the procedures set forth by the Regulations.

Chapter Five
Powers of the Ministry and the Commission

Article (15):

Overseeing the implementation of the provisions of this Law shall be in accordance with the following:

1. The Ministry shall set general policies and draw development plans and programs for electronic transactions and signatures, submit draft laws and amendments thereto, coordinate with government agencies and others with regards to the implementation of this Law, and represent the Kingdom in local, regional and international organizations as regards electronic transactions

and signatures. The Ministry may delegate the Commission or any other agency it deems fit to represent the Kingdom.

2. The Commission shall be in charge of implementation of this Law and shall, to this end that, have the power to do the following:
    a. Issue, renew, suspend and revoke licenses of the certification service provider. The Regulations shall provide for the necessary requirements and procedures for obtaining a license and its validity, renewal, suspension, revocation and assignment, as well as obligations of licensees, the conditions and procedures for suspending the activities thereof and legal effects thereof.
    b. Ensure compliance of the certification service providers with licenses issued to them, the provisions of this Law as well as the Regulations and decisions issued by the Commission.
    c. Take necessary measures– in accordance with the Regulations– to ensure the continuity of services to clients of the certification service provider upon suspension of the activities thereof or revocation or non-renewal of the license granted thereto.
    d. Propose draft laws and regulations relating to electronic transactions, and amendments thereof and submit the same to the Ministry to take necessary procedures.
    e. Determine the fees for providing licensing certification services, subject to the Minister's approval.

Chapter Six
National Center for Digital Certification

Article (16):

1. A national center for digital certification shall be established in the Ministry in accordance with this Law to oversee and manage tasks relating to issuance of digital certificates.
2. The Regulations shall set forth the rules for determining the center's location, formation, powers and tasks as well as the manner of carrying out its duties.

The Minister may assign the Commission, or any other agency, the power to carry out some or all of the center's duties.

Article (17):

The Center shall have the power to approve digital certificates issued by foreign parties outside the Kingdom. Said certificates shall be considered equal to those issued in the Kingdom, in accordance with the conditions and procedures specified in the Regulations.

Chapter Seven
Obligations and Responsibilities of Certification Service Providers

Article (18):

A certification service provider shall observe the following:

1. Obtain the necessary license from the Commission before commencing activities.

2. Issue, deliver and store digital certificates in accordance with the license issued therefor by the Commission and the procedures specified in the Regulations.
3. Use reliable means to issue, deliver and store certificates, and take necessary measures to protect said certificates from forgery, fraud and damage, in accordance with the Regulations and the license.
4. Create a database for certificates issued and store said data and any modifications thereon, including suspended and revoked certificates, and grant continuous electronic access to such data.
5. Maintain, along with his staff, the confidentiality of information obtained in the course of business, excluding information that certificate holders permit – in written or electronic form- to be published or disclosed, or as provided for by law.
6. Obtain applicant's personal information, directly or indirectly, with the applicant's written consent.
7. Issue certificates containing data specified in the Regulations in accordance with systems' security and protection requirements and the digital certification rules set by the Center.
8. Deliver, whenever his activities are ceased, all information and documentation in his possession to the Commission, to be disposed of in accordance with provisions and standards provided for in the Regulations.

Article (19):

A certification service provider may not ceased licensed activities, assign licenses issued to him or merge with

another entity without the prior written approval of the Commission, in accordance with the procedures specified in the Regulations.

Article (20):

A certification service provider shall warrant the accuracy of information provided in the certificate at the time of delivery, and the relevance of said electronic data to the certificate holder. A certification service provider shall also be liable for any damage incurred by any person relying, in good faith, on such information.

Article (21):

A certification service provider shall, upon the request of a certificate holder or as specified in the Regulations, revoke or suspend such a certificate, and immediately notify the certificate holder of such revocation or suspension and the reasons therefore. If such reasons no longer stand, he shall lift said revocation or suspension. A certification service provider shall be liable for any damage incurred by any in bona fide person due to failure to suspend or revoke the certificate.

Chapter Eight
Responsibilities of Certificate Holders

Article (22):

1. A certificate holder shall be responsible for the integrity and confidentiality of his own electronic signature system, and any use of such system shall be deemed originated by him. A certificate holder shall comply with the conditions of using his

certificate as well as conditions for creating his electronic signature.

2. A certificate holder shall provide accurate information to the certification service provider or any other party required to accept his electronic signature.
3. A certificate holder shall notify the certification service provider of any modification or declassification of information provided in the certificate.
4. A holder of a suspended or revoked certificate may not reuse elements of the electronic signature relating to said certificate with another certification service provider. The Regulations shall specify necessary procedures for preventing such incidents.

Chapter Nine
Offences and Penalties

Article (23):

The following acts shall be deemed in violation of the provisions of this Law:

1. Engaging in the activities of a certification service provider without a license from the Commission.
2. A certificate holder's use of information concerning the applicant, for purposes other than certification without the applicant's consent in a written or electronic form.
3. A certificate holder's disclosure of information accessed by virtue of his work without the certificate holder's consent in a written or electronic form, or as provided for by law.

4. A certification service provider's provision of false or misleading information to the Commission, or misuse of certification services.
5. Creating, publishing or using digital certificates or electronic signatures for fraudulent or any other unlawful purposes.
6. Forging electronic records, electronic signatures or digital certificates or using them with knowledge of forgery.
7. Willfully providing false information to a certification service provider, or false electronic signature information to any party relying on such signature under this Law.
8. Accessing, copying, restructuring or taking over another person's electronic signature system without valid authorization.
9. Steeling the identity of another person or falsely claiming to represent him in applying for, accepting or requesting the suspension or revocation of a digital certificate.
10. Publishing a forged, false, revoked or suspended digital certificate or knowingly placing such certificate at the disposal of another person, excluding the right of a certification service provider set forth in paragraph (4) of Article (18).

Article (24):

Without prejudice to any severer penalty provided for in any other law, anyone found guilty of any of the actions set forth in Article (23) of this Law shall be subject to a fine not exceeding five million riyals, imprisonment for a period not exceeding five years or both penalties. Equipment, systems and programs used in committing

the violation may be confiscated pursuant to a judgment.

Article (25):

The Commission, in cooperation and coordination with competent authorities, shall be in charge of recording and inspecting violations set forth in Article (23) of this Law and making a record thereof. The Commission may seize equipment, systems and programs used in committing the violation until such violation is decided. The Governor shall issue a decision naming employees for the task and setting procedures for recording and inspection.

Article (26):

The violation record set forth in Article (25) of this Law shall, upon the Commission's completion of its task, be referred to the Bureau of Investigation and Public Prosecution to undertake, in accordance with its law, the investigation and prosecution thereof before the competent judicial authority.

Article (27):

Any person incurring damage– due to violations set forth in this Law or failure to comply with any controls or obligations provided for therein - shall reserve the right to claim damages before the competent judicial authority.

Chapter Ten
Concluding Provisions

Article (28):

Application of this Law shall not prejudice provisions of relevant laws, particularly those related to intellectual property rights, and international agreements to which the Kingdom is party.

Article (29):

Staff of Ministry, Commission and Center shall maintain the confidentiality of information relating to certification service providers or clients thereof, obtained in the course of their work and may not disclose such information for any reason, except in cases provided for by law.

Article (30):

The Minister shall issue the Regulations of this Law, upon a recommendation by the Commission, within one hundred and twenty days from the issuance date of this Law.

Article (31):

This Law shall come into force one hundred and twenty days from the date of its publication in the Official Gazette.