Legislative Decree No. 54 of 2018
Promulgating the Electronic Communications and Transactions Law

We, Hamad Bin Isa Bin Salman Al-Khalifa, the King of the Kingdom of Bahrain,

- Having perused the constitution, particularly section 38 thereof;
- The Civil and Commercial Procedural Law promulgated by Legislative Decree No. 12 of 1971 (as amended);
- Legislative Decree No. 14 of 1971 in respect of Notarization, as amended by Legislative Decree No. 37 of 2017;
- The Penal Code promulgated by Legislative Decree No. 15 of 1976 (as amended);
- The Law of Commerce promulgated by Legislative Decree No. 7 of 1987 (as amended);
- The Law of Evidence in Civil and Commercial Matters promulgated by Legislative Decree No. 14 of 1996 (as amended);
- The Civil Code promulgated by Legislative Decree No. 19 of 2001, as amended by Law No. 27 of 2017;
- The Commercial Companies Law promulgated by Legislative Decree No. 21 of 2001 (as amended);
- Legislative Decree No. 28 of 2002 in respect of the Electronic Transactions Law (as amended);
- The Criminal Procedural Law promulgated by Legislative Decree No. 46 of 2002 (as amended);
- The Telecommunications Law promulgated by Legislative Decree No. 48 of 2002, as amended by Legislative Decree No. 38 of 2017;
- Law No. 46 of 2006 in respect of the Identity Card;
- The Central Bank and Financial Instructions Law promulgated by Law No. 64 of 2006 (as amended);
- Law No. 35 of 2012 in respect of the Consumer Protection;
- Law No. 16 of 2014 in respect of the Protection of Information and Documents of the State;
- Law No. 60 of 2014 in respect of the Information Technology Crimes;
- Law No. 2 of 2017 in respect of the Ratification of the Arab Treaty on Combating Information Technology Crimes; and
- The Personal Data Protection Law promulgated by Law No. 30 of 2018;
- Furthering to tabling by the Prime Minister; and
- Upon approval of the Council of Ministers;

We have decreed the following:

Article One

The accompanying law shall apply in respect of Electronic Communications and Transactions.

Article Two

1. The provisions of the Law of Evidence in Civil and Commercial Matters promulgated by Legislative Decree No. 14 of 1996 shall be applicable in respect of all matters that are not specifically provided for under this law.

2. Any electronic record, electronic signature created and electronic transaction, made in accordance with Legislative Decree No. 28 of 2002 with respect to the Electronic Transactions Law, shall remain valid after this law enters into force.
3. Until implementing regulations are issued pursuant to this law, regulations issued pursuant to Legislative Decree No. 28 of 2002 with respect to the Electronic Transactions Law shall remain applicable to the extent that they are not inconsistent with the provisions of this law.
4. All decisions made before this law enters into force, in respect of domain name registration shall, to the extent that these are not inconsistent with the provisions of this law, remain valid until the term of the respective registration expires.

Article Three

Legislative Decree No. 28 of 2002 with respect to the Electronic Transactions Law shall be repealed. Any provision in any law that is inconsistent with the provisions of this law shall also be repealed.

Article Four

The Prime Minister and the Ministers shall each – in his respective capacity - be charged with the implementation of this Law which shall come into force on the first day of the month that follows sixty (60) days after the date of its publication in the Official Gazette.

Issued in Rifa'a Palace:
Date: 20 Rabeea Al'Awal 1440H
Corresponding: 28 November 2018

The Electronic Communications and Transactions Law

1. Definitions

In this Law, the following terms and expressions shall have the corresponding meaning provided hereunder against each unless the context requires otherwise:
Competent administrative agency: the administrative agency designated in a decree;
Competent authority: the Minister or the head of the competent administrative agency;
Electronic record: information generated, communicated, received or stored by electronic means and includes, where appropriate, all information logically associated with or otherwise linked together so as to become part of the record, whether generated contemporaneously or not;
Electronic: using means which are electrical, magnetic, electromagnetic, optical, biometric, photonic or any other similar form of technology;
Electronic agent: a computer programme or any other electronic means used to initiate an

action or to respond to electronic records or actions, in whole or in part, without review or actions by a natural person at the time of the action or response;

Trust services: electronic services related to electronic signatures, electronic seals, electronic time stamps, electronic registered delivery and website authentication;

Trust service provider: a person who provides one or more trust services;

Accredited trust service provider: a trust service provider who is accredited under Section (20) or (21) of this law to provide one or more of the trust services;

Certificate service provider: a trust service provider that issues certificates;

Communication: any statement, declaration, acknowledgement, notice or request, including an offer and the acceptance of an offer made in the course of concluding a contract;

Electronic communication: any communication that a party makes by means of electronic records;

Electronic seal: data in electronic form, which is attached to or logically associated with an electronic record to ensure the latter's integrity and origin;

Secure electronic seal: an electronic seal that is:

1. Uniquely linked to the creator of the seal;
2. Capable of identifying the creator of the seal;
3. Created using electronic seal creation data that the creator of the seal can use, with a high level of confidence, under its control; and
4. Linked to the electronic record to which it relates in such a way that any subsequent change in the electronic record is detectable; and
5. Created by a secure electronic seal creation device, issued by a service provider who is accredited for that purpose, and that is based on a secure electronic seal.

Electronic seal creation data: unique data, which is used by the creator of the electronic seal to create an electronic seal;

Electronic seal creation device: configured software or hardware used to create an electronic seal;

Secure electronic seal creation device: an electronic seal creation device which meets the requirements set out in a regulation issued by the competent authority;

Certificate for electronic seal: an electronic attestation that links electronic seal validation data to a person and confirms the name of that person;

Secure certificate for electronic seal: a certificate for electronic seal, issued by a trust service provider accredited for such purpose, that meets the requirements set out in a regulation issued by the competent authority;

Electronic signature: data in electronic form in, attached to or logically associated with, an electronic record, which may be used to identify the signatory in relation to the electronic record and to indicate the signatory's intention in respect of the information contained in the

electronic record;

Secure electronic signature: an electronic signature that is:

1. Uniquely linked to the signatory;
2. Capable of identifying the signatory;
3. Created using electronic signature creation data that the signatory can use, with a high level of confidence, under its sole control;
4. Linked to the electronic record signed therewith in such a way that any subsequent change in the electronic record is detectable; and
5. Created by a secure electronic signature creation device, issued by a service provider who is accredited for that purpose, and that is based on a secure electronic signature.

Electronic signature creation data: unique data which is used by the signatory to create an electronic signature;

Electronic signature creation device: configured software or hardware used to create an electronic signature;

Secure electronic signature creation device: an electronic signature creation device which meets the requirements set out in a regulation issued by the competent authority;

Certificate for electronic signature: an electronic attestation which links electronic signature validation data to a natural person and confirms the name of that person;

Secure certificate for electronic signature: a certificate for electronic signature, issued by a trust service provider accredited for such purpose, which meets the requirements set out in a regulation issued by the competent authority;

Certificate: a certificate for electronic signature, electronic seal or website authentication;

Certificate for website authentication: an electronic attestation that authenticates a website and links that website to the person to whom the certificate is issued;

Secure certificate for website authentication: a certificate for website authentication, issued by a trust service provider accredited for such purpose, which meets the requirements set out in a regulation issued by the competent authority;

Personal identification data: a set of data enabling the establishment of the identity of a natural, or a natural person representing a private or public legal person or other public body;

Electronic identification: the process of using personal identification data in electronic form uniquely representing either a natural person, or a natural person representing a private or public legal person or other public body;

Electronic identification means: a material and/or immaterial unit containing personal identification data and which is used for authentication for an online service;

Electronic identification scheme: a system for electronic identification under which electronic identification means are issued to natural persons, or natural persons representing private or public legal persons or other public bodies;

Electronic registered delivery service: a service that provides evidence relating to the

handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, damage or any unauthorized alterations;
Secure electronic registered delivery service: an electronic registered delivery service, provided by a trust service provider accredited for this purpose, which meets the requirements set out in a regulation issued by the competent authority;
Electronic time stamp: data in electronic form which binds an electronic record to a particular time establishing evidence that the latter data existed at that time;
Secure electronic time stamp: an electronic time stamp which satisfies the requirements set out in a regulation issued by the competent authority;
Information: data, text, images, shapes, sounds, codes, computer programs, software, databases and similar matters;
Information system: an electronic system for generating, sending, receiving, storing, displaying or processing electronic records;
Originator: a person by whom, or on whose behalf, the electronic record has been generated or sent prior to storage, if any, but not a person acting as an intermediary with respect to that electronic record;
Addressee: a person who is intended by the originator to receive the electronic communication but does not include a person acting as an intermediary with respect to that electronic communication;
Intermediary: a person who, on behalf of another person, sends, receives, transmits or stores the electronic record or provides other services with respect to that electronic record;
Signatory: a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents by using such data to create an electronic signature;
Person: any natural persona, private or public legal person or other public body;
Record: information that is inscribed on a tangible medium or that is stored in an electronic, or any other medium and is retrievable in an intelligible form;
Validation: the process of verifying and confirming that an electronic signature or an electronic seal is valid;
Validation data: data that is used to validate an electronic signature or an electronic seal; and
Consumer: any natural person who is acting for purposes which do not fall within the scope of commerce;

2. Scope of Application

1. This law shall apply to all transactions and dispositions of all types. It shall also apply to negotiable instruments and negotiable documents in the form of electronic record to the extent and subject to provisions under laws specific to such instruments and documents.
2. This law does not override any rule prescribed pursuant to any law for the protection of consumers.

3. Acceptance of Non-Public Bodies of Electronic Transactions, Electronic Communications and Trust Services

1. Except where any law expressly provides otherwise, this law does not require any person without its express consent to engage in electronic transactions, send or receive electronic communication or use or accept any electronic trust service. Notwithstanding the foregoing, except for public bodies, consent may be inferred from the person's positive conduct.
2. This law does not prohibit any person who wishes to be engaged in electronic transaction from establishing reasonable requirements that would ensure its acceptance of engaging in electronic transaction, sending or receiving electronic communications or using or accepting any other trust service.

4. Acceptance of Public Bodies of Electronic Transactions, Electronic Communications and Trust Services

1. The consent of a public body to be engaged in electronic transactions, send or receive electronic communications or use or accept any electronic trust service shall be subject to regulations issued in this respect, by the competent minister or head of the relevant public body as the case may be. The regulation shall prescribe the extent and the scope of consent to sending and receiving electronic communications together with any administrative requirements to be observed.
2. Any consent issued in accordance with subsection (a) shall be subject to compliance with the technical requirements prescribed in a regulation issued by the Minister or head of the competent administrative agency for information technology networks and systems of the government entities.
3. The provisions of the preceding subsections do not derogate from the provisions of any law that expressly prohibit the use of electronic communications, or trust services, or requires them to be used in a particular manner. For the purpose of applying this sub-section, it shall not constitute a prohibition on the use of electronic communication or a trust service a provision in any other law merely requiring that the information or documents are evidenced in writing or to be signed.

5. Evidential Weight of Electronic Records

1. Electronic records shall have, in the context of civil and commercial transactions, the same evidential weight accorded to private documents, and shall have the same evidential weight accorded to public documents under the Law of Evidence in Civil and Commercial Matters where they meet the conditions prescribed therein, other conditions prescribed under this law and a regulation issued by the competent authority after coordinating with the competent Minister for justice affairs.
2. Information included in electronic records shall not be denied legal effect, validity or enforceability, solely on the grounds that it is wholly or partly in the form of an electronic record or referred to in such record.

3. Where the law requires information to be in writing, that requirement is met by an electronic record that contains the information provided that the information contained therein is accessible so as to be usable for subsequent reference.
4. In assessing the evidential weight of an electronic record, regard shall be had to the following:

1. The reliability of the manner in which the electronic record was generated, stored or communicated;
2. The reliability of the manner in which the electronic record was signed;
3. The reliability of the manner in which the integrity of the information was maintained; and
4. Any other factors relevant to the integrity of the electronic record.

6. Electronic Signatures

1. Where the law requires a party's signature, an electronic signature affixed to an electronic record meets the requirements of the law, if a method is used to identify that party and to indicate that party's intention in respect of the information contained in that record, and where that method used is either as reliable as appropriate for the purpose, for which the electronic record was generated or communicated, in light of the relevant circumstances; or proven in fact to have fulfilled the function described in this sub-section either by itself or together with further evidence.
2. The relevant circumstances referred to under subsection (a) may include:

1. Any operational rules relevant to the assessment of reliability of the system;
2. The assurance of data integrity;
3. The ability to prevent unauthorized access to and use of the system;
4. The security of hardware and software systems;
5. The regularity and extent of audit of the system by an independent body;
6. The existence of a declaration by a supervisory body, an accreditation body or a voluntary scheme regarding the reliability of the method;
7. Any applicable industry standards; and
8. Any relevant agreement.

7. Evidential Presumptions

1. Where a secure electronic signature certificate is used to sign an electronic record, it shall be presumed, until evidence to the contrary is adduced, that:
    1. Such electronic signature is the signature of the person to whom it correlates by virtue of the certificate;
    2. Such electronic signature was affixed by that person named in the certificate for the purpose of signing that electronic record; and
    3. The electronic record has not been altered since the specific point in time at which the electronic signature was affixed.
2. Where a secure electronic seal is used to seal an electronic record, until evidence to the contrary is adduced, the integrity of the electronic record and of correctness of the origin of that electronic record to which the secure electronic seal is linked shall be presumed.
3. Where a secure electronic time stamp is placed on an electronic record, until evidence to the contrary is adduced, the accuracy of the date and the time it indicates and the

integrity of the electronic record to which the date and time are bound, shall be presumed.

4. Where an electronic record is sent and received using a secure electronic registered delivery service, until evidence to the contrary is adduced, the integrity of the electronic record, the sending of that electronic record by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the secure electronic registered delivery service shall be presumed.

8. Originals of Documents, Records and Information

a. A legal requirement to retain or provide the original of a document, record or information in electronic form is satisfied where:

1. There exists a reliable assurance as to the integrity of the information contained in the electronic record, from the time it was made in its final form, whether such information was in its original form in a document in writing or as an electronic record;
2. Where the document, record or information is to be provided to a specific person, the electronic record that is provided to the person is capable of being displayed to such person; and
3. The relevant public body, which has jurisdictional oversight over the relevant activity, has consented to the provision or retention in the form of an electronic record and any additional requirements specified in a regulation by such competent public body in respect of the provision and retention are complied with.

b. For the purpose of paragraph (1) of subsection (a):

1. The criterion for assessing integrity is whether the information in the electronic record has remained complete and unaltered, apart from the introduction of changes that arise in the normal course of communication, storage and display of the information; and
2. The standard of reliability shall be assessed in light of all the circumstances in which, including the purpose for which, the record was generated.

c. A person may satisfy the requirement referred to in subsection (1) by using the services of any other person.

9. Legal Requirements for One or More Copies

Where multiple copies of the same document are required by the parties or under the law, this requirement is satisfied by providing an electronic record containing the information which that document must contain.

10. Retention of Documents, Records or Information

a. A legal requirement to retain any documents, records or information is satisfied by retaining the document, information or record in the form of an electronic record if the following conditions are met:

1. The information in the electronic record that is retained is accessible so as to be usable for subsequent reference;
2. The electronic record is retained in the format in which it was originally generated, sent or received, or in a format that may be proven to be accurately representing the information originally generated, sent or received;
3. Where the document, record or information to be retained was sent or received electronically, the information - if any - that identifies its origin and destination and the date and time when it was sent or received is retained; and
4. The competent public body, which has jurisdictional oversight over the relevant activity, has consented to the retention in the form of an electronic record and any additional requirements specified in a regulation by such competent public body in respect of the retention are complied with.

b. An obligation to retain any document, record or information in accordance with paragraph (3) of subsection (a) shall not extend to any information necessarily and automatically generated solely for the purpose of enabling a record to be sent or received.

c. A person may satisfy the requirement referred to in subsection (a) by using the services of any other person.

11. Formation of Contracts

In the context of the formation of contracts, unless otherwise agreed by the parties, an offer, the acceptance of an offer and any variation or withdrawal of the offer or acceptance may be expressed in whole or in part by means of electronic communications.

12. Invitation to Make Offers

A proposal to conclude a contract made through one or more electronic communications which is not addressed to one or more specific parties, but is generally accessible to parties making use of information systems, including a proposal that makes use of interactive applications for the placement of orders through such information systems, is to be considered as an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.

13. Declaration of Intent

As between the originator and the addressee, a declaration of intent shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of an electronic communication.

14. Electronic Agents

a. A contract formed by the interaction of an electronic agent and a natural person, or by the interaction of electronic agents, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the electronic agent or the resulting contract.

b. Where a natural person makes an input error in an electronic communication exchanged with the electronic agent of another party and the electronic agent does not provide the person with an opportunity to correct the error, that natural person, or the party on whose behalf that person was acting, has the right to withdraw the portion of the electronic communication in which the input error was made if:

1. The natural person, or the party on whose behalf that person was acting, notifies the other party of the error as soon as possible after having learned of the error and indicates that he made an error in the electronic communication; and
2. The natural person, or the party on whose behalf that person was acting, has not used any goods or services he may have received or obtained any material benefit or value from such goods or services.

c. The notification required under paragraph (1) of subsection (b) only applies where the other party has provided the natural person, or the party he is acting on behalf, with the information necessary for communicating with such other party.

15. Acknowledgement of Receipt of Electronic communications

a. Where, on or before sending an electronic communication, the originator has requested or has agreed with the addressee that receipt of the electronic communication be acknowledged:

1. If the originator has not agreed with the addressee that the acknowledgement of the receipt of the electronic communication be given in a particular form or by a particular method, an acknowledgement may, provided that it is sufficient to indicate to the originator that the electronic communication has been received, be given by any conduct of the addressee or any communication by the addressee, automated or otherwise.
2. If the originator has stated that the electronic communication is conditional on receipt of an acknowledgement, the electronic communication is treated as though it has never been sent until the acknowledgement is received; or
3. If the originator has requested an acknowledgement of receipt but has not stated that the validity of the electronic communication is conditional on receipt of an acknowledgement, within a time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator may give notice to the addressee stating that no acknowledgment has been received and specifying a reasonable time by which the acknowledgment must be received; and if the acknowledgement is not received within the time specified the originator may, upon notice to the addressee, treat the electronic communication as though it had never been sent, or exercise any other rights the originator may have under the law.

b. Where the originator receives the addressee’s acknowledgement of receipt, it is presumed, until proven otherwise, that the related electronic communication was received by the

addressee. That presumption does not imply that the content of the electronic communication sent corresponds to the record received.

c. Where the acknowledgement received by the originator states that the related electronic communication met technical requirements, either agreed upon or set forth in the criteria in force, it is presumed that those requirements have been met until proven otherwise.

d. The provisions of this section applies only to the sending or receipt of the electronic communication, and is not intended to address the legal consequences that may flow from that electronic communication and the acknowledgement of its receipt.

16. Time and Place of Dispatch and Receipt of Electronic Communications

1. Unless agreed otherwise between the originator and addressee, the time of dispatch of an electronic communication is the time when it leaves an information system under the control of the originator or of the party who sent it on behalf of the originator; or, where the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time when the electronic communication is received.
2. Unless agreed otherwise between the originator and addressee, the time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee; and the time of receipt of an electronic communication at another electronic address of the addressee is the time when it becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address. For the purposes of this subsection, an electronic communication is presumed unless proven otherwise to be capable of being retrieved by the addressee when it reaches the addressee’s electronic address.
3. Unless agreed otherwise between the originator and addressee, an electronic communication 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.
4. Subsection (b) shall apply notwithstanding that the place where the information system supporting an electronic address is located may be different from the place where the electronic communication is deemed to be received under subsection (c).

17. Location of the Parties

1. A party’s place of business in any transaction is the location indicated by that party, unless another party demonstrates that the party making the indication does not have a place of business at that location.
2. If a party has not indicated a place of business and has more than one place of business, then the place of business for the purposes of this law is that which has the closest relationship to the relevant transaction, having regard to the circumstances known to or contemplated by the parties at any time before or at the conclusion of the transaction; or where there is no underlying transaction in relation to the electronic communication the place of business is the principal place of business.

3. If a person does not have a place of business, reference is to be made to the person's habitual residence.
4. A location is not a place of business merely because that is where equipment and technology supporting an information system used by a party to the transaction is located; or where the information system may be accessed by third parties.
5. The sole fact that a party makes use of an electronic address or a domain name that is connected to a specific country does not create a presumption that its place of business is located in that country.

18. Notarization Using Electronic Means

1. Documents may be notarized and authenticated using electronic means. The competent Minister for justice affairs shall, after coordinating with the concerned bodies, issue a regulation specifying conditions and information technology standards that to be used for the purpose of ascertaining the identity of those requiring notarization, and for the creation, dispatch, retention and security of the electronic records related to the electronic notarization, type of electronic signature required for notarization, form for affixing the electronic signature on the document and specifying the documents that may be notarized or authenticated using electronic means.
2. Electronic records may be notarized, electronic signatures may be authenticated and date on private documents that are in the form of electronic records may be endorsed in accordance with rules and conditions to be specified in a regulation issued by the competent Minister for justice affairs after coordinating with the relevant concerned bodies.

19. Forgery Plea in respect of Electronic Records, Electronic Communications, Electronic Seals and Electronic Signatures

A person having an interest may plead as forgery electronic records, electronic communications, electronic seals and electronic signatures. The court shall rule on such pleas and defenses in respect of such electronic records, communications, seals and signatures in accordance with evidential rules specified under the law and consistent with the nature of the electronic records, electronic communications and electronic signatures.

20. Accreditation of Trust Service Providers

1. The competent authority may issue a regulation specifying the conditions and relevant criteria for the accreditation of any trust service, and specifying procedure for submitting and processing applications for accreditation, provided that such conditions and criteria may not include a requirement to use a specific type of software or hardware. In such case, a trust service provider incorporated or established in the Kingdom of Bahrain may apply to the competent administrative agency to approve its accreditation as an accredited trust service provider for a service that he specifies in his application. A resolution approving the accreditation and specifying its scope shall be issued by the competent authority and published in the Official Gazette upon ascertaining that the

trust service provider meets the conditions and relevant criteria including the standardization criteria to be used.

2. A fee shall be payable in respect of the application for accreditation and an annual fee for the accreditation if approved. Categories of the payable fees shall be prescribed in a regulation issued by the competent authority upon the approval of the Council of Ministers.
3. Accredited trust service providers shall be subject to oversight by the competent administrative agency and such audit requirements as the competent authority may prescribe in a regulation.
4. The competent authority may by virtue of a resolution withdraw, either fully or in respect of a specific trust service forming part of the scope of the accreditation, the accreditation of a trust service provider where the provider no longer meets the prescribed conditions and relevant criteria.
5. Before withdrawing an accreditation of a trust service provider, the competent administrative agency shall give notice in writing, by way of a registered letter with acknowledgement of delivery, to the accredited trust service provider of its intention to do so and specifying the reasons for the proposed withdrawal. The accredited trust service provider may within fourteen (14) days of its receipt of the notice submit representations in writing as to why the accreditation should not be withdrawn and such representation shall be considered within thirty (30) days of its receipt. Where the representation is rejected, the resolution withdrawing the accreditation and specifying the scope of the withdrawn accreditation shall be published in the Official Gazette.
6. The Council of Ministers may by virtue of a resolution appoint a government agency as an accredited trust service provider to provide one or more of the trust services and specifying the conditions to be complied with by such agency together with the fees payable by users of the trust services to such agency and the cases in which such fees may be waived.

21. Accreditation of External Trust Service Providers

a. A trust service provider which is incorporated outside the Kingdom and does not have a place of business in the Kingdom may apply to be accredited as a trust service provider for the services that he specifies in his application where such services are among those in respect of which a regulation has been issued by the competent authority in accordance with sub-section (a) of section 20 of this law. The procedure for submitting the application and its processing shall be subject to the same procedure specified in the regulation issued by the competent authority.

b. The competent authority shall issue a resolution published in the Official Gazette approving the application for accreditation and identifying its scope if the Service provider meets the following requirements:

1. The trust service provider operates in accordance with a criteria, including standardization to be used, of no lesser standard than the criteria referred to under sub-section (a) of section (20) of this law;
2. The trust service provider is accredited for the purpose of providing the relevant trust service in a foreign jurisdiction acceptable to the competent authority; and
3. Any other conditions specified by the competent authority in a regulation.

c. A fee shall be payable in respect of the application for accreditation and an annual fee for the accreditation if approved. Categories of the payable fees shall be prescribed in a regulation issued by the competent authority upon the approval of the Council of Ministers.

d. The provisions of sub-section (d) and (e) of section 20 shall apply in respect withdrawing the accreditation of external trust service providers.

22. Electronic Identification Scheme

The government department responsible for issuing personal identities may set up, operate and administer an electronic identification scheme. A regulation shall be issued by the Council of Ministers identifying the electronic identification services fee and the fee applicable in respect of certain services and cased in which payment of the fee may be waived.

23. Liability of Trust Service Providers

1. A trust service provider shall be liable for damage to any person, who reasonably relied on a trust service provided by the trust service provider, due to a failure to comply with the obligations under this law and its implementing regulation and if the damage was caused intentionally or negligently.
2. An accredited trust service provider shall not be liable where the person who relied on the certificate knew or ought reasonably to have known in the normal course of events that the certificate has expired or was revoked, suspended or that the accreditation of the relevant trust service provider has been withdrawn.
3. The intention or negligence of an accredited trust services provider shall be presumed unless that accredited trust service provider proves that the damage occurred without intention or negligence.
4. The burden of proving that the damage was not caused intentionally or negligently by a non-accredited trust services provider shall lie with the person claiming the damage.
5. Where a trust service provider duly informs its customers in advance of limitations on the use of its services and those limitations, including limitations on the value of transactions the subject of the services, are recognizable to third parties, the trust service provider shall not be liable for damages arising from the use of its services exceeding the indicated limitations provided that such damage was not intentionally caused.

24. Liability of Intermediaries

a. An intermediary is not subject to any civil or criminal liability in respect of any third party information, contained in a form of electronic records, that is not originated by the intermediary and to which the intermediary merely provides access and/or storage.

b. The exclusion of liability is subject to the following:

1. the intermediary has no knowledge that the information gives rise to civil or criminal liability;
2. the intermediary is not aware of any facts or circumstances that indicates, in the normal course of events, that a civil or criminal liability may arise; and

3. the intermediary promptly, after acquiring knowledge of any of the above, removes the information from any information system within the intermediary's control and cease to provide, or offer to provide, access or storage in respect of such information.

c. Nothing in this section imposes a legal obligation on an intermediary to monitor any third party information in the form of electronic records, if the intermediary's role is limited to providing access or storage to such records, in order to establish knowledge of any facts or circumstances that may in the normal course of events give rise to civil or criminal liability.

d. Nothing in this section shall affect:

1. Any obligations founded on contract;
2. Any obligations imposed by virtue of any law in connection with the provision of telecommunication services; or
3. Any obligations imposed by virtue of any other law, or by an executable judgement of a court, to restrict or remove or block or deny access to any information contained in the form of electronic records.

e. For the purpose of this section:

1. "provide access" in relation to third-party information , means the provision of the technical means by which third party information, in the form of electronic records , may be accessed or transmitted and includes the automatic, intermediate and temporary storage of the third-party information for the purpose of providing access to such information; and
2. "third-party" in relation to an intermediary means a person over whom the provider has no effective control.

25. Domain Name Registration

a. The competent Minister for Telecommunications shall issue a regulation after seeking the opinion of the competent Minister for Industrial Property, Telecommunication Regulatory Authority and such other persons whom the Minister deems appropriate, including the body known as the Internet Corporation for Assigned Names and Numbers, to regulate the registration and use of the domain name of the Kingdom of Bahrain.

b. The regulation under subsection (a) for the registration and use of the domain name of the Kingdom of Bahrain may include the following:

1. Subject to the prior approval of the Council of Ministers, appointing a non-governmental body to be responsible for all matters related to the domain name registration and collection of the fees payable in this respect. This body may appoint accredited registrars to undertake registration of domain names in accordance with conditions specified in the said regulation;
2. All particulars to be provided in an application for registration;
3. The period during which registration remains in force;

4. The procedure for submitting and processing applications for registration and renewal of the registration;
5. Circumstances in which applications for registration, and renewal of registration, may be declined and the circumstances in which approval of the registration or its renewal may be withdrawn;
6. Procedure for challenging decisions on registration made by the domain name registration body;
7. Determine the categories of fees to be paid for the application of registration and renewal of registration and the manner in which such fees are to be paid, subject to prior approval of the Council of Ministers; and
8. Such other matters related to registration.

c. A decree may be issued, upon presentation by the competent Minister for Telecommunications, appointing a public body to undertake all tasks related to the Domain Names registration and levy the applicable fees.

d. The competent Minister for Telecommunications shall issue a regulation prescribing a procedure for the settlement of disputes related to domain name registration, including disputes related to trademarks and tradenames, based on the principles established in the Uniform Domain-Name Dispute-Resolution Policy issued by the Internet Corporation for Assigned Names and Numbers. The Regulation shall prescribe a schedule of fees to be paid by parties using the procedure. A lawsuit related to a Domain Name Registration may not be lodged at the court unless the dispute was referred for resolution, and a ruling is rendered, according to the foregoing procedure.

e. The body registering domain names shall provide online public access to a reliable and accurate database of contact information for domain-name registrants.

f. For the purposes of this law, domain name of the Kingdom of Bahrain means the top level of the global domain name in Arabic and English assigned to the Kingdom of Bahrain by the Internet Corporation for Assigned Names and Numbers.

26. Criminal Offences

a. Without prejudice to any severer punishment prescribed under any other law, a person who wilfully commits any of the following acts shall be sanctioned by imprisonment for a term not exceeding ten (10) years and ordered to pay a fine not exceeding BD 100,000:

1. Accesses, copies or otherwise obtains possession of, or recreates the signature creation device or an electronic seal creation device of another person without the authorisation of that other person;
2. Alters, modifies, discloses or uses the electronic signature creation device, or an electronic seal creation device, of another person, without the authorisation of that other person or in excess of such authorisation;
3. Creates, publishes, alters, modifies or otherwise uses a certificate, an electronic signature, electronic seal or any trust service for a fraudulent or other unlawful purpose;

4. Misrepresents a person's identity or authorisation in requesting or accepting a certificate or in requesting suspension or revocation of a certificate; or
5. Publishes a certificate, or otherwise knowingly makes it available to anyone likely to rely on the certificate, or on an electronic signature or electronic seal listed in such certificate with reference to data in such certificate such as codes, passwords, algorithms, cryptographic keys or other data which are used for the purposes of verifying an electronic signature, or electronic seal, listed in the certificate, if the person knows that:
   i. The certificate service provider listed in the certificate has not issued it;
   ii. The subscriber listed in the certificate has not accepted it; or
   iii. The certificate has been revoked or suspended, unless its publication or making it available to the public is for the purpose of verifying an electronic signature, or an electronic seal, created prior to such revocation or suspension, or giving notice of the revocation or suspension.

b. Without prejudice to any severer punishment prescribed under any other law, a person who commits an act of forgery in an public electronic record shall be sanctioned by imprisonment for a term of not less than one (1) year and not exceeding ten (10) years and ordered to pay a fine not exceeding BD 150,000, and a person who commits an act of forgery in an private electronic record shall be sanctioned by imprisonment for a term of not less than six (6) months and not exceeding five (5) years and ordered to pay a fine not exceeding BD 100,000 or either of such sanctions.

27. Corporate Liability

Without prejudice to any criminal liability in respect of any natural person, a body corporate shall be criminally liable and punished by a fine not exceeding two times the maximum monetary fine prescribed in respect of the relevant offence under section (26) of this law where the offence had been committed in its name, for its own account or benefit, and where the offence had been the result of an action, default, gross negligence, consent or connivance of any of its directors, managers or officers of that body corporate or any other natural person who was purporting to act in any such capacity.

28. Regulations

Unless it is specifically prescribed in this Law that another authority is competent, the competent authority shall issue the implementing regulations that are necessary for the implementation of this Law.