

LEGISLATIVE DECREE NO.28 of 2002 WITH RESPECT TO ELECTRONIC TRANSACTIONS

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

having examining the constitution, and

The Code of Criminal Procedure of 1966, as amended, and

Civil and Commercial Procedures Act promulgated by Legislative Decree No. 12 of 1971, as amended, and

Law Governing the Judiciary promulgated by Legislative Decree No. 13 of 1971, as amended, and

Notarisation Law promulgated by Legislative Decree No. 14 of 1971, and

Bahrain Monetary Agency Law promulgated by Legislative Decree No. 23 of 1973, as amended per the Legislative Decree No. 14 of 1981, and

The Penal Code promulgated by Legislative Decree No. 15 of 1976, as amended, and

The Law of Commerce promulgated by Legislative Decree No. 7 of 1987, as amended, and

The Law of Evidence in Civil and Commercial Matters promulgated by Legislative Decree No. 14 of 1996, and

The Civil Code promulgated by Legislative Decree No. 19 of 2001,

Commercial Companies Law Legislative Decree No. 21 of 2001, and,

Upon the submission of the Economic Development Board's Chief Executive,

With the approval of the Council of Ministers,

Hereby decree the following Law:

Article 1

Definitions

For the application of the provisions of this Law, the following words and expressions shall have the meanings assigned against each, unless the context otherwise requires:

Electronic: means technology of using electrical, magnetic, electromagnetic, optical, biometric or photon means or any other similar technological devices.

Electronic Agent: means 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 an individual at the time of the action or response.

Record: means 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.

Electronic Record: means a record created, sent, received or communicated, stored by electronic means.

Originator: means a person whom, or on whose behalf, the electronic record purports to have been sent or generated prior to storage, if any, but does not include a person acting as a network intermediary with respect to that electronic record.

Addressee: means a person who is intended by the originator to receive the electronic record but does not include a person acting as a network intermediary with respect to that electronic record.

Network Intermediary: means a person who, on behalf of another person, sends, receives, transmits or stores that electronic record or provides other services with respect to that electronic record.

Information: includes data, text, images, figures, sounds, codes, computer programmes, software, databases, speech and the like.

Information System: means an electronic system for creating, sending, communicating, receiving, storing, displaying or presenting information.

Electronic Signature: means information in electronic form in, affixed to, or logically associated with an electronic record, and which may be used by the signatory to authenticate its identity.

Signatory: means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the person he represents.

Signature-creation device: means a device, such as configured software or hardware used by the signatory in creating an electronic signature.

Signature-creation data: means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.

Signature-verification device: means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature.

Accredited Certificate: means an electronic record that:

- (i) associates a signature verification data to a particular person;
- (ii) confirms the identity of that person.
- (iii) is used by an Accredited Certification Service Provider; and
- (iv) meets the relevant criteria agreed by the parties concerned or set out in resolutions issued pursuant to the provisions of this Law.

Certification Service Provider: means a person who issues identity certificates for the purposes of electronic signatures or provides other services to the public related to electronic signatures.

Accredited Certification Service Provider: means a Certification Service Provider accredited under Articles 16 and 17 of this Law to provide Accredited Certificates.

Security Procedure: means a procedure that is employed for the purpose of verifying that an electronic signature or record is that of a particular person or for detecting changes or errors in the content of an electronic record as transmitted by the originator.

Person: means any natural or legal person or public body.

Individual: means any natural person.

Ministry: means Ministry of Commerce and Industry.

Minister: means Minister of Commerce and Industry.

Article 2

Applications of this Law

1. The provisions of this Law shall apply to electronic records and signatures.
2. The provisions of this Law shall not apply to the following:
 - (i) all matters and transactions within the jurisdiction of the Sharia' Courts as set out in the Law Governing the Judiciary promulgated by Legislative Decree No. 13 of 1971, as amended;
 - (ii) all personal affairs of non-Muslims such as marriage, divorce, custody of children, adoption, inheritance, wills and codicils;
 - (iii) all matters and transactions which by virtue of any law are required to be notarised or evidenced by authentic documents;

- (iv) Negotiable bonds;
- (v) Title deeds, except those prescribed under Article 20 of this Law.

Article 3

Acceptance of Electronic Transaction

1. Nothing in this Law shall require a person to send, receive or display any electronic record or signature except upon explicitly obtaining their consent.

Except for the public bodies, the consent may be implicitly given through a positive behaviour.

2. Nothing in this Law shall prohibit a person engaging in an electronic transaction from establishing his own reasonable requirements about the manner in which to accept an electronic signature or electronic records.

Article 4

Requirements for Acceptance of Electronic Records

1. The consent of a public body to send or accept an electronic record or signature is given explicitly by way of a Ministerial regulation, issued pursuant to this Law by the minister responsible for that public body and published in the Official Gazette.

This regulation shall determine the extent to which it will send and accept electronic records and signatures.

2. The aforesaid consent indicated in the foregoing Paragraph shall always be subject to compliance with the technical requirements to be prescribed in a ministerial regulation to be issued by the Minister of Cabinet Affairs within a period not exceeding six months from the date of implementation of the provisions of this Law and its publication in the Official Gazette.

The requirements may specify the following:

- (i) The manner and format (including the information system standards) in which the electronic records must be created, generated, sent, communicated, received and stored and the systems established for such purposes.
- (ii) If electronic records must be signed by electronic means, the type of electronic signature required, information system standards to be used, the manner and format in which the electronic signature must be affixed to the electronic record and any requirements to be met by the electronic signature as to reliability.

- (iii) Control processes and procedures as are appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality and auditability of electronic records.
 - (iv) Any other required attributes for electronic records, deemed necessary or reasonable under the circumstances.
 - (v) Any requirements for acknowledgement of receipt by the public body of the electronic records.
3. The aforesaid provisions shall not prejudice any legislation that expressly prohibits the use of electronic means or expressly requires them to be used in specific ways.
 4. For the purpose of the preceding Paragraph, a reference to writing or signing does not in itself constitute a prohibition of the use of electronic means.

Article 5

Legal Recognition of Electronic Records in Evidence

1. Electronic records have the established legal recognition in evidence specified in the common documents. Information 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 not contained in the electronic record purporting to give rise to such legal effect, but is merely referred to in that electronic record.
2. Where a rule of law requires information to be in writing, or provides a legal effect if it is not, that requirement is met by an electronic record provided the information contained therein is accessible so as to be useable for subsequent reference whether by transmission, printing or otherwise.
3. Where a rule of law requires a person to provide information in writing to another person, that requirement is met by the provision of that information in an electronic form that is:
 - (i) accessible by the addressee so as to be usable for subsequent reference whether by transmission, printing or otherwise; and
 - (ii) capable of being retained by the addressee.
4. Information in the form of an electronic record shall be presumed to be authentic unless evidence is adduced;
 - (i) that the manner in which the electronic record was generated, stored or communicated was unreliable.

- (ii) that the manner in which the electronic record was signed was unreliable
- (iii) that the manner in which the integrity of the information was maintained was unreliable.
- (iv) of any other relevant factors to the integrity of the electronic record.

Article 6

Electronic Signature

1. Use of electronic signature shall not be denied legal effect, validity or enforceability solely on the grounds that it is wholly or partly in electronic form.
2. Where the law requires a signature of a person, or provides for a legal effect if a document is not signed, an electronic signature of that person satisfies the requirements of this Law.
3. In any legal proceedings involving an electronic signature that is associated with an Accredited Certificate, it shall be presumed unless the parties have agreed otherwise or unless evidence to the contrary is adduced that:
 - (i) such electronic signature is the signature of the person to whom it correlates;
 - (ii) such electronic signature was affixed by that person to whom it correlates for the purpose of signing such electronic record;
 - (iii) the electronic record that is signed with such signature has not been altered since the time at which the electronic signature was affixed.
4. If the electronic signature is not made with the use of an Accredited Certificate, the presumption of an authenticity created under the provisions of the preceding Paragraph shall not be attached to the electronic signature or record.

Article 7

Originals

1. A legal requirement that a document be presented or retained in its original form is satisfied by presenting or retaining the document as an electronic record provided:

- (i) there exists a reliable assurance as to the integrity of the information contained in the electronic record, from the time the electronic record was first created in its final form as an electronic record or written form;
 - (ii) where it is required that the original document is to be presented to a person, that electronic record is accessible, and capable of being displayed in an intelligible form to the concerned person.
 - (iii) The consent of the public body which has supervision, if applicable, over the requirements for the retention of such records has been obtained and any relevant requirements stipulated by that particular body have been complied with.
2. For the purpose of Paragraph (1)(a) of this Article, the following shall observed:
- (i) the criterion for assessing integrity is whether the information in the electronic record has remained complete and unaltered, apart from the addition of any endorsement or changes which arise in the normal course of generating, processing, transmitting, storing or safekeeping and displaying; and
 - (ii) the standard of reliability shall be assessed in light of all the circumstances in which, including the purpose for which, the record was created.

Article 8

Legal Requirements for One or More Copies

If the use of an electronic record is accepted between certain parties or otherwise permitted by law, a requirement that a copy or multiple copies of a document be provided to a person is satisfied by the provision of a single electronic record to that person.

Article 9

Retention of Documents

1. A legal requirement to retain documents, records or information that is created, sent or received in a paper form or electronically is satisfied by its retention as an electronic record if the following conditions are satisfied:
- (i) the electronic record is retained in the format in which it was created, sent or received, or in a format that can be demonstrated to accurately represent the information contained in the document that was originally created, sent or received;

- (ii) the information retained in the electronic record is accessible and is capable of being accurately displayed in an intelligible form so as to be useful for subsequent reference.
 - (iii) where the document 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 also retained; and
 - (iv) the consent of the public body which has supervision, if applicable, over the requirements for the electronically retention of such records has been obtained and any relevant requirements stipulated by that particular body have been complied with.
2. The requirements stipulated in the preceding Paragraph shall not apply to any information that may arise in the regular context for creation, processing, transmission, sending, retention or displaying.
 3. A person may satisfy the requirements referred to in Paragraph (1) of this Article by using the services of any other person.

Article 10

Formation of Contracts

In the context of the formation of the contracts, unless otherwise agreed by the parties, an offer and the acceptance of an offer or any other matter that is material to the formation to operation of a contract including any subsequent amendment or cancellation or revocation of the offer or acceptance of the offer, may be expressed in whole or in part by means of electronic records.

Article 11

Declaration of Intent or Similar Statements

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

Article 12

Involvement of Electronic Agents in Formation of Contracts

1. A contract may be formed by the interaction of an electronic agent and a person or by the interaction of electronic agents.
2. An electronic transaction between an individual and an electronic agent is voidable at the option of the individual if,

- (i) the individual makes a material error in any electronic information or electronic record used in or which was part of the transaction;
 - (ii) the electronic agent did not give the individual an opportunity to prevent or correct the error;
 - (iii) on becoming aware of the error, the individual promptly notifies the other party; and
 - (iv) in a case where consideration is received as a result of the error, the individual returns or destroys the consideration in accordance with the instructions agreed between the parties or according to the other person's instructions or, if there are no instructions, deals with the consideration in a reasonable manner and does not benefit materially by receiving the consideration.
3. Reference to "individual" in this Article shall be deemed to include the individual acting on his behalf or for another individual or legal person.
4. The requirement to notify under Paragraph (2) of Paragraph (C) above is only applicable where the other person has made available relevant contact details to the individual.

Article 13

Attribution

1. Unless otherwise agreed between the originator and the addressee of an electronic record, an electronic record is attributable to the originator if it was:
- (i) sent by the originator;
 - (ii) sent with the implied or express consent by an originator or an electronic agent of the originator; or
 - (iii) sent by any person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify an electronic record as that of its own unless the originator proves that such access had not resulted due to his negligence.
2. Attribution under the above Paragraph may be proven in any manner, including evidence as to the use of any security procedure previously agreed to by the parties or approved by a resolution adopted in implementation of the provisions of this Law or by showing the effectiveness of any other security procedure applied to determine the person to whom the electronic record is attributable.

3. Nothing in this Article shall affect any rule of law with respect to agency or the formation of contracts.

Article 14

Acknowledgement of Receipt of Electronic Record

1. Where, on or before sending an electronic record, the originator has agreed with or requested the addressee that receipt of the electronic record be acknowledged, then:
 - (a) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by:
 - any communication by the addressee, automated or otherwise; or
 - any communication by the addressee, sufficient to indicate the originator that the electronic record has been received.
 - (b) Where the originator has stated that the electronic record is conditional upon receipt of an acknowledgement, unless the parties agree otherwise the electronic record is treated as though it has never been sent, until the acknowledgement is received.
 - (c) Where the originator has not stated that the validity of the electronic record is conditional on receipt of an acknowledgement, and the acknowledgement has not been received by the originator within the 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 acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received and if the acknowledgement is not received within the time specified may, upon notice to the addressee, treat the electronic record as though it is null and void or invoke any other rights the originator may have.
2. Where the originator receives the addressee's acknowledgement of receipt, it is presumed, unless evidence to the contrary is adduced, that the related electronic record was received by the addressee. That presumption shall not imply that the content of the electronic record corresponds to the record received.
3. Where the received acknowledgement states that the related electronic record met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

4. Except in so far as it relates to the sending or receipt of the electronic record, the provisions of this Article shall not be intended to deal with the legal consequences that may flow either from that electronic record or from the acknowledgement of its receipt.

Article 15

Time and Place of Dispatch of Electronic Record

1. Unless otherwise agreed between the originator and the addressee, the dispatch of an electronic record shall be deemed to have occurred:
 - (i) when it enters an information system outside the control of the originator or of the person who sent the electronic record on behalf of the originator; or
 - (ii) if the originator and the addressee use the same information system, when it comes to the attention of and becomes capable of being retrieved by the addressee.
2. Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic record is determined as follows:
 - (i) Where the addressee has designated an information for the purpose of receiving electronic records, receipt shall be deemed to have occurred:
 - at the time when the electronic record enters the designated information system; or
 - if the electronic record is sent to an information system of the addressee that is not the designated information system, at the time when the electronic record comes to the attention of and becomes capable of being retrieved by the addressee.
 - (ii) If the addressee has not designated an information system, receipt occurs when the electronic record enters an information system of the addressee.
3. Unless otherwise agreed upon between the originator and the addressee, an electronic record is deemed to have been 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.

For the purposes of this Paragraph:

- (i) If the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction to which the electronic

record relates or, where there is no underlying transaction, the principal place of business;

- (ii) If the originator or the addressee does not have a place of business, the place of business is taken to be the place where the originator made it as his habitual residence.
- (iii) For the purpose of the above paragraph, "habitual place of residence" in relation to a body corporate is the place where it is incorporated.

Article 16

Certification and Revocation of Certification

1. The Minister, on application by a Certification Service Provider and on payment of such accreditation fees as may prescribed under a resolution issued by the Minister, may, if satisfied that the applicant meets the relevant criteria which may include criteria in respect to standards to be used, by notice published in the Official Gazette, accord the applicant the status of an Accredited Certification Service Provider.

The application and certification shall be subject to payment of fees the rates of which shall be determined by an order of the Minister to be first sanctioned by the Council Of Ministers.

2. Subject to the above provision, the Minister, if satisfied that an Accredited Certification Service Provider no longer meets the relevant requirements and criteria, shall be empowered according tot the provisions of the preceding Paragraph by notice published in the Official Gazette revoke an accreditation given.
3. Before revoking an accreditation, subject to the above provision, the Ministry shall give notice in writing with acknowledgment receipt to the Accredited Certification Service Provider regarding the procedure to be taken and indicating the reasons for the proposed revocation.

The Accredited Certification Service Provider shall, within 14 days of the notice, submit representations in writing as to why the accreditation should not be revoked, and consideration for such representations shall be determined within 30 days from the date of submitting the application.

Under no circumstance, a resolution, whether in acceptance or revocation of accreditation, as the case may be, shall be issued within maximum 45 days from the date the Accredited Certification Service Provider submitted the above notice.

4. In this Article, the "relevant requirements and criteria" means such requirements and criteria as the Minister may specify by regulation published within a period not exceeding four months from the date this Law comes into force.

Such criteria shall not include requirements for using certain software or hardware.

5. Accredited Certification may be issued by a government authority appointed by the Minister to act as an Accredited Certification Service Provider and indicate the applicable criteria, certification service charges and exemption cases in regulation from the Council of Ministers published in the Official Gazette.

Article 17

Accreditation of External Certification Service Provider

1. Following an application for accreditation made by a Certification Service Provider established outside Bahrain, the Minister may accord such accreditation as prescribed under Paragraph 1 of the preceding Article.
2. In determining to accord accreditation under the above Paragraph, the Minister shall have regard to whether the Certification Service Providers do in fact meet requirements and criteria equivalent to those required for an Accredited Certification Service Provider.
3. The Minister shall be empowered, by order published in the Official Gazette, revoke any accreditation accorded to External Certification Service Provider in cases and according to procedures and guarantees prescribed in Clauses (2) and (3) of the preceding Article.

Article 18

Liability of Accredited Certification Service Provider

1. An Accredited Certification Service Provider shall be deemed liable to any person who reasonably relied on the certificate for:
 - (i) the accuracy of all information in the Accredited Certificate as at the time at which it was issued;
 - (ii) assurance that the person identified in the Accredited Certificate held, at the time the Accredited Certificate, was issued, the signature creation data corresponding to the signature verification data given or identified in the Accredited Certificate;
 - (iii) If the Accredited Certification Service Provider generates both the signature creation data and the signature verification data, assurance that such data can be used together in a complementary manner, and
 - (iv) Failure to register or publish notice of the expiry, cancellation or suspension of an Accredited Certificate as prescribed under

regulations issued for the implementation of the provisions of this Law.

2. An Accredited Certification Service Provider shall not be deemed liable in the following circumstance:
 - (i) An Accredited Certification Service Provider committed no negligence.
 - (ii) Unless the person who relied on the Accredited Certificate knows or ought reasonably to have known that the certificate has expired or cancelled or suspended or that the accreditation of the Certification Service Provider has been revoked.
3. An Accredited Certification Service Provider that indicates in the Accredited Certificate limits on the uses of that certificate, including a limit on the value of transactions for which the certificate can be used, and makes those limits known to third parties, shall not be liable for damages arising from the use of the Accredited Certificate contrary to those limits, unless such damages were the result of an intentional or reckless misrepresentation made by the Accredited Certification Service Provide.

Article 19

Liability of Network Intermediaries

1. A network intermediary is not subject to any civil or criminal liability in respect of any third party information in the form of electronic records to which the network intermediary merely provides access and if the network intermediary was not the originator of such information, and if such liability is founded on:
 - (i) the making, publication, dissemination, or distribution of such information or any statement made in such information;
 - (ii) the infringement of any rights subsisting in or in relation to such information;
2. The exclusion of liability under the preceding Paragraph is subject to the following:
 - (i) the network intermediary has no actual knowledge that the information gives rise to civil or criminal liability;
 - (ii) is not aware of any facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known;
 - (iii) the network intermediary shall as soon as practicable, after acquiring actual knowledge of the above, removes the information from any information system within the network intermediary's control and ceases to provide or offer to provide access in respect of that information.

3. Nothing in this Article requires a network intermediary to monitor any third party information contained in an electronic record in respect of which the network intermediary provides access in order to establish knowledge, or to become aware, of facts or circumstances to determine whether or not the information gives rise to civil or criminal liability where the role of the network intermediary is limited to providing access to such records.
4. Nothing in this Article shall affect:
 - (i) any obligation founded on contract;
 - (ii) the obligations of a network intermediary under any legislation in connection with the provision of telecommunication services;
 - (iii) any obligations imposed under any other legislation or by an applicable court judgment to suspend, remove, block or deny access to any information in the form of electronic records.
5. In implementation of the provisions of this Article, "provide access" in relation to third-party information, means the provision of the technical means by which third-party information may be accessed, transmitted or merely transmitted more efficiently and includes the automatic, intermediate and temporary storage of the third-party information for the purpose of providing access.

"Third-party" in relation to a network intermediary means a person over whom the provider has no effective control.

Article 20

Transport Documents

1. This Article applies to any action done in connection with or pursuant to a contract for the carriage of goods, including but not limited to:
 - (i) furnishing the marks, number, quantity or weight of goods;
 - (ii) stating or declaring the nature or value of goods;
 - (iii) issuing a receipt of goods;
 - (iv) conforming that goods have been loaded;
 - (v) giving instructions to a carrier of goods;
 - (vi) claiming delivery of goods;
 - (vii) authorising release of goods;

- (viii) giving notice of loss of, or damage to, goods;
 - (ix) undertaking to deliver goods to a named person or a person authorised to claim delivery;
 - (x) granting, acquiring, renouncing, surrendering, transferring or negotiating any rights in connection with the goods;
 - (xi) notifying a person of terms and conditions of a contract of carriage of goods;
 - (xii) giving a notice or statement in connection with the performance of a contract of carriage of goods; and
 - (xiii) acquiring or transferring rights and obligations under a contract for carriage of goods.
2. A legal requirement that an act referred to in the preceding Paragraph be done in writing or by using a written document, that requirement is satisfied if the act is done using one or more electronic records.
 3. Without prejudice to the preceding Paragraph, if a right is to be granted to, or an obligation is to be acquired by a particular person, and if there is a legal requirement that this be done by the transfer or use of a written document, that legal requirement is satisfied by using one or more electronic records only if they are created by a method that gives reliable assurance that the right or obligation has become the right or obligation of that person.
 4. For the purpose of the preceding Paragraph, whether an assurance is reliable shall be determined in light of all the circumstances, including the purpose for which the right or obligation is conveyed and any other relevant agreement.
 5. Where one or more electronic records are used to do an act referred to in sub-paragraphs (1)(J) or (1)(m) above, no paper document used to do the same act is valid with respect to the same goods unless:
 - (i) the use of electronic records has been terminated with respect to the act and the goods, unilaterally or by agreement; and
 - (ii) the paper document that replaces the electronic record contains a statement of the termination.
 6. The replacement of the electronic records by a paper document as described in the preceding Paragraph does not affect the rights or obligations of the parties involved.

7. No rule of law is inapplicable to a contract of carriage of goods by reason only that the contract is set out in or evidenced by one or more electronic records instead of paper documents.

Article 21

Domain Name Registration

1. The Minister of Transportation may, by regulations made after consultation with the Minister of Commerce and Industry and such other persons and public bodies as the Minister considers appropriate or desirable, including the body known as the Internet Corporation for Assigned Names and Numbers, authorise, prohibit or regulate the registration and use of the "**bh**" domain name in Bahrain.
2. The regulation issued as to regulate the registration and use of the "**bh**" domain name may prescribe the following:
 - (i) the establishment of Domain Name Registration Office at the Ministry of Transportation;
 - (ii) the form of registration;
 - (iii) the period during which registration continues in force;
 - (iv) the manner in which the terms on which and the period or periods for which registration may be renewed;
 - (v) the circumstances and manner in which registrations may be granted by the Domain Name Registration Office;
 - (vi) process for contesting the decision of the Domain Name Registration Office;
 - (vii) determine the fees, if any, to be paid for the grant or renewal of registration and the time and manner in which such fees are to be paid, subject to prior consultation and approval of the Council of Ministers;
 - (viii) such other matters relating to registration.
3. For the application of the provisions of this Article, "bh domain name" means the top level of the global domain name systems assigned to Bahrain according to the two-letter code in the International Standard ISO 3166-1 (Codes for Representation of names of Countries and their Subdivision) of the International Organisation for Standardisation.

Article 22

Challenges to the Authenticity and integrity of Electronic Documents and Signature

1. An interested person may challenge electronic records and electronic signature thereon as false and he may also challenge the use of such signature as invalid if it is committed without the signatory's authorisation, or otherwise is invalid for reasons that would invalidate the effect of a signature in written form.
2. In any legal proceedings, challenges referred to in the preceding Paragraph as to the authenticity and integrity of electronic record and electronic signature shall be determined by the competent court in accordance with the applicable evidence procedures and rules and the provisions of this Law.

Article 23

Search Authority

Where there are reasonable grounds for believing that any place is used or is connected with committing an offence under this Law, such place may be searched, any person found at that place may be examined and all materials found are to be seized and taken away all or any part of such materials which appear to be relevant to committing an offence under the procedures and terms prescribed in the Code of Criminal Procedure of 1966, as amended.

To benefit from their experience in this regard, help may be sought from named officers of the Ministry of Commerce and industry during the search and seizure process.

Article 24

Penalties

1. Without prejudice to a harsher penalty provided for any other law, a person who intentionally commits any of the following acts shall be guilty of an offence and if convicted shall be liable to imprisonment for a term not exceeding ten years and to a fine not exceeding BD 100,000 or either penalty:
 - (i) Copies or otherwise obtains possession of, or recreates in bad faith, the signature creation device of another person without the authorisation of that other person;
 - (ii) alters, discloses or uses the signature creation device of another person without the authorisation of that other person or in excess of lawful authorisation;

- (iii) creates, publishes, alters or otherwise uses a certificate or an electronic signature for a fraudulent or other unlawful purposes;
 - (iv) misrepresents a person's identity or authorisation in requesting or accepting a certificate or in requesting suspension or revocation of a certificate;
 - (v) publishes a certificate, or otherwise makes it available to anyone likely to rely on the certificate or on an electronic signature that is verifiable with reference to data such as codes, passwords, algorithms, public cryptographic keys or other data which are used for the purposes of verifying an electronic signature, listed in the certificate, if the person knows that:
 - the Certification Service Provider listed in the certificate has not issued it;
 - the subscriber listed in the certificate has not accepted it; or
 - the certificate has been revoked or suspended, unless its publication is for the purpose of verifying an electronic signature created before such revocation or suspension, or giving notice of revocation or suspension.
2. Without prejudice to a harsher penalty provided for any other law, every person who intentionally obstructs an officer who has the power of summary arrest or an authorised officer to carry out an inspection or prevents them from carrying out the acts prescribed in Article 23 of this Law, shall be guilty of an offence and if convicted shall be liable to imprisonment for a term not exceeding three years and to a fine not exceeding BD 10,000 or either penalty.

Article 25

Liability of Corporate Officers

Where an offence under this Law has been committed by a body corporate, and it is proved to have been committed with the consent or connivance of, or to be attributable to any act or default on the part of, any director, manager or other similar responsible officer of the body corporate, or any person who was purporting to act in such capacity, as well as the body corporate, shall be guilty of that offence and shall be liable to a fine not exceeding BD 200,000.

Every natural person who is imputed to commit any of the above acts shall be guilty and shall be liable for the penalty prescribed under the provisions of this Law.

Article 26

Regulations

Unless it is specifically prescribed in this Law that another authority is competent, the Minister may make regulations generally for any matter the Minister considers necessary to give effect to the provisions in this Law:

- (i) prescribing the relevant requirements and criteria for accrediting Certification Service Providers and for issuing Accredited Certificates; and
- (ii) specifying the due fees categories on applications and services prescribed in Articles 16 and 17 of this Law with the approval of the Council of Ministers;
- (iii) respecting any matter for which provision may be made by regulations under this Law.

Such regulations shall be published in the Official Gazette.

Article 27

Coming into Force

The Ministers shall, each in his respective capacity, be charged with the implementation of this Law and it shall come into effect on the date of its publication in the Official Gazette.

Signed: Hamad bin Isa Al Khalifa
King of the Kingdom of Bahrain
Khalifa bin Salman Al Khalifa
Prime Minister

Issued at Rifa'a Place on: on 7th Rajab 1423 Hijra
Corresponding to: 14 September 2002