

ELECTRONIC TRANSACTIONS ACT

B.E. 2544 (2001)

BHUMIBOL ADULYADEJ, REX.

Given on the 2nd day of December B.E. 2544

Being the 56th year of the Present Reign

His Majesty King Bhumibol Adulyadej is graciously pleased to proclaim that,

Whereas it is deemed expedient to have a law on electronic transactions,

And whereas this Act contains certain provisions relating to the restriction of personal rights and freedom, for which Section 29 incorporating Section 50 of the Constitution of the Kingdom of Thailand provides that it can be made by virtue of the provisions of a law.

Be it therefore enacted by H. M. the King an Act, by and with the advice and consent of the Parliament, as follows:

Section 1. This Act shall be called the ‘Electronic Transactions Act B.E. 2544 (A.D. 2001)’

Section 2. This Act shall come into force after one hundred and twenty days as from the date of its publication in the Government Gazette.

Section 3. This Act shall apply to all civil and commercial transactions performed by using a data message, except the transactions prescribed by a Royal Decree to be excluded from this Act wholly or partly.

The provisions of paragraph one do not prejudice any law or rule enacted for consumer protection.

This Act shall apply to the transactions in connection with the carrying out of the affairs of the State as prescribed in Chapter 4.

Section 4. In this Act:

“transaction” means any act relating to a civil and commercial activity or carrying out of the affairs of the State as prescribed in Chapter 4.

“electronics” means an application of an electron means, an electrical means, an electromagnetic means or any other means of a similar nature including an application of an optical means, a magnetic means or a device in connection with an application of any of the aforesaid means;

“electronic transaction” means a transaction in which an electronic means is used in whole or in part;

“information” means an incident or fact regardless of whether expressed in the form of a letter, number, sound, image or any other form capable of connotation by itself or through any means;

“data message” means information generated, sent, received, stored or processed by electronic means, such, as electronic data interchange (EDI), electronic mail, telegram, telex or facsimile;

“electronic signature” means letter, character, number, sound or any other symbol created in electronic form and affixed to a data message in order to establish the association between a person and a data message for the purpose of identifying the signatory who involves in such data message and showing that the signatory approves the information contained in such data message;

“information system” means a system of (data message) processing by using an electronic device for generating, sending, receiving, storing or processing a data message;

“electronic data interchange” means the despatch or receipt of information by an electronic from computer to computer using an agreed standard;

“originator” means a person by whom the data message purports to have been sent or generated prior to storage before being sent pursuant to the method designated by such person, whether such data message is sent by such person, or generated in the name of or on behalf of such person, but does not include an intermediary with respect to that data message;

“addressee” means a person who is intended by the originator to receive the data message and who receives such data message, but does not include an intermediary with respect to that data message;

“intermediary” means a person who, on behalf of another person, sends, receives or stores a particular data message, including the providing of other services with respect to that data message;

“certificate” means a data message or other record confirming the link between a signatory and signature creation data;

“signatory” means a person that holds signature creation data and creates the electronic signature either on his own behalf or on behalf of other persons;

“relying party” means a person that may act on the basis of a certificate or an electronic signature;

“State agency” means a Ministry, Bureau, Department, other Government agency by a different name and having the status of a Department, a provincial administration, a local administration and a State enterprise established by an Act or a Royal Decree and shall also include a juristic person, a group of persons or a person having the power and duties to perform the State affairs in any matter whatsoever;

“Commission” means the Electronic Transaction Commission;

“Minister” means the Minister in charge of this Act.

Section 5. The provisions of Section 13 to Section 24 and the provisions of Section 26 to Section 31 may be agreed otherwise.

Section 6. The Prime Minister shall be in charge of this Act.

CHAPTER 1

ELECTRONIC TRANSACTIONS

Section 7. Information shall not be denied legal effect and enforceability solely on the ground that it is in the form of a data message.

Section 8. Subject to the provision of Section 9, in the case where the law requires any transaction to be made in writing, to be evidenced in writing or supported by a

document which must be produced, if the information is generated in the form of a data message which is accessible and usable for subsequent reference without its meaning being altered, it shall be deemed that such information is made in writing, is evidenced in writing or is supported by a document.

Section 9. In the case where a person is to enter a signature in a writing, it shall be deemed that such data message bears a signature if:

(1) the method used is capable of identifying the signatory and indicating that the signatory has approved the information contained in such data message as being his own; and

(2) such method is a reliable one and appropriate for the purpose for which the data message is generated or sent, having regard to the surrounding circumstances or an agreement between the parties.

Section 10. In the case where the law requires that any information be presented or retained in its original form as an original document, if such information is presented or retained in the form of data message pursuant to the following requirements, it shall be deemed that such information is presented or retained as an original document under the law:

(1) a reliable method is used with the data message to assure the integrity of the information from the time when it is generated in its final form; and

(2) the information is capable of being subsequently displayed.

The integrity of the information under (1) shall be determined by having regard to its completeness and unalteration, apart from the addition of any endorsement or record or any change which may arise in the normal course of communication, storage or display of the information, which does not affect the integrity of that information.

In determining the method used for assuring the integrity of the information under (1), all relevant circumstances must be taken into consideration, including the purpose for which such information is generated.

Section 11. The admissibility of a data message as an evidence in the legal proceedings shall not be denied solely on the grounds that it is a data message.

In assessing the evidential weight of a data message whether it is reliable or not, regard shall be had to the reliability of the manner in which or the method by which the data message was generated, stored or communicated, the manner in which or the method by which the completeness and integrity of the information was maintained, the manner in which or the method by which the originator was identified or indicated, including all relevant circumstances.

Section 12. Subject to the provision of Section 10, in the case where the law requires that certain documents or information be retained, if such retention is made in the form of a data message pursuant to the following requirements, it shall be deemed that such document or information is retained pursuant to the requirements of the law:

(1) that data message is accessible so as to be usable for subsequent reference without its meaning being altered;

(2) that data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(3) the information, if any, which specifies the source, origin and destination of a data message including the date and time sent or received, is retained.

The provisions of paragraph one shall not apply to the information the sole purpose of which is to enable the data message to be sent or received.

The State agency responsible for retaining any document or information may prescribe additional details with respect to the requirement in retaining such document or information insofar as they are not contrary to the provisions of this Section.

Section 13. An offer or acceptance in entering into a contract may be expressed by means of a data message. A contract shall not be denied legal effect solely on the grounds that such offer or acceptance is made in the form of a data message.

Section 14. As between the originator and the addressee of a data message, a declaration of will or notice may be made in the form of a data message.

Section 15. Whoever sends a data message by whatever means, it shall be deemed that the data message belongs to such person.

As between the originator and the addressee, a data message is deemed to be that of the originator if it is sent by:

(1) a person who is authorized to act on behalf of the originator in respect of that data message; or

(2) an information system programmed to operate automatically in advance, by the originator or a person authorized to act on behalf of the originator.

Section 16. The addressee is entitled to regard a data message as being that of the originator and shall also be entitled to act pursuant to such data message if:

(1) the addressee has properly applied a procedure previously agreed with the originator to verify whether the data message was that of the originator; or

(2) the data message received by the addressee results from an act of a person who uses a method which is used by the originator to identify data message as his own and to which that person has gained access through the relationship with the originator or person who is authorized to act on behalf of the originator.

The provisions of paragraph one shall not apply if:

(1) as of the time when the addressee has received notice from the originator that the data message is not that of the originator and, at the same time, the addressee had a reasonable time to verify the facts to which the notice relates; or

(2) in a case pursuant to paragraph one (1), at any time when the addressee knew or should have known, had the addressee exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.

Section 17. In the case of Section 15 or Section 16 paragraph one, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send and to act on that assumption on the data message unless the addressee knew or should have known, had the addressee exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

Section 18. The addressee is entitled to regard each data message received as a separate data message and to act on that assumption with respect to each data message except to the extent that it duplicates another data message and the addressee knew or

should have known, had the addressee exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

Section 19. *In the case where an acknowledgement of receipt of a data message is required whether at the request of the originator or as agreed with the addressee before or at the time of sending such data message or as appeared in that data message, the following rules shall apply:*

(1) where the originator has not agreed 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, whether by an automated information system or by any other method, or by any conduct of the addressee sufficient to indicate to the originator that the addressee has received the data message.

(2) where the originator has stated a condition that the data message shall be regarded as having been sent only upon receipt of an acknowledgement by the addressee, it shall be deemed that the data message has never been sent, until the originator has received the acknowledgement.

(3) where the originator has not stated such a condition under paragraph (2) and the originator has not received the acknowledgement within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator:

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be made by the addressee; and

(b) if the acknowledgement is not received by the originator within the time specified in subparagraph (a), may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.

Section 20. *Where the originator receives the addressee's acknowledgement of receipt it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message received by the addressee corresponds to the data message sent by the originator.*

Section 21. *Where the received acknowledgement states that the related data message received by the addressee met the technical requirements, either agreed upon by*

the originator and the addressee or set forth in the applicable standards, it is presumed that those requirements have been met.

Section 22. The dispatch of a data message is deemed to occur when such data message enters an information system outside the control of the originator.

Section 23. The receipt of a data message is deemed to occur from the time when such data message enters an information system of the addressee.

If the addressee has designated an information system for the purpose of receiving data message specifically, it shall be deemed that the receipt of a data message occurs at the time when the data message enters the designated information system. However, if such data message is sent to an information system of the addressee that is not the designated information system, it shall be deemed that the receipt of a data message occurs at the time when the data message is retrieved from that information system.

The provision of this section applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received by the addressee under Section 24.

Section 24. The dispatch or the receipt of a data message shall be deemed to be dispatched at the place where the originator has its place of business or received at the place where the addressee has its place of business, as the case may be.

If the originator or the addressee has more than one place of business, it shall be deemed that the place of business is that which has the closest relationship to the underlying transaction for the purpose of paragraph one. However, if it is unable to determine that which place of business has the closest relationship to the underlying transaction, it shall be deemed that the principal place of business is the place where such data message is received or dispatched.

If the originator or the addressee does not have a place of business, it shall be deemed that his habitual residence is the place where a data message is received or dispatched.

The provisions of this section shall not apply to the dispatch and receipt of a data message by telegramme and telex or by any other means of communication prescribed in the Royal Decree.

Section 25. Any electronic transaction made in accordance with the security procedure prescribed in the Royal Decree is presumed to be made by a reliable method.

CHAPTER 2 ELECTRONIC SIGNATURES

Section 26. An electronic signature is considered to be a reliable electronic signature if it meets the following requirements:

(1) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(2) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(3) any alteration to the electronic signature, made after the time of signing, is detectable; and

(4) where a purpose of the legal requirement for a signature is to provide assurance as to the completeness and integrity of the information and any alteration made to that information after the time of signing is detectable.

The provision of paragraph one does not limit that there is no other way to prove the reliability of an electronic signature or the adducing of the evidence of the non-reliability of an electronic signature.

Section 27. Where signature creation data can be used to create a signature that has legal effect, each signatory shall:

(1) exercise reasonable care to avoid unauthorized use of its signature creation data;

(2) without undue delay, notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:

(a) the signatory knows or should have known that the signature creation data have been lost, damaged, compromised, unduly disclosed or known in the manner inconsistent with their purpose;

(b) the signatory knows from the circumstances occurred that there is a substantial risk that the signature creation data may have been lost, damaged, compromised, unduly disclosed or known in the manner inconsistent with their purpose;

(3) where a certificate is issued to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory which are relevant to the certificate throughout its life-cycle, or as specified in the certificate.

Section 28. Where a certification service is provided to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall perform as follows:

(1) act in accordance with representations made by it with respect to its policies and practices;

(2) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life-cycle, or as specified in the certificate;

(3) provide reasonably accessible means which enable a relying party to ascertain in all material representations from the certificate in the following matters:

(a) the identity of the certification service provider;

(b) that the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;

(c) that signature creation data were valid at or before the time when the certificate was issued;

(4) provide reasonably accessible means which enable a relying party to ascertain from the certificate or otherwise as follows:

(a) the method used to identify the signatory;

(b) any limitation on the purpose or value for which the signature creation data or the certificate may be used;

(c) that the signature creation data are valid and have not been lost, damaged, compromised, unduly disclosed or known in a manner inconsistent with their purpose;

(d) any limitation on the scope or extent of liability stipulated by the certification service provider;

(e) the availability of the means for the signatory to give notice upon the occurrence of the events pursuant to Section 27 (2); and

(f) a timely revocation service is offered;

(5) where services under subparagraph (4) (e) are offered, provide a means for a signatory to give notice pursuant to Section 27 (2) and, where services under (4) (f) are offered, ensure the availability of a timely revocation service;

(6) utilize trustworthy systems, procedures and human resources in performing its services.

Section 29. *In determining whether any systems, procedures and human resources under Section 28 (6) are trustworthy, regard shall be had to the following factors:*

(1) financial and human resources, including existence of assets;

(2) quality of hardware and software systems;

(3) procedures for processing of certificates and applications for certificates and retention of records in connection with the provision of such services;

(4) availability of information on the signatories identified in certificates and on the potential relying parties;

(5) regularity and extent of audit by an independent body;

(6) the certification issuing organizations or certification service provider with respect to the practice or existence of the factors specified in subparagraphs (1) to (5);

(7) any other factor prescribed by the Commission.

Section 30. *A relying party is required to do the following:*

(1) take reasonable steps to verify the reliability of an electronic signature;

(2) where an electronic signature is supported by a certificate, take reasonable steps to:

(a) verify the validity, suspension or revocation of the certificate; and

(b) observe any limitation with respect to the certificate.

Section 31. *A certificate or an electronic signature shall be deemed to be legally effective without having to consider:*

(1) the geographic location where the certificate is issued or the electronic signature created or used; or

(2) the geographic location of the place of business of the issuer of the certificate or signatory.

A certificate issued in a foreign country shall have the same legal effect as a certificate issued in the country if the level of reliability used in issuing such certificate is not lower than as prescribed in this Act.

An electronic signature created or used in a foreign country shall have the same legal effect in the country as an electronic signature created or used in the country if the level of reliability used in creating or using such electronic signature is not lower than as prescribed in this Act.

In determining whether which certificate or electronic signature offers reliability pursuant to paragraph two or paragraph three, regard shall be had to recognized international standards and any other relevant factors.

CHAPTER 3
SERVICE BUSINESS RELATING TO
ELECTRONIC TRANSACTIONS

Section 32. Persons shall have the right to operate service business relating to electronic transaction. In the event where it is necessary to maintain financial and commercial stability, or for benefit of strengthening the credibility and acceptance of electronic transactions system, or to prevent damage to the public, a Royal Decree prescribing the service business relating to electronic transaction which shall be subject to prior notification, registration or licence shall be issued.

As to which case would require notification, registration or licence under paragraph one, the determination shall be taken based on the appropriateness of damage prevention in accordance with degree of severity of the impact which may occur from such business operation.

For this purpose, any particular State agency may be designated by such Royal Decree to be the responsible supervisory agency.

Prior to the proposal of the issuance of the Royal Decree under paragraph one, a public hearing shall be conducted as it may be deemed proper and the information to be derived therefrom shall be taken into account.

Section 33. In the event where there is a Royal Decree prescribing the service business relating to electronic transactions which shall be subject to prior notification or registration, the person wishing to operate such business shall notify, or apply for registration with the competent official as prescribed in the Royal Decree prior to the commencement of such business operation.

The rules and procedures for notification or registration under paragraph one shall be as prescribed in the Royal Decree. When the competent official under the Royal Decree is notified or accepts the registration, he or she shall issue a certificate of notification or a certificate of registration as evidence of the notification or registration on the date of notification or registration. The person making notification or applying for registration can operate such business as from the date of the notification or registration. If, subsequently, the competent official under the Royal Decree finds out that the notification or the registration has been made inaccurately or incompletely, the competent official shall have the power to order the person having made the notification or having applied for the registration to correct or complete it within seven days from the receipt date of such order.

In operating the business, the person having made the notification or having applied for the registration under paragraph one shall comply with the rules prescribed in the Royal Decree and those prescribed by the Commission.

If the person having made the notification or having applied for the registration under paragraph one fails to correct the inaccurate or incomplete notification or registration under paragraph two, or violates or fails to comply with the rules for the business operation under paragraph three, the Commission shall consider and issue an order imposing an administrative fine not exceeding one million Baht, taking into account the severity of the offence and, in case where it deems fit, the Commission may issue an order requiring such person to take any corrective action as appropriate.

The rules used for determination to impose an administrative fine shall be as prescribed by the Commission. If the person subject to administrative fine fails to make payment, the provisions relating to the administrative execution under the law on administrative procedure shall apply mutatis mutandis. In case where there is no official to proceed with the execution in accordance with such order, the Commission shall be empowered to bring a lawsuit before the Administrative Court to enforce payment of the fine. In this connection, if the Administrative Court has a view that the order imposing the

fine is lawful, the Administrative Court shall be empowered to try and adjudicate the case and order the seizure or attachment of the property for sale by auction to pay for the fine.

In case where the person committing the offence under paragraph four fails to make correction in accordance with the order of the Commission or repeats the offence, the Commission shall be empowered to issue an order prohibiting such person from further operating the business as notified or registered.

Section 34. In case where a Royal Decree is issued prescribing the service business relating to electronic transactions which shall be subject to prior licence, the person wishing to operate such business shall apply for such licence with the competent official as prescribed in the Royal Decree.

The qualifications of the applicant for the licence, the rules and procedures for applying for the licence, the licence issuance, the licence renewal, the return of the licence, the suspension or revocation of the licence shall be as prescribed in the Royal Decree.

In operating the business, the person who has obtained the licence under paragraph one shall comply with the rules prescribed in the Royal Decree and those prescribed by the Commission or conditions stipulated in the licence.

In case the person who has obtained the licence violates or fails to comply with the rules for operating the service business relating to electronic transactions under paragraph three, the Commission shall be empowered to consider and issue an order imposing an administrative fine not exceeding two million Baht, taking into account of the severity of the offence. In case where it deems fit, the Commission may issue an order requiring such person to take any corrective action as appropriate. In this connection, the provisions of section 33, paragraph five, shall apply mutatis mutandis.

If the person committing the offence under paragraph four fails to make correction in accordance with the order of the Commission or repeats the offence, the Commission shall be empowered to issue an order revoking the licence.

CHAPTER 4
ELECTRONIC TRANSACTIONS
IN THE PUBLIC SECTOR

Section 35. An application, permission, registration, administrative order, payment, notification or any legal action taken against or by a State agency shall, if made in the form of data message in accordance with the rules and procedures prescribed by the Royal Decree, be governed by this Act and shall have the same legal effect as those undertaken in accordance with the rules and procedures provided by law governing such particular matter. For this purpose, the Royal Decree may also require the person concerned to act or refrain from acting or require the State agency to issue rules prescribing details in certain cases.

In issuing the Royal Decree under paragraph one, such Royal Decree may require the person operating the service business relating to electronic transactions to notify or apply for registration or licence, as the case may be, prior to the commencement of the business operation. In this case, the provisions of Chapter 3 and the relevant penalty provisions shall apply mutatis mutandis.

CHAPTER 5
ELECTRONIC TRANSACTIONS COMMISSION

Section 36. There shall be the Electronic Transactions Commission which consists of the Minister of Science, Technology and Environment acting as the Chairman and the other twelve members appointed by the Cabinet from qualified persons, provided that, two qualified persons must be from each of the following fields:

- (1) finance;***
- (2) electronic commerce;***
- (3) law;***
- (4) computer science;***
- (5) science or engineering;***
- (6) social science.***

Provided that each qualified person from each field must be from the private sector and the Director of the National Electronics and Computer Technology Center, National Science and Technology Development Agency, shall be a member and secretary.

The rules and procedures in selecting and nominating the qualified persons to the Cabinet for their consideration to appoint to be the Commission under paragraph one must be in accordance with the rules prescribed by the Minister.

The secretary shall appoint no more than two persons as assistant secretaries.

Section 37. The Electronic Transaction Commission shall have the following authorities and duties:

(1) To make recommendation to the Cabinet to lay down policies for promotion and development of electronic transactions including solving relevant problems and obstacles;

(2) To monitor and supervise the operation of service business relating to electronic transactions;

(3) To make recommendation or give advice to the Minister to issue Royal Decrees pursuant to this Act.

(4) To issue rules or notifications relating to electronic signature in compliance with this Act or the Royal Decrees issued pursuant to this Act.

(5) To perform any other act in compliance with this Act or other laws.

In performing acts under this Act, the Commission shall be an official under the Penal Code.

Section 38. A qualified member shall hold the position for a term of three years.

A retired member may be re-appointed for no more than two consecutive terms.

Section 39. Other than retirement by rotation under Section 38, a qualified member shall be discharged from the position upon:

(1) death;

(2) resignation;

(3) being removed by the Cabinet due to misbehavior, negligence or dishonesty, or lack of competence;

(4) being an incompetent or quasi-incompetent person;

(5) having been imprisoned by a final judgement, except in a case where an offence committed through negligence or a petty offence.

Section 40. In case where a qualified person is discharged from the position under section 39, it shall be deemed that the Commission consists of the remaining members and a new member must be appointed to fill such vacancy within sixty days from the date the member is discharged from the office.

The member appointed to fill such vacancy shall remain in office for the balance of the term of the replaced member.

Section 41. The quorum of the Commission's meeting shall consist of no less than one-half of the total number of its members.

If the Chairman is not present at the meeting or is unable to perform his duty, the Commission shall elect one of its members to act as the Chairman of the meeting.

A decision of the meeting shall be made by a majority votes. Each member shall have one vote. In case of a tied vote, the Chairman shall have a second or casting vote.

Section 42. The Commission shall have the power to appoint a sub-committee to consider or perform any act on behalf of the Commission.

The provision of Section 41 shall apply to a meeting of the sub-committee mutatis mutandis.

Section 43. The National Electronics and Computer Technology Center, National Science and Technology Development Agency shall be the secretariat of the Commission.

CHAPTER 6

PENALTIES

Section 44. Any person operating the service business relating to electronic transactions without notifying or applying for registration with the competent official as prescribed by the Royal Decree under Section 33, paragraph one, or in violation of the prohibition order to operate business of the Commission pursuant to Section 33, paragraph

six, shall be liable to imprisonment for a term of not more than one year, or to a fine of not more than one hundred thousand Baht, or both.

Section 45. Any person operating the service business relating to electronic transactions without acquiring a license pursuant to Section 34 shall be liable to imprisonment for a term of not more than two years, or to a fine of not more than two hundred thousand Baht, or both.

Section 46. All offences under this Act, if committed by a juristic person, the manager or representative of the juristic person or the person participating in the operation of that juristic person shall also be liable to such offence, unless such person can prove that he did not know about such offence or did not participating in committing such offence.

Countersigned by:

Pol. Lieutenant Colonel Taksin Shinawatre

Prime Minister

Note:- The reasons for promulgation of this Act are as follows: At present, the communication methods are likely to be adjusted based on the development of the electronic technology which is convenient, fast and efficient. However, the methods of such electronic transactions are greatly different from those of transactions supported by existing laws. This results in the necessity to provide legal recognition of data messages by treating them the same as the message made or evidenced in writing, recognition methods of dispatch and receipt of data messages, use of electronic signatures, including the evidential admissibility of data messages, aiming to promote the reliability of electronic transactions to enable them to have the same legal effect as that given to transactions made by traditional means. The Electronic Transactions Commission should also be set up to lay down policies and prescribe rules to promote electronic transactions to monitor the business operation of electronic transactions. Its duties shall include to promote the development of technology to monitor the development of technology which is constantly changing, so that the reliable standards can be achieved. In addition, it is to give advice to resolve problems and obstacles in order to promote the use of electronic transactions domestically and internationally. The foregoing can be achieved by adopting a law in line with internationally recognised standard. It is, therefore, necessary to promulgate this Act.