

Electronic Transactions

AN ACT TO RECOGNIZE AND FACILITATE THE FORMATION OF CONTRACTS, THE CREATION AND EXCHANGE OF DATA MESSAGES, ELECTRONIC DOCUMENTS, ELECTRONIC RECORDS AND OTHER COMMUNICATIONS IN ELECTRONIC FORM IN SRI LANKA ; AND TO PROVIDE FOR THE APPOINTMENT OF A CERTIFICATION AUTHORITY AND LICENSING AND AUTHORISING OF CERTIFICATION SERVICE PROVIDERS; TO GIVE EFFECT TO THE PROVISIONS OF THE UNITED NATIONS CONVENTION ON THE USE OF ELECTRONIC COMMUNICATIONS IN INTERNATIONAL CONTRACTS AND TO PROVIDE FOR MATTERS CONNECTED THEREWITH OR INCIDENTAL THERETO.

BE it enacted by the Parliament of the Democratic Socialist Republic of Sri Lanka as follows

:-

Act Nos,
25 of 2017

Short title and date of operation. 1. (1) This Act may be cited as the Electronic Transactions Act, No. 19 of 2006.

(2) The provisions of subsection (1) of this section shall come into operation on the date on which this Act is Certified as an Act of Parliament and the other provisions shall come into operation on such date as the Minister may appoint, by Order published in the Gazette (hereinafter referred to as the 'appointed date').

CHAPTER I GENERAL PROVISIONS

Objectives of the Act.
[3, 25 of 2017]

2. The objectives of the Act shall be-

- (a) to facilitate domestic and international electronic commerce by eliminating legal barriers and establishing legal certainty;
- (b) to encourage the use of reliable forms of electronic commerce;
- (c) to facilitate electronic filing of any application, petition, plaint, answer, written submission or any other document with any court;

(ca) to facilitate electronic filing of any form, application, or any other document with any ministry, department, provincial council, provincial ministry and department or local authority or, office, body or agency owned or controlled by the Government or a statutory body in a particular manner and to promote efficient delivery of public service by means of reliable forms of electronic communications;

(d) to promote public confidence in the authenticity, integrity and reliability of data messages, electronic documents, electronic records or other communications; and.

(e) to implement the provisions of the Convention subject to such restrictions specified in section 23 of this Act declared at the time of ratification of the Convention.

CHAPTER II

RECOGNITION DATAMESSAGES AND OTHER COMMUNICATIONS IN ELECTRONIC FORM

- | | |
|--|---|
| Legal recognition of electronic records. | 3. No data message, electronic document, electronic record or other communication shall be denied legal recognition, effect, validity or enforceability on the ground that it is in electronic form. |
| Requirement for writing. | 4. Notwithstanding the fact that the provisions of written laws for the time being in force in Sri Lanka attach legal validity to certain instruments, only if such instruments have been reduced to writing, such requirement shall be deemed to be satisfied by a data message, electronic document, electronic record or other communication in electronic form if the information contained therein is accessible so as to be usable for subsequent reference. |
| Requirements for original form.
[4, 25 of 2017] | 5. (1) Where the law requires information to be presented or retained in its original form, that requirement shall be deemed to be satisfied by a data message, electronic document, electronic record or other communication in electronic form if there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form as a data message, electronic document, electronic record or communication or otherwise and the information contained in the data message, electronic document, electronic record or other communication is available and can be used for subsequent reference.

(2) For the purposes of subsection (1)- |

(a) the criterion for assessing the integrity of information, is whether such information has remained complete and unaltered, apart from the addition of any endorsement or any change which arises in the normal course of communication, storage or display; and

(b) the standard for reliability of the assurance shall be assessed having regard to the purpose for which the information was generated and all other relevant circumstances.

Requirements for retention.

6. The requirement under any law that information be retained, shall be deemed to be satisfied by the retention in electronic form of information contained in a data message, electronic document, electronic record or other communication notwithstanding the fact that such information was not originally generated in electronic form, if-

(a) the information in the data message, electronic document, electronic record or communication is accessible so as to be usable for subsequent reference ; and

(b) the data message, electronic document, electronic record or communication 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

(c) such information, enables the identification of the origin and destination of the data message, electronic document, electronic record or other communication and the date and time when such information was generated, sent or received, is retained :

Provided that the provisions of this section shall not apply to any information, which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

Legal recognition of electronic signatures.

[5, 25 of 2017]

7. Where any written law provides that a communication or any other document shall, be signed or bear the signature of any person, then notwithstanding anything to the contrary in such written law, that requirement shall be deemed to be met in relation to a data message, electronic document, electronic record or communication if-

(a) a method is used to identify that person and to indicate that person's intention in respect of the information contained in the electronic communication; and

(b) the method used is,

- (i) as reliable as appropriate for the purpose for which the electronic communication was generated, sent or communicated, in the light of all the circumstances, including any relevant agreement; or
- (ii) proven to have fulfilled the functions described in paragraph (a) by itself or together with further evidence.

Use of electronic records and electronic signatures in Government institutions and statutory bodies.
[6, 25 of 2017]

8. (1) Where any written law for the time being in force requires -

- (a) the filing of any form, application, or any other document with any Government department, office, body or agency owned or controlled by the Government or a statutory body in a particular manner;
- (b) the issue of grant of any license, certificate, permit or any other form of approval; or
- (c) the receipt of payment of money, procurement or other transaction to be effected in a particular manner,

then, notwithstanding anything to the contrary contained in any other written law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, creation, retention, issue, grant, receipt, payment, procurement or transaction, as the case may be, is effected in the form of electronic records, electronic document, data message or any electronic communication as may be specified by the relevant Ministry, Government department, Institution, statutory body or public corporation or other similar body.

(2) The relevant authority requiring the use of data message, electronic record, electronic document or electronic communication specified in subsection (1), may recommend the making of regulations for the purpose of authorizing or facilitating the use of such data message, electronic record, electronic document or electronic communication, to the Minister in charge of the subject, by specifying-

- (a) the manner and format in which such electronic records shall be filed, created, retained or issued ;
- (b) where such electronic documents or electronic records have to be signed, the type of electronic signature required ;
- (c) the manner and format in which such signature shall be affixed to the electronic documents or electronic records and the identity of, or the criteria which, a Certification Authority or Certification Service Provider used by such person filing the document should

possess ;

(d) the control process and procedures required in order to secure confidentiality, authenticity and integrity of electronic documents, records, procurements, transactions or payments ;

(e) the manner or method of payment of any fee or charges for the filing, creation, retention or issue of any electronic record under paragraph (a) ;

(f) the manner of doing anything which under any such provisions is required to be done as evidence in writing or otherwise using a document, notice or instrument ;

(g) the manner of doing anything which under any such provision, is required to be or which may be, done by post or other specified means of delivery ;

(h) the doing of anything which under any such provision is required to be, or which may be, authorized by a person's signature or seal ;

(i) the making of any statement or declaration which under any such provision is required to be made under oath ;

(j) the making of any payment that is required to be, or which may be, made under any such provision ;

(k) any other matter relating to electronic records or payments that are presently specified for the corresponding paper documents.

Publication in electronic forms of Gazette &c., deemed to be publication.

9. Where any Act or enactment provides that any Proclamation, rule, regulation, order, by-law, notification, or other matter shall be published in the Gazette, then such requirement shall be deemed to have been satisfied if such rule, regulation, order, by-law, notification or other matter is published in an electronic form of the Gazette.

Ministry, department, & etc, to accept or issue any document in electronic form.
[7, 25 of 2017]

10. Every ministry, department, institution, public corporation or other similar body may, subject to the provisions of this Act, accept or issue, any document in the form of data message, electronic record, electronic document or other communication in electronic form.

CHAPTER III ELECTRONIC CONTRACTS

Electronic

11. In the context of contract formation, unless otherwise agreed by the

Contracts. parties, an offer and the acceptance of an offer may be expressed in electronic form. A contract shall not be denied legal validity or enforceability on the sole ground that it is in electronic form.

Invitation to make offers. **11A.** 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 any information systems, shall 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.
[8, 25 of 2017]

Attribution of electronic records. 12.(1) Unless otherwise agreed as between an originator and the addressee, a data message, electronic document, electronic record or other communication shall be deemed to be that of the originator, if it was sent-

(a) by the originator himself ;

(b) by a person who had the authority to act for and on behalf of the originator in respect of that data message, electronic document, electronic record or other communication ; or

(c) by an automated information system programmed by, or on behalf of the originator.

(2) Unless otherwise agreed as between the originator and the addressee, the addressee is to regard a data message, electronic document, electronic record or other communication as being that of the originator, and is entitled to act on that assumption, if :-

(a) the addressee has no reason to doubt the authenticity of the data message, electronic document, electronic record or other communication ; or

(b) there do not exist any circumstances where the addressee knows, or ought to have known by exercising reasonable care, that the data message, electronic document, electronic record or other communication was authentic.

Acknowledgement of receipt. 13.(1) Where the originator has not agreed with the addressee that acknowledgement of receipt be given in a particular form or by a particular method, such an acknowledgement may be given by-

(a) any data message, electronic document, electronic record or other communication by the addressee, automated or otherwise;
or

(b) any conduct of the addressee, sufficient to indicate to the originator that the data message, electronic document, electronic record or other communication has been received.

(2) Where the originator has stipulated that data message, electronic document, electronic record or other communication shall be binding only on receipt of an acknowledgement of receipt of such data message, electronic document, electronic record or other communication by him, then, unless acknowledgement has been so received, the data message, electronic document, electronic record or other communication shall be deemed to have never been sent by the originator.

(3) Where the originator has not stipulated that the data message, electronic document, electronic record or other communication shall be binding only on receipt of such acknowledgement of receipt, and the acknowledgement of receipt had not been received by the originator within the time specified or agreed, or if no time has been specified or agreed to, within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgement of receipt has been received by him, and specifying a reasonable time by which the acknowledgement of receipt must be received by him and if no acknowledgement of receipt is received within the aforesaid time limit he may after giving notice to the addressee, treat the data message, electronic document, electronic record or other communication as though it has never been sent.

Time and place of
dispatch and
receipt of
electronic records.
[9, 25 of 2017]

14.(1) Unless otherwise agreed to between the originator and the addressee, the dispatch of a data message, electronic document, electronic record or other communication occurs when it leaves an information system under the control of the originator, or if the data message, electronic document, electronic record or other 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 data message, electronic document, electronic record or other communication is received.

(2)

(a) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message, electronic document, electronic record or other communication shall be determined as follows, namely-

(i) if the addressee has designated an electronic address for the purpose of receiving data message, electronic document, electronic record or other communication, time of receipt occurs at the time when the said data message, electronic document, electronic record or other communication becomes capable of being retrieved by the addressee; or

(ii) if the addressee has not designated an electronic address or has indicated another electronic address for the purpose of receiving data message, electronic document, electronic record or other communication, time of receipt occurs at the time when the said data message, electronic document, electronic record or other communication becomes capable of being retrieved by the addressee at that electronic address and the addressee becomes aware that the said data message, electronic document, electronic record or other communication has been sent to that electronic address.

(b) For the purpose of this subsection, a data message, electronic document, electronic record or other communication is presumed to be capable of being retrieved by the addressee when the said data message, electronic document, electronic record or other communication reaches the addressee's electronic address.

(3) Unless otherwise agreed between the originator and the addressee, the data message, electronic document, electronic record or other communication is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(4) The provisions of subsection (2) shall apply notwithstanding that the place where the information system is located may be different from the place where the data message, electronic document, electronic record or other communication is deemed to have been received under subsection (3).

(5) For the purposes of this section -

(a) if the originator or the addressee has not indicated a place of business or has more than one place of business, the place of business is that which has the closest relationship to the relevant contract, having regard to the circumstances known to or contemplated by the originator or the addressee before or at the conclusion of the contract;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(c) a location is not a place of business merely because-

(i) the equipment and technology supporting an information system used by a particular originator or the addressee in connection with the formation of a contract, are in that particular location; or

(ii) the information system may be accessed by addressee in that location;

(d) the fact that the originator or the addressee makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that the said originator or the addressee's place of business is located in that country;

(e) a party's place of business is presumed to be 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; and

(f) 'usual place of residence' in relation to a body corporate, means the place where it is registered.

Error in electronic communications.
[10, 25 of 2017]

14A. (1) Where a natural person in relation to the formation or performance of an electronic contract, makes an input error in an electronic communication exchanged with the automated message system of another party and the automated message system does not provide the person with an opportunity to correct the error, that 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-

(a) the 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

(b) the person, or the party on whose behalf that person was acting, has not used or received any material benefit or value from the goods and services, if any, received from the other party.

(2) Nothing in this section affects the application of any rule of law

that may govern the consequences of any error other than as provided for in subsection (1).

Variation by agreement.

15. The Minister may by regulation prescribe the matters which may be agreed to between the parties to such contract, involving the generating, sending, receiving, storing or otherwise processing of data messages, electronic documents, electronic records or other communication, in relation to the provisions of Chapter III.

Liability of Certification Service Providers.

16. (1) A Certification Service Provider shall not be subject to any civil or criminal liability for any transaction under this Act in respect of third party information in the form of data messages, electronic documents, electronic records or other communications to which he merely provides access, if such liability is founded, on -

- (a) the making, publication, dissemination, or distribution of such information or any statement made in such information ; or
- (b) the infringement of any rights subsisting in or in relation to such information.

(2) Nothing in this section shall effect-

- (a) any obligation founded on contract ;
- (b) the obligations of a Certification Service Provider providing such services under a licensing or other regulatory regime established under any written law ; or
- (c) any obligation imposed under any written law or by a court to remove, block or deny access to any information.

Avoidance of doubt.

17. For the avoidance of doubt it is hereby declared that-

- (a) if an offer and acceptance of an offer has been in whole or in part expressed by means of an electronic record, an electronic signature attached to, or logically associated with, such electronic record shall not be denied legal effect solely on the ground that it is with an electronic signature;
- (b) if an electronic communication is used in the formation of a contract, the contract shall not be denied validity or enforceability solely on the ground that an electronic record had been used for such purpose;
- (c) the accepted principles of common law relating to contracts that the offeror may prescribe the method of communicating acceptance, shall not be affected by anything contained in this

Chapter;

(d) a contract formed by the interaction of an automated message system and a natural person or by the interaction of automated message systems, shall not be denied validity or enforceability solely on the ground that there was no review or intervention by a natural person of the final contract or of each of the actions carried out by the automated message system.

CHAPTER IV
CERTIFICATION AUTHORITY AND CERTIFICATION OF SERVICE
PROVIDERS

- | | |
|---|--|
| Designation of a Certification Authority.
[11, 25 of 2017] | <p>18. (1) There shall be a Certification Authority designated by the Minister for the purposes of this Act in consultation with the Minister in charge of the subject of Information and Communication Technology.</p> <p>(2) In designating a Certification Authority the Minister may by Order published in the Gazette, designate any Government Department, Public Corporation, Statutory Body, Institution, or authority or any branch or unit thereof which shall be charged with the implementation of the provisions of this Act; the Minister shall in making the Order take into consideration the capacity of the Government Department, Public Corporation, Statutory Body, institution or authority to be designated in relation to its overall ability to discharge the obligations under this Act in ensuring the proper functioning of certification services by licensed or authorized Certification Service Providers.</p> |
| Minister to appoint the task forces.
[12, 25 of 2017] | <p>18A. The Minister shall, on the recommendation of the Secretary to the Ministry of the Minister, appoint a task force or a body of persons to manage and administer the Certification Authority, having regard to the qualifications and experience as well as the need to represent relevant stakeholders, with the objective of ensuring its proper administration.</p> |
| Powers of Certification Authority.
[13, 25 of 2017] | <p>19. The Certification Authority shall have the power to-</p> <p>(a) identify the criteria which will form the basis for licensing or authorization of Certification Service Providers and the qualifications required by them;</p> <p>(b) hear appeals and specify the procedure to be followed in the granting of a license or an authorization for the purposes of this Act;</p> |

(c) specify the procedure for the hearing of appeals in the event of a refusal to grant or renew a license or an authorization under section 20, as the case may be;

(d) issue licences or any other form of authorisation to Certification Service Providers to provide prescribed services;

(da) authorize Certification Service Providers to issue various types of electronic signatures in accordance with such criteria and guidelines as may be prescribed, including operational framework and security procedure for the use of biometric data and other authentication technologies for verification purposes;

(e) require Certification Service Providers to maintain such records and registers as may be prescribed;

(f) from time to time call for information as may be necessary from Certification Service Providers and issue directions to such Certification Service Providers.

Licensing or
authorizing the
Certification
Service Providers.
[14, 25 of 2017]

20.(1) A Certification Service Provider may be licensed or authorized by the Certification Authority in accordance with the criteria prescribed from time to time.

(2) Nothing in this Act shall be construed as impeding or in any way restricting the rights of any certification service provider to engage in the business of providing certification services without being licensed or authorized.

(3) Repealed.

CHAPTER V RULES GOVERNING EVIDENCE

Applicability of the
Rules of Evidence. 21.(1) Notwithstanding anything to the contrary in the Evidence Ordinance or any other written law, the following provisions of this section shall be applicable for the purposes of this Act.

(2) Any information contained in a data message, or any electronic document, electronic record or other communication -

(a) touching any fact in issue or relevant fact ; and

(b) compiled, received or obtained during the course of any business, trade or profession or other regularly conducted activity,

shall be admissible in any proceedings :

Provided that, direct oral evidence of such fact in issue or relevant fact if available, shall be admissible ; and there is no reason to believe that the information contained in a data message, or any electronic document, electronic record or other communication is unreliable or inaccurate :

Provided further that, for the purposes of paragraphs (a) and (b), if any information is contained in a data message, electronic document, electronic record or other communication made by a person-

(i) who is dead or who by reason of his bodily or mental condition is unfit to attend as a witness ; or

(ii) who is outside Sri Lanka and where reasonable steps have been taken to find such person and he cannot be found ; or

(iii) who does not wish to give oral evidence through fear ; or

(iv) who is prevented from so giving evidence,

evidence relating to such information shall, if available, be admissible.

(3) The Courts shall, unless the contrary is proved, presume the truth of information contained in a data message, or in any electronic document or electronic record or other communication and in the case of any data message, electronic document, electronic record or other communication made by a person, that the data message, electronic document or electronic record or other communication was made by the person who is purported to have made it and similarly, shall presume the genuineness of any electronic signature or distinctive identification mark therein.

Provisions of the Evidence (Special Provisions) Act, No. 14 of 1995 not to apply.

22. Nothing contained in the Evidence (Special Provisions) Act, No. 14 of 1995 shall apply to and in relation to any data message, electronic document, electronic record or other document to which the provisions of this Act applies.

CHAPTER VI MISCELLANEOUS

Restriction on application of the Act.
[15, 25 of 2017]

23. The provisions contained in this Act shall not apply to -

(a) the creation or execution of a will, or any other testamentary disposition by whatever name called;

(b) a license for a Telecommunication system issued under subsection (6) of section 17 of the Telecommunications Act, No.

25 of 1991;

(c) a Bill of Exchange as defined in subsection(1) of section 3 of the Bills of Exchange Ordinance (Chapter 82);

(ca) any financial matter in the nature of the following:-

(i) transactions on a regulated exchange;

(ii) foreign exchange transactions;

(iii) inter-bank payment systems, inter-bank payment agreements or clearance and settlement systems relating to securities or other financial assets or instruments; and

(iv) the transfer of security rights in sale, loan or holding of or agreement to repurchase securities or other financial assets or instruments held with an intermediary;

(d) a Power-of-Attorney as defined in section 2 of the Power of Attorney Ordinance (Chapter 122);

(e) a trust as defined in the Trusts Ordinance (Chapter 87) excluding a constructive, implied and resulting trust;

(f) a contract for sale or conveyance of immovable property or any interest in such property;

(g) or any other document act or transaction specified by the Minister by regulations made under section 24.

Regulations.
[16, 25 of 2017]

24.(1) The Minister may, in consultation with the Minister in Charge of the subject of Information and Communication Technology, make regulations in respect of any matter required or authorized by this Act to be made, or for the purpose of carrying out or giving effect to the objectives of this Act, as specified in section 2.

(2) In particular and without prejudice to the generality of the powers conferred by subsection (1), the Minister may make regulations for and in respect of all or any of the following matters :-

(a) specifying the electronic infrastructure and guidelines that are-

(i) sufficiently secure to meet the needs of Ministries, Government Departments, bodies or agencies owned and controlled by the Government, and Statutory bodies;

(ii) interoperable to the maximum extent possible;

(b) the conditions of service of the members of the Certification

Authority in relation to the implementation of the provisions of this Act;

(c) the powers, duties and functions of the Task Force or body of persons being appointed to manage and administer the Certification Authority in terms of section 18A and the other terms and conditions applicable to them;

(d) criteria for licensing or authorizing of certification service providers under section 20, its cryptography services, electronic signature or advance electronic signature and security procedures or any other legal consequences connected therewith;

(da) prescribe criteria and guidelines for Certification Service Providers to issue various types of electronic signatures, including the operational framework and security procedures for the use of biometric data and other authentication technologies for verification purposes;

(e) the procedure for appeals against refusal to grant or renew a license or an authorization;

(f) the qualifications required of persons seeking to provide certifications services;

(g) the procedure for the recognition of Certification Service Providers, the issue of licences to such Certification Service Providers and the categories of services required to be provided by them;

(h) the records to be maintained by the Certification Service Providers and the manner in which information has to be furnished to the Certification Authority by such Certification Service Provider; and

(i) the matters referred to in section 15.

(3) Every regulation made by the Minister shall be published in the Gazette and shall as soon as convenient after its publication in the Gazette be brought before Parliament for approval.

(4) Every regulation, which is not so approved, shall be deemed to be rescinded as from the date of such disapproval, but without prejudice to anything previously done thereunder.

(5) The date on which such regulations shall be deemed to be so rescinded shall be published in the Gazette.

prevail in case of inconsistency.

of this Act, the Sinhala text shall prevail.

Interpretation.
[17, 25 of 2017]

26.

For the purposes of this act, unless the context otherwise requires -

'addressee'

'addressee' means the person intended by the originator to receive the communication but does not include an intermediary;

'automated message system'

'automated message system' means a computer program or an electronic or other automated means used to initiate an action or respond to data messages or performances in whole or in part, without review or intervention by a natural person each time an action is initiated or a response is generated by the system;

'Certification Authority'

'Certification Authority' means the Certification Authority appointed in terms of Chapter IV of the Act;

'certification services'

'certification services' means any service which is provided to the senders or recipients of information in electronic form, or to those storing such information, and is designed to facilitate the use of cryptographic techniques for the purpose of ascertaining that the confidentiality, authenticity and integrity of such information is secured;

'Certification Service Provider'

'Certification Service Provider' means a person providing certification services within the meaning of this Act;

'communication'

'communication' means any statement, declaration, demand, notice or request, including an offer and the acceptance of an offer that a person is required to make or chooses to make in connection with an electronic transaction within the meaning of this Act;

'computer'

'computer' means an electronic or similar device having information processing

	capabilities;
'Convention'	'Convention' means the United Nations Convention on the Use of Electronic Communications in International Contracts ratified by Sri Lanka on July 7, 2015 subject to the declaration made at the time of ratification;
'data message'	'data message' means information generated, sent, received to stored by electronic, magnetic, optical or other similar means;
'electronic'	'electronic' means information generated, sent received or stored by electronic, magnetic, optical, or similar capacities regardless of the medium;
'electronic address'	'electronic address' means a communication network or an electronic mailbox, telecopy devise or a designated portion or location in an information system that a person uses to receive a data message, electronic document, electronic record or any communication;
'electronic communication'	'electronic communication' means any communication made by means of data message;
'electronic document'	'electronic document' includes documents, records, information, communications or transactions in electronic form;
'electronic record'	'electronic record' means a written document, or other record created, stored, generated, received, or communicated by electronic means;
'electronic signature'	'electronic signature' means data in electronic form, affixed to logically associated with a data message, electronic document, electronic record or communication which may be used to identify the signatory in relation to the data message, electronic document, electronic record or communication and to indicate the signatory's intention in respect of the information contained therein;

'information'	'information' includes text, message, data, voice, sound, database, video, signals, software, computer programs, including object codes and source codes;
'information system'	'information system' means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing information;
'intermediary'	'intermediary' means a person acting as a service provider on behalf of another person in relation to the sending, receiving, storing or processing of the electronic communication or the provision of other services in relation to it;
'Minister'	'Minister' means the Minister to whom the implementation of the provisions of Electronic Transactions Act, No. 19 of 2006 is assigned;
'network service provider'	'network service provider' means a person who owns, possesses, operates, manages or controls a public switched network or provides telecommunication services;
'originator'	'originator' of an electronic communication means a person by whom, or on whose behalf, the electronic communication has been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that electronic communication;
'prescribe'	'prescribe' means prescribe by regulations made under this Act;
'provides access'	'provides access' in relation to third-party information, means the provision of the necessary technical means by which third-party information may be accessed and includes the automatic and temporary storage of the third-party information for the purpose of providing access;
'security procedure'	'security procedure' means a procedure which in relation to a license or an authorization

issued by a certification service provider, is specified in its certification practice statement for establishing the authenticity or integrity, or both, of any electronic document, which may require the use of algorithms or codes, identifying words and numbers, encryption, answer back or acknowledgment procedures, software, hardware or similar security devices;

'third party'

'third party' in relation to a network service provider means a person over whom the provider has no effective control;