VARIOUS LEGAL ASPECTS OF EMAIL CONTRACTS

It is one of the theories of political science that the society and state is based on contract. If it is not true, then even the importance of contract cannot be denied at all. All groups, sects, associations etc are formed on the basis of like minded people on the basis of contract between two and more persons which subsequently establishes state or society. The law of contract is based on the natural principles of contract itself for contracting parties. In ancient India there was no specific law of contract as it appears today. All religious groups got there own law of contract. Hindu's were having Hindu law of Contract & Muslim's were governed by Muslim law of contract which was visible only after the advent of Mughal rule in India. The residuary parts of these laws are still available. The rule of Damdupat, among Hindu's is still applicable which prescribes that any money lender cannot recover amount of interest just double of the principle amount. When the British came & established there Kingdom in India, the principle's of English Law of Contract, under the garb of doctrine of equity justice & good conscience, were incorporated as a law of contract for Indians. The First Law Commission made best efforts to chalk out a proper law of contract for India, consequently on the recommendation of the first law commission 'Contract Act 1872' was passed to avoid the conflicting law of contract for different communities in India. Later on two chapters regarding sale of goods & partnership were separated from the original contract act and separate sale of goods act and partnership act were form. Presently Law of Contract is covered by contract act, sale of goods act, partnership act. Still these acts are working satisfactorily. The specific relief act is also a part of Law of Contract indirectly. Presently certain other acts have also been formed which are governing the law of contract today i.e. Forward Contract Regulation Act 1952, Hire Purchase Act 1972, Multi Modal Transportation of Goods Act 1993, Securities Contract Regulation Act 1956, Consumer Protection Act 1886, Recovery of Debt. due to Bank & Financial Institutions Act 1993 and various other claim tribunals such as railway claim tribunal, road transport tribunal etc.

Advancement of Science & Technology has changed the scenario of the world at large. It has affected every walk of life. The law of contract is exception to it. The present law of contract which is consisting roughly eleven enactments is proving insufficient, inefficient and traditional. It is unable to keep pace with time in society due to new technologies which are being used in the formation of contract. The Supreme Court although tried it all best to include every kind of technology in the present law of contract keeping in view the flexible language of the contract act. Although it is a fact that contract act has not contemplated such exigency but no where the contract has prohibited the use of such devices which was not feasible when the contract act was passed 135 years ago. Hidayatullah, C.J.I. convinced that through the law was framed at a time when telephones, wireless, Telstar and Early Bird were not contemplated, and the language of section 4 is flexible enough to cover telephonic communication. The courts should not completely ignore the language of the Act. When the word of acceptances is spoken into the telephone, they are put into the course of transmission to the offer or so as to be beyond the power of the acceptor. The acceptor cannot recall them.

The position deteriorated further. The present Law of Contract could not face the contracts based on new technologies such as email contracts and other contracts through electronic media & devices. The use of Computer & Internet is frequent now a days and present law has no provision to regulate the contracts based on these devices. The legislatures felt a strong need for a law regulating contract based on electronic devices. A survey was conducted which was headed by Justice Fazal Ali who strongly recommended for a separate law regulating contracts based on electronic devices. He refused to modify the present law of contract so as to include electronic devices into the preview of present law of contract. It was also noted that in future contracts and other commercial activities shall mostly be based on electronic devices due to its smoothness and fastness. Legislatures then decided to form a new law in this regard which was called 'Electronic Commerce Act 1998'. The act has overview of various foreign laws also. Maximum provisions of Singapore have been borrowed in the present act. Following Table will show us that how this act has borrowed provisions from foreign countries in this regard, it will also show how much references have been taken from foreign countries.

ABA Digital Signature Guidelines	*ABA Digital Signature Guidelines* (August 1, 1996), Information Security Committee, Electronic Commerce Division, Section of Science and Technology, American Bar Association, Chicago, Illinois, United States. Available online at *http://www.abanet.org/scitech/ec/isc/dsgfree.html.*
Florida Electronic Signature Act of 1996	Enacted 1996. Available online at *http://www.leg.state.fl.us/session/1996/senate/bills/billtext/html/billtext/sb0942.html.*
Illinois Electronic Commerce Security Act	Enacted 1998. Available online at *http://www.ag.state.il.us/resource/cecc/ceccact.html.*
Maine Criminal Code - Computer Crimes	Enacted 1989. Available online at *http://janus.state.me.us/legis/statutes/17a/title119.htm*
Malaysia Computer Crimes Act 1997	Enacted 1997. Available online at *http://www.cert.org.my/crime.html.*
Malaysia Digital Signature Act 1997	Enacted 1997. Available online at *http://www.cert.org.my/digital.html.*
Singapore Electronic Transactions Act	Enacted June 1998. Available online at *http://www.ec.gov.sg/policy.html.*
Texas Penal Code - Computer Crimes Statute	Enacted 1985 Available online at *http://www.med.uth.tmc.edu/ecs/statelaw.html.*
UCC Article 2B	National Conference of Commissioners on Uniform State Law, Uniform Commercial Code Draft Article 2B (August 1998 draft). Available online at *http://www.law.upenn.edu/ library/ulc/ucc2b/2b898.htm.*
UNCITRAL Model Law	United Nations Commission on International Trade Law ("UNCITRAL"), Model Law on Electronic Commerce, adopted December 16, 1996. Available online at *http://www.un.or.at/ uncitral/english/texts/electcom/ml-ec.htm.*
UNCITRAL Draft Rules	UNCITRAL Draft Uniform Rules on Electronic Signatures, July 10, 1998 draft. Available online at *http://www.un.or.at/ uncitral/english/sessions/wg_ec/index.htm.*
Uniform Electronic Transactions Act	National Conference of Commissioners on Uniform State Laws, Uniform Electronic Transactions Act (September 1998 draft). Available online at *http://www.law.upenn.edu/ library/ulc/ulc.htm#ueccta*
Utah Digital Signature Act	Utah Code Annotated, Title 46, Chapter 3 (originally enacted in 1995). Available online at *http://www.le.state.ut.us/ ~code/TITLE46/46_03.htm.*
United States Code	Available online at *http://law.house.gov/usc.htm.*

Sources

Section 2
(a)"Asymmetric cryptosystem" Source: ABA Digital Signature Guidelines 1.3.
(b) "Authentication" Source: ABA Digital Signature Guidelines 1.4.
(c) "Authorized officer" Source: Singapore Electronic Transactions Act 50.
(d) "Certificate" Source: ABA Digital Signature Guidelines 1.5.
(e) "Certification authority. Source: ABA Digital Signature Guidelines 1.6.
(f) "Certification practice statement" Source: ABA Digital Signature Guidelines 1.8.
(g) "Computer" Source: Malaysia Computer Crimes Act 2(1); Uniform Electronic Transactions Act 102(12)
(i) "Computer program" Source: Uniform Electronic Transactions Act 102.
(j) "Computer security system" Source: Texas Penal Code 33.01.
(k) "Computer virus" Source: Maine Criminal Code 431(9).
(l) "Controller" Source: Singapore Electronic Transactions Act 2.
(m) "Correspond" Source: ABA Digital Signature Guidelines 1.10;
(n) "Damage" Source: United States Code, 18 U.S.C. 1030.
(o) "Data" Source: Malaysia Computer Crimes Act 2.
(p) "Digital signature" Source: Singapore Electronic Transactions Act 2.
(q) "Electronic. Source: Illinois Electronic Commerce Security Act §5-105;
(r) "Electronic device" Source: Uniform Electronic Transactions Act 102(6)(September 1998 draft); UCC Article 2B 2B-102(19)(August 1998 draft).
(s) "Electronic record" Source: UNCITRAL Model Law, Article 2(a).
(t) "Electronic signature" Source: Singapore Electronic Transactions Act 2.
(u) "Hash function" Source: Singapore Electronic Transactions Act 2.
(v) "Information" Source: Singapore Electronic Transactions Act 2.
(w) "Information system Source: Uniform Electronic Transactions Act 102(12).
(y) "Key pair" Source: Singapore Electronic Transactions Act 2.
(z) "Network service provider" Source: United States Code, 47 U.S.C. 230(e).
(aa) "Operational period of a certificate" Source: Singapore Electronic Transactions Act.
(bb) "Private key" means the key of a key pair used to create a digital signature. Source: Singapore Electronic Transactions Act 2.
(dd) "Provide access" Source: Singapore Electronic Transactions Act 2.
(ee) "Public key" Source: Singapore Electronic Transactions Act §2;
(ff) "Record" Source: Singapore Electronic Transactions Act 2.
(gg) "Repository" Source: Singapore Electronic Transactions Act 2.
(hh) "Revoke a certificate" Source: Singapore Electronic Transactions Act 2.
(jj) "Security procedure" Source: Singapore Electronic Transactions Act 2.
(kk) "Signed" or "signature," . Source: Singapore Electronic Transactions Act 2.
(ll) "Subscriber" Source: Singapore Electronic Transactions Act 2.
(mm) "Suspend a certificate" Source: Singapore Electronic Transactions Act 2.
(nn) "Third party" Source: Singapore Electronic Transactions Act 10(3).
(oo) "Trustworthy system or manner" Source: Illinois Electronic Commerce Security Act 5-105; See ABA Digital Signature Guidelines 1.35.
(pp) "Valid certificate. Source: Singapore Electronic Transactions Act 2.
(qq) "Verify a digital signature" Source: Singapore Electronic Transactions Act 2.
3. Purpose and Construction. Source: Florida Electronic Signature Act of 1996 2;

4. Application. Source: Singapore Electronic Transactions Act §4; Illinois Electronic Commerce Security Act 5-115.
5. Variation by Agreement Source: UNCITRAL Model Law, Article 4; UCC Article 2B 2B-107(b); ABA Digital Signature Guidelines 2.2.
PART II - ELECTRONIC RECORDS AND SIGNATURES GENERALLY
6. Legal Recognition. Source: UNCITRAL Model Law, Article 5.
7. Requirements of Writing. Source: UNCITRAL Model Law, Article 6.
8. Electronic Signatures. Except as provided in Section 4, Source: UNCITRAL Model Law, Article 7. :
9. Original Record. Source: UNCITRAL Model Law, Article 8.
10. Admissibility and Evidentiary Weight of Electronic Records and Electronic Signatures. Source: UNCITRAL Model Law, Article 9.
11. Retention of Electronic Records. Source: UNCITRAL Model Law, Article 10; Illinois Electronic Commerce Security Act, Section 5-135.
PART III -- SECURE ELECTRONIC RECORDS AND SIGNATURES
12. Secure Electronic Record. Source: Singapore Electronic Transactions Act §16; Illinois Electronic Commerce Security Act §10-115; UCC Article 2B 115(b) (November 1, 1997 draft); ABA Digital Signature Guidelines 5.4.
13. Secure Electronic Signature. Source: Singapore Electronic Transactions Act 17.
14. Presumptions Relating to Secure Electronic Records and Signatures. Source: Singapore Electronic Transactions Act 18.
PART IV -- ELECTRONIC CONTRACTS
15. Formation and Validity. Source: UNCITRAL Model Law, Article 11; UCC Article 2B §2B-204.
16. Effectiveness Between Parties.. Source: UNCITRAL Model Law, Article 12; Singapore Electronic Transactions Act 12.
17. Attribution. Source: UNCITRAL Model Law, Article 13; Uniform Electronic Transactions Act §202; Illinois Electronic Commerce Security Act §306.
18. Acknowledgment of Receipt. Source: UNCITRAL Model Law, Article 14.
19. Time and Place of Dispatch and Receipt Source: UNCITRAL Model Law, Article 15.
20 .Applicable Law. laws as reflected in Section 28 of the Arbitration and Conciliation Act, 1996.
PART V -- EFFECT OF DIGITAL SIGNATURES
21. Secure Electronic Record with Digital Signature. Source: Singapore Electronic Transactions Act 19.
22. Digital Signature as a Secure Electronic Signature. Source: Singapore Electronic Transactions Act 20.
23. Unreliable Digital Signatures. Source: Singapore Electronic Transactions Act 22.
PART VI -- GENERAL DUTIES RELATING TO DIGITAL SIGNATURES
24. Foresee ability of Reliance on Certificates. Source: Singapore Electronic Transactions Act 23.
25. Prerequisites to Disclosure of Certificate. Source: Singapore Electronic Transactions Act 24.
26. Publication for Fraudulent Purpose. Source: Singapore Electronic Transactions Act 25.
27. False or Unauthorized Request. Source: Singapore Electronic Transactions Act 26.

On the basis of perusal of aforesaid provisions ‘Electronic Commerce Act 1998’ was passed to govern the electronic commercial activities. It was kept in view that all kinds of electronic activities which create contract, liabilities and rights should be covered by it. Email contract is also a most important electronic activity. These Email contracts are based on electronic devices i.e. internet & computers etc. Roughly I hope that these kinds of contracts are on rampant increase. As per an estimate today 70% of electronic activities regarding commercial transactions are covered by email contracts. It shall grow up further in future.

The rapid development of information and communication technologies over the past decade has revolutionized business practices. Transactions accomplished through electronic means - collectively "electronic commerce" - have created new legal issues. The shift from paper-based to electronic transactions has raised questions concerning the recognition, authenticity and enforceability of electronic documents and signatures. The challenge for lawmakers has been to balance the sometimes conflicting goals of safeguarding electronic commerce and encouraging technological development.

The Electronic Commerce Act of 1998 (the "Act") aims to facilitate the development of a secure regulatory environment for electronic commerce by providing a legal infrastructure governing electronic contracting, security and integrity of electronic transactions, the use of digital signatures and other issues related to electronic commerce.

The Act is divided into fifteen parts, which can be summarized as follows:

Part I of the Act outlines the general purpose of the Act, provides definitions for terminology used within the Act and defines the scope of the application of the Act.

Part II of the Act addresses *electronic records* and *electronic signatures* generally. It provides that, with limited exceptions, electronic records and signatures should be accorded the same treatment as paper records and signatures for purposes of complying with statutory writing, signature, evidentiary and record-keeping requirements.

Part III of Act addresses the integrity and authentication of *secure electronic records* and *secure electronic signatures*. Secure electronic records and signatures define specific categories of records and signatures that are afforded greater evidentiary presumptions because of their enhanced reliability and trustworthiness. The concept of a secure electronic record or a secure electronic signature will foster the growth of electronic commerce by providing businesses with assurances that records and signatures which meet the statutory definitions of "secure" records or signatures will be accorded the heightened evidentiary presumptions necessary to make business transactions effectively non reputable.

Part IV of the Act addresses issues of *electronic contracting*. This Part deals with the form in which an offer and an acceptance may be expressed and legal recognition of contracts formed in an electronic medium. This Part aims to provide increased legal certainty as to the conclusion of contracts by electronic means.

Parts V, VI, VII, VIII and IX of Act address the legal issues related to the use of *digital signatures.* Digital signature technology, which utilizes asymmetric cryptography technology, has been developed to facilitate secure transactions over the Internet and other computer networks. Although the electronic contracting sections of the Act have been drafted to be technologically neutral, Parts V-IX has been included to establish rules for the use of the most prominent current technology. Thus, a digital signature issued in accordance with Part V will be presumed to be a secure electronic signature.

Part X of the Act addresses the *acceptance and use of electronic records and electronic signatures by governmental entities*. This section authorizes any department or ministry to accept electronic filing of documents and to issue permits, licenses or approvals electronically. This section also empowers any department or ministry of the Government to specify the conditions and procedures for electronic filing or retention of documents. However, this section does not compel any department or ministry of the Government to accept or issue any document in electronic form if it does not wish to do so.

Part XI of the Act deals with issues relating to the *liability of network service providers*.
Part XII of the Act provides *criminal penalties* for intentional damage or destruction of information systems or data, intentional "trespass" into a system and intentional theft of computer services, tampering with data, interrupting network services and intentionally introducing viruses into computers or computer networks.
Part XIII of the Act contains *general provisions* relating to the use of electronic records.
The detailed provisions of the act are annexed herewith.

Conclusion

It is still a fact that the new electronic commerce act is governing various legal aspects of the Email contracts but the provisions of Indian Contract Act, Sales of Goods Act, Partnership Act and Specific relief Act, Forward Contract Regulation Act 1952, Hire Purchase Act 1972, Multi Modal Transportation of Goods Act 1993, Securities Contract Regulation Act 1956, Consumer Protection Act 1886, Recovery of Debt Due to Bank & Financial Institutions Act 1993 and various other claim tribunals such as railway claim tribunal, road transport tribunal etc cannot be ignored. I have to submit that the provisions of Electronic Commerce Act should be read with other laws governing contract as described by me here. It may be said that electronic commerce act is one of the specie of a great tree of Law of Contract covering various legislation. Electronic Commerce Act 1998 has laid down various legal aspects of the Email contracts by electronic devices like email etc. Section 15 to 20 prescribes the condition for formation of valid contract by such devices. This contract does not require signature. Section 6 to 12 of the aforesaid act prescribes the ground & essential ingredients of electronic contract. Delhi High Court recently in the case of Himachal Joint Venture vs. Pani Peena World Transport (Manu / DE / 002 / 2008) has described email contracts to be valid for all purposes. This case law has followed the earlier decision of Hon'ble Delhi High Court itself, in Ratna vs. Vasutech Ltd. (Manu / DE / 806 / 2007) and the verdict of Hon'ble Supreme Court in Citi Bank vs. TLC (Manu / SC / 3879 / 2007). The Hon'ble supreme court has also said in the case of Cable network vs. CNN (MANU / DE / 0022 / 2008) that in case of email contracts it is the duty of the parties to prove that everything is bonafied and genuine and nothing has been concealed and no fraud or any other kind of technical or electronic mistake has been committed.

Hence it is very clear that the law of Email contract is governed by the Electronic Commerce Act 1998 for the purposes mentioned in the act. Other purposes which have not been mentioned in the act are being covered by other ancillary enactments regarding law of contract i.e. Indian Contract Act, Sales of Goods Act, Partnership Act and Specific relief Act, Forward Contract Regulation Act 1952, Hire Purchase Act 1972, Multi Modal Transportation of Goods Act 1993, Securities Contract Regulation Act 1956, Consumer Protection Act 1886, Recovery of Debt. due to Bank & Financial Institutions Act 1993 and various other claim tribunals such as railway claim tribunal, road transport tribunal etc, looking into the relevancy of the facts whichever is applicable. It is also a fact that at present time the Electronic Commerce Act 1998 is at the stage of childhood under development. Future circumstances and other technological developments may suggest or compel us to add, remould, delete, modify or otherwise change any provision. These situations must be undertaken and studied minutely to thrash out a proper law relating to email contract and other electronic activities in future better than the present one.

A-1, Alkapuri, Sector C,
Aliganj, Lucknow.

(Dr. Gokulesh Sharma)
Ph.D.(Law), Judge

Annexure:

Electronic Commerce Act 1998.

An Act to establish the law relating to electronic commerce.
WHEREAS it is expedient to establish the law relating to electronic commerce;
It is hereby enacted as follows:--
PART I - PRELIMINARY
1. Short Title, Extent and Commencement.
(1) This Act may be called the Electronic Commerce Act, 1998.
(2) This Act extends to the whole of India, except the State of Jammu and Kashmir.
(3) This Act shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint in this behalf.
2. Definitions. In this Act, unless the context otherwise requires –
(a) "Asymmetric cryptosystem" means a computer-based system capable of generating and using a secure key pair, consisting of a private key for creating a digital signature and a public key to verify the digital signature.
Comments: Asymmetric cryptography is the core of the current digital signature technology. An asymmetric cryptosystem is an information system utilizing an algorithm or series of algorithms that provide for a cryptographic key pair consisting of a private key and the corresponding public key. A secure key pair is a key pair that is cryptographically strong and is capable of reliably creating and verifying digital signatures.
(b) "Authentication" means a process used to ascertain the identity of a person or the integrity of specific information. For a message, authentication involves ascertaining its source and confirming that it has not been modified or replaced in transit.
Comments: Authentication is necessary to determine the source and integrity of information. Authentication requires the verification that a record was sent by the sender and that the integrity of the record was not compromised. This concept has been added here to recognize the importance of determining the identity of the sender and the integrity of the contents of an electronic record in an electronic commerce transaction. Authentication is distinguishable from verification of a digital signature.
(c) "Authorized officer" means any officer that has been authorized by the Controller to exercise the powers of the Controller under this Act as identified in Section 41 of this Act.
Comments: An Authorized Officer will have the authority, if delegated by the Controller (as defined herein), to perform the duties and obligations of the Controller as specified herein.
(d) "Certificate" means a record, that at a minimum: (i) identifies the certification authority issuing it; (ii) names or otherwise identifies its subscriber, or a device or electronic agent under the control of the subscriber; (iii) contains a public key that corresponds to a private key under the control of the subscriber; (iv) specifies its operational period; and (v) is digitally signed by the certification authority issuing it.
Comments: A certificate binds a particular public key to a person that controls the corresponding private key. A certificate is used to identify the subscriber who actually controls the private key. A certificate usually helps the recipient of a digitally signed message attribute the digital signature to the sender by determining whether the public key and corresponding private key are identified with the signer. See Part VII and VIII of this Act for discussion of certificates in connection with the

use of digital signatures. A certificate must be signed by the certification authority issuing it so that the certificate may not be forged.

(e) "Certification authority" means a person who authorizes or causes the issuance of a certificate.

Comments: This definition expands on the definitions provided in the Singapore Electronic Transactions Act and others by regulating the process of issuance of certificates. The certification authority is responsible for issuing certificates for digital signatures to subscribers and for creating and digitally signing certificates. Once the certificate is issued by the certification authority, a representation is made as to the identity of the person named in the certificate and the binding of that person to a particular public-private key pair. See Part VII of this Act for discussion of certification authorities in connection with the use of digital signatures.

(f) "Certification practice statement" means a statement issued by a certification authority that specifies the policies or practices that the certification authority employs in issuing, managing, suspending and revoking certificates and providing access to them.

Comments: The certification practice statement generally takes the form of a declaration that the systems and procedures that it uses in creating certificates for digital signatures are trustworthy. These statements typically describe the types of procedures that a certification authority uses to verify an applicant's identity before it issues the certificate, the security measures used to protect cryptographic keys and the process that the certification authority takes to generate keys. See Part VII of this Act for discussion of certification practice statements in connection with the use of digital signatures.

(g) "Computer" means an electronic, magnetic, electromagnetic, digital, optical, or other information processing system or device used for creating, generating, transmitting, receiving, storing, displaying, or otherwise processing information, together with any supporting software, input, output, or data storage devices used therewith.

Comments: This definition is broader than other definitions found in similar acts in order to encompass the broadest range of apparatus used in electronic transactions. For example, facsimile machines, sophisticated telephone systems, telex and telegraph systems all are covered by this definition, in addition to the devices commonly known as computers. The definition also is intended to cover computer software and peripheral devices.

(h) "Computer network" means two or more computers in communication with or connected to each other.

Comment: This definition is intended to encompass the broadest range of computer interconnections that could be used in facilitating electronic transactions.

(i) "Computer program" means a set of instructions or statements, and related data, to be used directly or indirectly in a computer or computer network in order to cause a certain result.

(j) "Computer security system" means the design, procedures or other measures that the person responsible for the operation and use of a computer employs to restrict the use of the computer to particular persons or uses, or that the owner or licensee of data stored or maintained by a computer in which the owner or licensee is entitled to store or maintain the data employs to restrict access to or protect the confidentiality of the data.

(k) "Computer virus" means any computer instruction, information, data or program that degrades the performance of a computer; disables, damages or destroys a computer; or attaches itself to another computer and executes when the host computer program, data or instruction is executed or when some other event takes place in the host computer, data or instruction.

(l) "Controller" means the Controller of Certification Authorities appointed under Section 41.

Comments: The Controller of Certification Authorities shall be appointed by the Central Government to regulate and control operation of certification authorities. The duties of the Controller of Certification Authorities include licensing, certifying, monitoring and overseeing the activities of all certification authorities in India.

(m) "Correspond" in relation to private or public keys, means to belong to the same key pair.

Comments: In an asymmetric cryptosystem, two keys are said to "correspond" if one key can be used to encrypt a message and only the other key can be used to decrypt the message.

(n) "Damage" means any destruction, alteration, disruption, deletion, addition, modification or other impairment to the integrity or availability of a computer, data, electronic record, a program, an information system or information.

Comment: The definition of "damage" is based on the definition contained in the United States Computer Fraud and Abuse Act, but includes a wider range of categories of impairment of computer resources.

(o) "Data" means a representation of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer.

(p) "Digital signature" means an electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can accurately determine: (i) whether the transformation was created using the private key that corresponds to the signer's public key and (ii) whether the initial electronic record has been altered since the transformation was made.

Comments: A digital signature is a form of an electronic signature.

(q) "Electronic" includes electrical, digital, magnetic, optical, electromagnetic or any other form of technology that entails capabilities similar to these technologies.

Comments: This definition clarifies that this Act applies broadly to existing technologies, as well as any future technologies. It also is intended to make clear that the use of the term "electronic" is not to be taken so literally as to exclude certain technologies obviously intended to be covered but not literally "electronic" (i.e., information stored in magnetic form on a computer disk or information contained on a CD-ROM).

(r) "Electronic device" means a computer program or electronic record or other automated means configured or enabled by a person to independently initiate or respond to electronic records or performances on behalf of that person without review by an individual.

Comment: In the electronic marketplace, an increasing number of agreements are executed automatically through the use of electronic devices. Therefore, it is critical to include provisions governing formation of contracts through the use of electronic devices in the proposed legislation. The definition of electronic device contemplates transactions where one or both parties are represented by automated devices configured to respond to specific input and to carry out transactions on behalf of their human counterparts. Given the automated nature of such devices, of course, the law of agency should not apply to such devices.

(s) "Electronic record" means a record generated, sent, received or stored by electronic means for use in an information system or for transmission from one information system to another.

Comments: Electronic records include all messages sent by some electronic means. This definition can encompass computer-generated data records created for internal record-keeping purposes as well as communications to a third party.

(t) "Electronic signature" means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record.

Comments: This definition is included for purposes of clarity and also to expressly state the requirement that the electronic signature be attached to or logically associated with the electronic record. Since electronic records can be communicated separately from any tangible media on which they may exist, this definition requires that the signature must, in some way, be "attached to or logically associated with" the electronic record being signed.

(u) "Hash function" means an algorithm mapping or translating one sequence of bits into another, generally smaller, set (the hash result) such that: (i) a record yields the same hash result every time the algorithm is executed using the same record as input; (ii) it is not feasible that a record can be derived or reconstituted from the hash result produced by the algorithm; and (iii) it is computationally infeasible that two records can be found that produce the same hash result using the algorithm.

(v) "Information" includes data, text, images, sound, codes, computer programs, software, databases and the like.

Comments: The term "information" is technologically neutral but intended to include anything that can be transmitted in electronic or digital form.

(w) "Information system" means a system for creating, generating, sending, receiving, storing, displaying or otherwise processing information.

(x)"Internet" means a global network of interconnected computer networks, each using the transmission control protocol/internet protocol or any combination thereof or such other standard network interconnection protocols as is used to transmit data that is directly or indirectly delivered to a computer.

(y) "Key pair" in an asymmetric cryptosystem, means a private key and its mathematically related public key, having the property that the public key can verify a digital signature that the private key creates.

Comments: A key pair is normally generated by the person or entity that intends to use the key pair in order to digitally sign electronic records. A key pair includes a private key that is used to create a digital signature and a public key, which is used to verify digital signatures on messages sent by the holder of the corresponding private key.

(z) "Network service provider" means a person that provides the software, hardware, telecommunications facilities or any combination of the above, to facilitate access to the Internet or any other computer network, and includes a value added network service provider.

Comments: This Act includes a definition based on the definition of "interactive computer service" contained in the United States Code. The definition is drafted broadly enough to encompass operators of online services, Internet access providers, VANS, and those entities that provide the telecommunications facilities to permit access to the Internet.

(aa) "Operational period of a certificate" begins on the date and time the certificate is issued by a certification authority (or on a later date and time if stated in the certificate), and ends on the date and time it expires as stated in the certificate or is earlier revoked or suspended.

Comments: The operational period of a certificate is the period of its validity.

(bb) "Private key" means the key of a key pair used to create a digital signature.

Source: Singapore Electronic Transactions Act §2.

Comments: A private key is the secret key used to create a digital signature.

(cc)"Prescribed" means prescribed by rules made under this Act.

(dd) "Provide access" means, in relation to material provided by a third party, the provision of the necessary technical means by which such material may be accessed and includes the automatic and temporary storage of such material for the purpose of providing access.

(ee) "Public key" means the key of a key pair used to verify a digital signature.

Comments: The public key is usually provided via a certificate issued by a certification authority and is used to verify the digital signature of a message purportedly sent by the holder of the corresponding private key.

(ff) "Record" means information that is inscribed, stored or otherwise fixed in a tangible medium or that is stored in an electronic or other intangible medium and may be retrieved in perceivable form.

(gg) "Repository" means a system for storing and retrieving certificates or other information relevant to certificates, including information related to the status of a certificate.

Comments: A repository is a collection of information related to issue certificates stored by the certification authority or another person. The repository may contain the certificates accepted by subscribers and any other necessary information.

(hh) "Revoke a certificate" means to permanently end the operational period of a certificate from a specified time forward.

Comments: A certificate may be revoked prior to the end of the operational period. Once a certificate is revoked, its effectiveness is terminated.

(ii) "Rule of law" includes any provision contained in an enactment or any rule derived from any other source of law.

(jj) "Security procedure" means a procedure for the purpose of: (i) verifying that an electronic record is that of a specific person or (ii) detecting error or alteration in the communication, content or storage of an electronic record since a specific point in time. A security procedure may require the use of algorithms or codes, identifying words or numbers, encryption, answer back or acknowledgment procedures, or similar security devices.

Comments: This definition does not attempt to define security procedure in terms of any specific technology, and recognizes that there are a variety of technologies in place today, as well as new technologies that will be developed in the future, that may qualify as appropriate security procedures.

(kk) "Signed" or "signature," in relation to electronic records, includes any symbol executed or adopted, or any security procedure employed or adopted, using electronic means or otherwise, by or on behalf of a person with the intent to authenticate such record.

Comments: This definition of the terms "signed" and "signature" has the effect of: (1) extending to the electronic medium the traditional paper-based definition of "signed" and (2) recognizing that a signature can be created both through the use of a symbol as well as through the use of a security procedure.

(ll) "Subscriber" means a person who is the subject named or identified in a certificate issued, who holds a private key that corresponds to a public key listed in that certificate and who is the person to whom digitally signed messages verified by reference to such certificate are to be attributed.

Comments: The subscriber is the person named or otherwise identified in a certificate. Note that a person who digitally signs an electronic record, but who has not been issued a certificate, is not a subscriber, even though such person is using a digital signature.

(mm) "Suspend a certificate" means to temporarily suspend the operational period of a certificate from a specified time forward.

Comments: Suspension of a certificate involves a temporary termination of its effectiveness prior to the end of its stated operational period.

(nn) "Third party" means, in relation to a network service provider, a person over whom the provider has no effective control.

(oo) "Trustworthy system or manner" means the use of, or adoption of any device involving the use of, computer hardware, software and procedures that, in the context in which they are used: (i) can be shown to be reasonably resistant to penetration, compromise and misuse; (ii) provide a reasonable level of reliability and correct operation; (iii) are reasonably suited to performing their intended functions or serving their intended purposes; (iv) comply with applicable agreements between the parties, if any; and (v) adhere to generally accepted security procedures

Comments: The term "trustworthy system or manner" is intended to define a general yet flexible standard, recognizing that computer security is a matter of degree and depends upon the circumstances. This definition focuses on a variety of different aspects of the trustworthiness of an information system, including (1) security from intrusion and misuse; (2) reliability and correct operation; (3) suitability to performing intended functions or purposes; (4) compliance with applicable agreements of the parties; and (5) adherence to generally accepted security procedures. The manner in which a system is configured to achieve the objectives of trustworthiness will vary depending on the type of technology available.

(pp) "Valid certificate" means a certificate that a certification authority has issued and that the subscriber listed in the certificate has accepted.

(qq) "Verify a digital signature" means to use a public key listed in a valid certificate to determine: (i) that the digital signature was created using the private key corresponding to the public key listed in the certificate and (ii) the electronic record has not been altered since its digital signature was created.

3. Purpose and Construction.

This Act shall be construed consistently with what is commercially reasonable under the circumstances and to effectuate the following purposes:

(a) To facilitate electronic communications by means of reliable electronic records;

(b) To facilitate and promote electronic commerce, to eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce;

(c) To facilitate the electronic filing of documents with government agencies and statutory corporations, and to promote efficient delivery of government services by means of electronic records;

(d) To minimize the incidence of forged electronic records, intentional and unintentional alterations of records, and fraud in electronic commerce and other electronic transactions;

(e) To promote public confidence in the integrity and reliability of electronic records, electronic signatures and electronic commerce;

(f) To establish uniform rules and standards regarding the authentication and integrity of electronic records; and

(g) To create a legal infrastructure for the use of digital signatures.

Comments: This Act aims to remove actual and perceived barriers to electronic commerce and to set forth a legal framework to promote and facilitate the development of electronic commerce. It seeks to remove barriers by clarifying existing uncertainty over whether electronic records are "writings" or "signatures" or "records" for legal purposes. To promote electronic commerce, this

Act provides for recognition of a class of electronic records known as "secure" electronic records and signatures. Secure electronic records and signatures are afforded higher evidentiary presumptions to provide parties engaged in electronic commerce assurance that their transactions are enforceable. In addition, this Act addresses evidentiary concerns as to the admissibility of electronic records. The Act presents a logical and coherent approach to resolving issues raised by electronic commerce and, where possible, seeks to preserve uniformity among the approaches to electronic commerce legislation taken by various countries.

4. Application.

(a) Parts II or IV of this Act shall not apply to any law requiring writing or signatures in any of the following circumstances:

(1) the creation or execution of a will;

(2) the execution of negotiable instruments;

(3) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney with the exception of constructive and resulting trusts;

(4) any contract for the sale or other disposition of immovable property, or any interest in such property;

(5) the conveyance of immovable property or the transfer of any interest in immovable property;

(6) documents of title for movable or immovable property; or

(7) where such application would involve a construction of a rule of law that is clearly inconsistent with the manifest intent of the lawmaking body or repugnant to the context of the same rule of law, provided that the mere requirement that information be "in writing," "written" or "printed" shall not by itself be sufficient to establish such intent.

(b) The Central Government may modify in the public interest, by notification published in the Official Gazette, the provisions of section (a) by adding, deleting or amending any class of transactions or matters specified in that section.

(c) In relation to this Act, electronic records shall not be liable to stamp duty under the Stamp Act, 1899.

(d) Notwithstanding anything contained in the Telegraph Act, 1885, or rules made under this Act, it shall be lawful to transmit and receive records electronically.

Comments: It is not feasible to give broad legal recognition to all documents that are signed with an electronic signature because, under Indian Law, hand written signatures are more appropriate for certain categories of agreements. Therefore, the purpose of limiting application of this Act is to acknowledge the intent of relevant laws that mandate the use of pen and ink for some documents. For example, in the case of negotiable instruments, the current state of technology does not adequately provide a reliable mechanism for the transfer or negotiation of electronic records to holders in due course beyond an originator and an initial recipient of the electronic record. Additionally, this section provides authority to the Central Government to amend, as appropriate, the limitations set forth in this section. Further, the application of the Stamp Act has been limited to recognize the intangible nature of electronic records, based upon precedent set in the Depositories Act, 1996. The applicability of the Telegraph Act also has been limited in recognition of the necessity to encrypt data in relation to the transmission of certain types of secure electronic records.

5. Variation by Agreement. As between parties involved in generating, sending, receiving, storing or otherwise processing electronic records, any provision of Part II or IV of this Act may be varied by agreement of the parties.

Comments: This section states the general principle that parties may vary the provisions of Parts II or IV by agreement. Thus, where the signer and the recipient of an electronic record, agree to the terms of a contract, the rules set forth in this Act may be varied by a contract between the parties.

PART II - ELECTRONIC RECORDS AND SIGNATURES GENERALLY

6. Legal Recognition. Except as provided in Section 4 of this Act, records and signatures shall not be denied legal effect, validity or enforceability solely on the ground that they are in electronic form.

Comments: This section sets forth the fundamental principle that electronic records and electronic signatures should not be denied legal recognition or evidentiary weight solely by virtue of the medium chosen.

7. Requirements of Writing. Except as provided in Section 4, where any rule of law requires any matter to be in writing, that requirement sufficiently is met by an electronic record if the matter contained therein is accessible so as to be usable for subsequent reference.

Comments: Statutes and regulations frequently require that certain documents must be "written" or "in writing." The principle of requiring agreements to be memorialized in writing has presented obstacles for electronic transactions. Traditionally, the use of "writings" in a paper-based environment: (1) ensures that there would be tangible evidence of the existence and nature of the intent of the parties to bind themselves; (2) fosters awareness of the consequences of entering into a contract; (3) provides a permanent, unaltered record of a transaction; (4) allows for the reproduction of a document so that each party would hold a copy of the same date; (5) serves as an indicator of the final intent of the author of the "writing" and provides a record of that intent; (6) permits the storage of data in a tangible form; and (7) brings into existence legal rights and obligations in those cases where a "writing" was required for validity purposes. The focus of this section as it relates to electronic transactions is to legally recognize the use of electronic "writings" through e-mail, EDI, the Internet and other electronic records transmitted over networks in electronic contracting.

8. Electronic Signatures. Except as provided in Section 4, where any rule of law requires that a record bear a signature, or provides for certain consequences if a record is not signed, an electronic signature satisfies that rule of law if:

(a) a method is used to identify the originator and to indicate the originator’s approval of the information contained in the electronic record; and

(b) that method is as reliable as was appropriate for the purpose for which the electronic record was generated or communicated, in light of all of the circumstances, including any relevant agreements among the parties involved.

Comments: This section clarifies existing law by expressly stating that, except for limited delineated exceptions, electronic signatures meet legal signing requirements wherever they exist. It is intended to remove any doubt regarding the enforceability of electronic signatures. In a paper-based environment, written signatures acknowledge the signer’s identity and his or her intent to be bound by the terms in the signed agreement. In addition, signed writings serve several practical purposes such as 1) calling the signer’s attention to the legal significance of the signer’s act; 2) expressing the signer’s approval or authorization of the writing; and 3) allowing the document to become attributable to the signer.

With today’s technological developments, open networks such as the Internet are overtaking the traditionally closed environment of paper-based transactions, and communication among parties without previous contacts is commonplace. In this context, the ability to authenticate messages or to ascertain the identity of the author is difficult. Therefore, many fear that business transactions over open networks lack the security and reliability of paper-based equivalents.

This section also addresses the issues of authentication and identification. It focuses on two basic functions of a signature: 1) it establishes the principle that, in an electronic environment, the basic legal functions of a signature are performed by way of a method that identifies the originator of the electronic record and 2) confirms that the originator approved the content of the electronic record. This section may be regarded as establishing a basic standard of authentication for electronic records that might be exchanged in the absence of a prior contractual relationship and, at the same time, to provide guidance as to what might constitute an appropriate substitute for a signature if the parties used electronic communications in the context of an agreement. This provision represents a comprehensive approach to resolving the issue of determining the authenticity and integrity of the electronic signatures. This section follows the UNCITRAL model for establishing criteria that sets forth a method for identifying the author and confirming that the author approved of the contents of the electronic document. The language is broad enough to encompass different methods and technologies and focuses on the issue of reliability.

9. Original Record.

(a) Where a rule of law requires a record to be presented or retained in its original form, that requirement is met by an electronic record if:

(i) there exists reliable assurance as to the integrity of the record from the time when it was first generated in its final form, as an electronic record or otherwise; and

(ii) where it is required that a record be presented, that record is capable of being displayed to the person to whom it is being presented.

(b) Subsection (a) applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the record not being presented or retained in its original form.

(c) For the purposes of subsection (a)(i):

(i) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(ii) the standard of reliability required shall be assessed in light of the purpose for which the information was generated and in light of all the relevant circumstances.

Comments: Section 9 addresses rules of law that require documents to be in original form for purposes of ensuring document integrity. It provides that an electronic record (whether or not signed) will constitute an original, provided that there exists a reliable assurance as to the integrity of the information. In a paper-based environment some contract documents are accepted only in original form. This section removes the possibility of parties being forced to use paper documents to complete a transaction by making an electronic record the functional equivalent to a paper original. This section is intended to show that an electronic record will be considered an original so long as it meets the authenticity and reliability requirements set forth in Section 9(c).

10. Admissibility and Evidentiary Weight of Electronic Records and Electronic Signatures.

(a) Nothing in the Indian Evidence Act, 1872 or any rules made under this Act shall apply in any legal proceedings so as to deny the admissibility of an electronic record or an electronic signature into evidence:

(i) on the sole ground that it is an electronic record or an electronic signature; or

(ii) on the grounds that it is not in its original form or is not an original.

(b) Information in the form of an electronic record shall be given due evidentiary weight without regard to the fact that it is an electronic record. In assessing the evidentiary weight of an electronic record or an electronic signature, regard shall be given to:
(i) the reliability of the manner in which it was generated, stored or communicated;
(ii) the reliability of the manner in which its integrity was maintained;
(iii) the manner in which its originator was identified or the electronic record was signed; and
(iv) any other factor that may be relevant.
(c) Nothing in this section shall be construed to affect the provisions of Section 4 of this Act.
Comments: The purpose of this section is to establish the principle that electronic records and electronic signatures should be admissible as evidence in legal proceedings. In addition, this section sets forth a standard for determining the evidentiary weight of electronic records and electronic signatures. It is important to recognize that electronic records and electronic signatures can be used in legal proceedings because such legal recognition removes any legal uncertainty that may occur in disputes over electronic transactions. This section does not establish the requirements for the admissibility of electronic records or electronic signatures into evidence. Rather, it simply provides that a court cannot refuse to admit an electronic record or electronic signature into evidence solely on the ground of its electronic format or on the ground that it is not an original. This section does not, however, mandate the admissibility of an electronic record or an electronic signature in the event of other proper objections such as relevance or lack of authenticity. It merely mirrors the fundamental principle expressed in Section 6 that electronic records should not be discriminated against solely on the nature of the medium chosen.
11. Retention of Electronic Records.
(a) Where any law for the time being in force requires that certain documents, records or information be retained, whether permanently or for a specified period, that requirement is satisfied by retaining them in the form of electronic records if the following conditions are fulfilled:
(i) the electronic record and the information contained therein remains accessible so as to be usable for subsequent reference;
(ii) the electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received; and
(iii) such information as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, if any, is retained.
(b) An obligation to retain documents, records or information in accordance with subsection (a) shall not extend to any data the sole purpose of which is to enable the record to be sent or received.
(c) It shall be lawful for a person to satisfy the retention requirement referred to in Section 11(a) by using the services of any other person, if the conditions in Sections 11(a)(i) through (iii) are complied with.
(d) Nothing in this section shall preclude any department or ministry of the Central Government, State Government or a statutory corporation under Central or State Government from specifying additional requirements for the retention of electronic records that are subject to its jurisdiction.
Comments: This section sets forth the basic rules regarding the retention of electronic records. It applies to the retention of records that originally exist in electronic form, as well as to the electronic retention of records that originally exist in paper form or on other tangible media. This section also makes it clear that the standards set forth here are minimum standards only; it does

not preclude a government agency from establishing additional requirements for the retention of records required under the regulations of that agency.

PART III -- SECURE ELECTRONIC RECORDS AND SIGNATURES

12. Secure Electronic Record.

(a) If a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved has been applied to an electronic record in a trustworthy manner and has been relied upon reasonably and in good faith by the relying party to verify that the electronic record has not been altered since a specified point in time, such record shall be treated as a secure electronic record from such specified point in time to the time of verification.

(b) For the purposes of this Section 12 and of Section 13, whether a security procedure is commercially reasonable shall be determined in light of the procedure used and the commercial circumstances prevailing at the time the procedure was used, including:

(i) the nature of the transaction;

(ii) the sophistication of the parties;

(iii) the volume of similar transactions engaged in by the parties involved;

(iv) the availability of alternatives offered to but rejected by any party;

(v) the cost of alternative procedures; and

(vi) the procedures in general use for similar types of transactions.

(c) Whether reliance on a security procedure was reasonable and in good faith shall be determined in light of all the circumstances known to the relying party at the time of the reliance, with regard to:

(i) the information that the relying party knew or should have known of at the time of reliance that would suggest that reliance was or was not reasonable;

(ii) the value or importance of the electronic record, if known:

(iii) any course of dealing between the relying party and the purported sender and the available indicia of reliability or unreliability apart from the security procedure;

(iv) any usage of trade, particularly trade conducted by trustworthy systems or other computer-based means; and

(v) whether the verification was performed with the assistance of an independent third party. Comments: This section sets forth the criteria that must be satisfied for an electronic record to qualify as a "secure" electronic record in a technologically neutral manner. Records that qualify as secure electronic records are accorded the presumptions set forth in Section 14.

This section attempts to balance the risk of loss between the sender and recipient of an electronic record, with the recipient bearing the burden of proof with respect to evidence or information that is available to or under the control of the recipient. This includes an evaluation of whether the security procedure is commercially reasonable under the circumstances, of whether the security procedure was implemented by the relying party in a trustworthy manner and, finally, of whether the security procedure was implemented and relied upon by the relying party reasonably and in good faith. This latter point takes into account the fact that if the relying party has knowledge indicating that reliance on the security procedure is not appropriate, the relying party should be charged with it and should not be able to rely on a security procedure that it knows may be unreliable. Once this burden is met by the recipient of an electronic record, Section 14 gives rise to a rebuttable presumption that the electronic record has not been altered, and imposes upon the purported sender the burden of going forward with evidence to rebut the presumption. The relying party is deemed to be responsible for information and events that are under its control.

In order for an electronic record to be deemed secure it must be possible to verify the integrity of the record through:

(1) A qualified security procedure

(2) that is commercially reasonable under the circumstances

(3) that is implemented in a trustworthy manner

(4) and relied upon reasonably and in good faith.

Because no single security procedure is sufficient for all situations, commercial reasonableness, trustworthy implementation and good faith by the relying party are all relevant factors to be considered, even with the strongest of security procedures in place.

By tying secured the electronic record to the "time of verification", this section recognizes that the fact that an electronic record is verified by a security procedure and qualified as a secure electronic record at a particular point in time does not necessarily ensure that it will be a secure electronic record indefinitely into the future. This section thus contemplates that the electronic record will be subjected to the appropriate qualified security procedure to verify the integrity of the electronic record not only when it is necessary to act on the record--but also at such later time when it may be necessary to establish the integrity of the electronic record, such as in court.

13. Secure Electronic Signature. If, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, an electronic signature is executed in a trustworthy manner and reasonably and in good faith is relied upon by the relying party, such signature shall be treated as a secure electronic signature at the time of verification to the extent that it can be verified that said electronic signature satisfied, at the time it was made, the following criteria:

(a) it was unique to the person using it;

(b) it was capable of being used to objectively identify such person;

(c) it was created in a manner or using a means under the sole control of the person using it, that cannot be readily duplicated or compromised; and

(d) it is linked to the electronic record to which it relates in a manner such that if the record was changed to electronic signature would be invalidated.

Comments: This section sets forth the criteria for an electronic signature to qualify as a secure electronic signature in a technologically neutral manner. Signatures that qualify as a secure electronic signature are qualified for the evidentiary presumptions set forth in Section 14. See Comments to Section 14.

The security procedure must satisfy four criteria before it can be deemed a prescribed security procedure:

(1) Uniqueness: This requirement is intended to ensure that there is no reasonable likelihood that more than one person would produce the same signature absent fraud or other inappropriate conduct.

(2) Objective Identification: This requirement is intended to ensure that a reasonable person could identify the author of the electronic signature.

(3) Reliability: There must be reasonably reliable assurance that the person identified as the signer is the person who signed the electronic record, and that the signature was not altered after it was made.

(4) Linkage to Record Signed: A secure signature must be both created and linked to the electronic record being signed in a manner such that the fact of such alteration would be disclosed if either the record or the signature is altered after the signature is made.

14. Presumptions Relating to Secure Electronic Records and Signatures.

(a) In any civil proceedings involving a secure electronic record, it shall be presumed, unless the contrary is proved, that the secure electronic record has not been altered since the specific point in time to which the secure status relates.

(b) In any civil proceedings involving a secure electronic signature, the following shall be presumed unless the contrary is proved:

(i) the secure electronic signature is the signature of the person to whom it correlates: and

(ii) the secure electronic signature was affixed by that person with the intention of signing or approving the electronic record.

(c) In the absence of a secure electronic record or a secure electronic signature, nothing in this Part shall create any presumption relating to the authenticity and integrity of the electronic record or an electronic signature.

(d) The effect of presumptions provided in this section is to place on the party challenging the integrity of a secure electronic record or challenging the genuineness of a secure electronic signature both the burden of going forward with evidence to rebut the presumption and the burden of persuading the Trier of fact that the nonexistence of the presumed fact is more probable than its existence.

(e) For the purposes of this section:

(i) "secure electronic record" means an electronic record treated as a secure electronic record by virtue of Sections 12 or 21; and

(ii) "secure electronic signature" means an electronic signature treated as a secure electronic signature by virtue of Sections 13 or 22.

Comments: The concepts of a secure electronic record and a secure electronic signature, and the rebuttable presumptions that flow from that status, are necessary for a viable system of electronic commerce. In the context of electronic commerce, none of the usual indicia of reliability present in a paper-based transaction (the use of watermarked paper, letterhead, etc.) exist, making it difficult to know when one can rely on the integrity and authenticity of an electronic record. This lack of reliability can make proving one’s case in court virtually impossible. Rebuttable presumptions with respect to secure records and secure signatures put a relying party in a position to know, at the time of receipt and/or reliance, whether the message is authentic and the integrity of its contents intact and, equally important, whether it will be able to establish both of these facts in court in the event of subsequent disputes.

Section 14(d) makes clear that the effect of the presumptions is to allocate both the burden of going forward with the allegations and evidence, as well as the ultimate burden of persuasion, to the party challenging the integrity of a secure electronic record or challenging the genuineness of a secure electronic signature. These presumptions apply only in the context of a civil dispute, not a criminal matter.

The presumption in Section 14(b) is not a presumption that the electronic record constitutes a legally binding obligation. That will be determined by the text of the record and the circumstances surrounding its execution. This section presumes only that the secure electronic signature affixed to an electronic record is the signature of the person objectively identified as the signer by application of the applicable qualified security procedure. If there is evidence that the person whose signature was affixed was the victim of mistake, misrepresentation, duress or other invalidating cause, the record may be denied legal effect, but the burden of raising these issues is on the person denying the legal effect of the record.

PART IV -- ELECTRONIC CONTRACTS

15. Formation and Validity.

(a) In the context of the formation of contracts, unless otherwise agreed by the parties involved, an offer and the acceptance of an offer may be expressed by means of electronic records.

(b) Where an electronic record is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that an electronic record was used for that purpose.

(c) A contract may be formed by the interaction of electronic agents. A contract is formed if the interaction results in the electronic agents' engaging in operations that confirm or indicate the existence of a contract.

(d) A contract may be formed by the interaction of an electronic agent and an individual. A contract is formed if the individual has reason to know that the individual is dealing with an electronic agent and the individual takes actions or makes a statement that the individual has reason to know will cause the electronic agent to perform the subject of the contract, or instruct a person or electronic agent to do so.

Comment: This section adopts the basic rule that offer and acceptance may be accomplished through the use of electronic exchange. There are a number of additional contractual issues that may arise, including acceptance that varies from the terms of an offer, and cases where an offer is made electronically and accepted in writing (or vice versa). The Act adopts a more general approach, simply giving recognition to electronic records as a means of forming a contract. This section also includes provisions governing the formation of contracts through the use of electronic agents, providing that enforceable agreements may be formed through the use of electronic agents.

16. Effectiveness Between Parties. As between the originator and the addressee of an electronic record, a declaration of intent or other statement shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.

Source: UNCITRAL Model Law, Article 12; Singapore Electronic Transactions Act §12.

Comments: This provision is included in order to establish the principle that in electronic contracts, the use of electronic communication should not be discriminated against. Expressions of will or intent issued in electronic form should be equally valid as written statements of this kind.

17. Attribution.

(a) An electronic record is that of the originator if it was sent by the originator himself.

(b) As between the originator and the addressee, an electronic record is deemed to be that of the originator if it was sent:

(i) by a person who had the authority (pursuant to a document in a non-electronic form) to act on behalf of the originator in respect of that electronic record; or

(ii) by an information system programmed by or on behalf of the originator to operate automatically.

(c) As between the originator and the addressee, an addressee is entitled to regard an electronic record as being that of the originator and to act on that assumption if:

(i) in order to ascertain whether the electronic record was that of the originator, the addressee properly and in good faith applied a procedure previously agreed to by the originator for that purpose; or

(ii) the data message as received by the addressee resulted from the actions of a 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 electronic records as its own.

(d) Section 17(c) shall not apply:

(i) from the time when the addressee has both received notice from the originator that the electronic record is not that of the originator, and had reasonable time to act accordingly;
(ii) at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the electronic record was not that of the originator; or
(iii) if in all the circumstances of the case, it is unconscionable for the addressee to regard the electronic record as that of the originator or to act on that assumption.
(e) Where an electronic record is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the electronic record received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when 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 electronic record as received.
(f) The addressee is entitled to regard each electronic record received as a separate electronic record and to act on that assumption, except to the extent that the addressee duplicates the electronic record or the addressee knew or should have known, had the addressee exercised reasonable care or used any agreed procedure, that an electronic record received from the originator was a duplicate.
(g) Nothing in this section shall affect the law of agency or the law on the formation of contracts.
Comments: This section sets forth the basic rules that apply in cases where there is a question about the origin of an electronic record and the recipient's ability to rely upon that record. In an electronic environment, it can be difficult to ascertain who is the originator of an electronic record and if, in fact, the originator is the person that the recipient believes him to be. This section provides a framework for attributing electronic records to specific persons.
In general, a person is bound by any electronic record he or she sends or by any transmission sent by an agent on behalf of that person. Additionally, under certain circumstances specified in this section, a recipient may lawfully regard an electronic record as originating from another specific individual, regardless of whether that specific individual actually is the originator, unless doing so would be unreasonable or unconscionable or the recipient knew or should have known that the electronic record did not come from the specified individual. However, an originator can disavow an electronic record once it has been sent, and not be held responsible for any reliance on such a record by the recipient, as of the time that the disavowal is received by the addressee and the recipient has had reasonable time to act accordingly.
18. Acknowledgment of Receipt.
(a) Sections 18(b), (c) and (d) shall apply where, on or before sending an electronic record, or by means of that electronic record, the originator has requested or has agreed with the addressee that receipt of the electronic record be acknowledged.
(b) Where the originator has not agreed with the addressee that the acknowledgment be given in a particular form or by a particular method, an acknowledgment may be given by:
(i) any communication by the addressee, automated or otherwise; or
(ii) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.
(c) Where the originator has stated that the electronic record is conditional on receipt of the acknowledgment, the electronic record is treated as though it had never been sent until the acknowledgment is received.

(d) Where the originator has not stated that the electronic record is conditional on receipt of the acknowledgment, and the acknowledgment 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:

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

(ii) if the acknowledgment is not received within the time specified in Section 18(a), may, upon notice to the addressee, treat the electronic record as though it has never been sent, or exercise any other rights it may have.

(e) Where the originator receives the addressee's acknowledgment of receipt, it is presumed, unless evidence to the contrary is adduced, that the related electronic record was received by the addressee, but that presumption does not imply that the content of the electronic record corresponds to the content of the record received.

(f) Where the received acknowledgment states that the related electronic record met technical requirements, either agreed upon or set forth in applicable standards, it is presumed, unless evidence to the contrary is adduced, that those requirements have been met.

(g) Except as it relates to the sending or receipt of the electronic record, this section is not intended to address the legal consequences that may flow either from that electronic record or from the acknowledgment of its receipt.

Comments: Many electronic transactions require acknowledgements of the receipt of electronic records. This section is intended to set forth procedures for originators of electronic records to use in assessing whether the intended recipient has acknowledged receipt of electronic records sent. In particular, if the method of acknowledgment has not been agreed to by the parties involved, any method of acknowledgement can be used so long as it suffices to indicate to the originator that the electronic record sent has been received. This section also sets forth the rule that if an electronic record is conditional on receipt of acknowledgement, the transmission will be treated as if it were never sent if no acknowledgement is received.

In cases where the electronic record was not stated to be conditional on receipt of acknowledgement, an originator may subsequently impose this condition and specify a time frame in which acknowledgement must be received, and if not received in that time frame, treat the original transmission as never having been sent. Of course, if an acknowledgement is received, a presumption can be made that the electronic record was received. Significantly, this section is not intended to address the legal consequences of the transmission or receipt of electronic records. For example, where an originator sends an offer to a recipient, the acknowledgment of receipt simply is evidence of receipt of the offer. Issues related to whether the offer is valid or has been accepted are left to general principles of contract law.

19. Time and Place of Dispatch and Receipt

(a) Unless otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters an information system outside the control of the originator or the person who sent the electronic record on behalf of the originator.

(b) Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic record is determined as follows:

(i) if the addressee has designated an information system for the purpose of receiving electronic records, receipt occurs:

(A) at the time when the electronic record enters the designated information system; or

(B) 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 is 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.

(c) Section 19(b) shall apply notwithstanding that the place where the information system is located may be different from the place where the electronic record is deemed to be received under Section 19(d).

(d) Unless otherwise agreed between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business.

(e) For the purposes of this section:

(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 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, reference is to be made to the usual place of residence; and

(iii) "usual place of residence" in relation to a body corporate, means the place where it is incorporated or otherwise legally constituted.

(f)This section shall not apply to such circumstances as may be prescribed.

20. Applicable Law. Where a contract to which this Act applies is a transnational contract, and a dispute arises out of or in connection with, such contract, the following provisions shall apply:

(a) The dispute shall be decided in accordance with the rule of law designated by the parties as applicable to the substance of the dispute;

(b) Any designation by the parties of the law or legal system of a given country shall be construed, unless otherwise expressed, as directly referring to substantive law of that country and not to its conflict of laws rules;

(c) Failing any such designation of the law under subsection (a) by the parties the court or arbitral tribunal shall apply the rules of law which it considers to be appropriate given all the circumstances surrounding the dispute;

(d) In all cases the court of tribunal shall decide in accordance with the terms of the contract and shall take into account the usage of the trade applicable to the transaction;

<u>Explanation:</u> In this section "transnational contract" means a contract in which at least one of the parties is (i) an individual who is a national of or habitually resident in any country other than India; (ii) a body corporate which is incorporated in any country other than India; (iii) a company or an association or a body of individuals whose central management and control is situated in any country other than India; or (iv) the Government of a foreign country.

Comments: This section addresses the issue of which laws apply in cases of dispute related to electronic contracts. Generally, this section incorporates the provisions regarding the applicability of laws as reflected in Section 28 of the Arbitration and Conciliation Act, 1996.

PART V -- EFFECT OF DIGITAL SIGNATURES

21. Secure Electronic Record with Digital Signature. The portion of an electronic record that is signed with a digital signature shall be treated as a secure electronic record if the digital signature is a secure electronic signature by virtue of Section 13.

Comments: This section acknowledges that an electronic record signed with a digital signature will be considered a secure electronic record.

22. Digital Signature as a Secure Electronic Signature. When any portion of an electronic record is signed with a digital signature, the digital signature shall be treated as a secure electronic signature with respect to such portion of the record, if:
(a) the digital signature was created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate; and
(b) the certificate is considered trustworthy, in that it is an accurate binding of a public key to a person's identity because the following requirements have been fulfilled:
(i) the certificate was issued by a certification authority operating in compliance with the rules made under this Act*;*
(ii) the certificate was issued by a certification authority outside India recognized for this purpose by the Controller pursuant to rules made under this Act*;*
(iii) the certificate was issued by a department or ministry of the Central Government, State Government or a statutory corporation of Central or State Government approved by Central Government to act as a certification authority on such conditions as the Controller may by rules impose or specify; or
(iv) the parties have expressly agreed between themselves (originator and addressee) to use digital signatures as a security procedure, and the digital signature was properly verified by reference to the originator's public key.
23. Unreliable Digital Signatures. Unless otherwise provided by a rule of law or contract, a person relying on a digitally signed electronic record assumes the risk that the digital signature is invalid as a signature or authentication of the signed electronic record, if reliance on the digital signature is not reasonable under the circumstances having regard to the following factors:
(a) facts which the person relying on the digitally signed electronic record knows or has notice of, including all facts listed in the certificate or incorporated in it by reference;
(b) the value or importance of the digitally signed record, if known;
(c) the course of dealing between the person relying on the digitally signed electronic record and the subscriber and any available indicia of reliability or unreliability apart from the digital signature; and
(d) usage of trade, particularly trade conducted by trustworthy systems or other electronic means.
Comment: A person relying on the digital signatures assumes the risk that the signature is invalid in circumstances where there is a questionable digital signature. A questionable digital signature is one that cannot be verified because of several reasons such as, error by the signer or a faulty digital signature system. However, this section does not prohibit a person from relying on a digital signature that cannot be verified. He may do so at his own risk.
PART VI -- GENERAL DUTIES RELATING TO DIGITAL SIGNATURES
24. Foresee ability of Reliance on Certificates. It may be presumed that persons relying on a digital signature also will rely on a valid certificate containing the public key by which the digital signature can be verified.
Comments: This section acknowledges that a recipient of a digitally signed message will rely on a certificate to determine whether the message was signed by the sender. A recipient of an electronic record signed with a digital signature will assume that the certificate is valid and rely upon the certification authority's representations in the certificate that the signer is indeed the subscriber that is listed on the certificate. However, reliance on the integrity of the certificate is only foreseeable during the operational period of the certificate.
25. Prerequisites to Disclosure of Certificate. A person shall not publish a certificate or otherwise make it available to anyone known by that person to be in a position to rely on the certificate or

on a digital signature that is verifiable with reference to a public key listed in the certificate, if such person knows that:
(a) the certification authority listed in the certificate has not issued it;
(b) the subscriber listed in the certificate has not accepted it; or
(c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

Comments: This section prevents the publication of a certificate if it does not meet the pre-requisites as set forth above. The underlying premise of this section is to prohibit a party from publishing a certificate if they know that the certificate was not issued by a certification authority, the subscriber listed in the certificate has not accepted it, or the certificate has been suspended or revoked. The purpose of this section is to discourage fraudulent activity and encourages due care on the part of those issuing certificates. This section applies to certification authorities, subscribers named in the certificate and third parties.

26. Publication for Fraudulent Purpose. Any person who knowingly creates, publishes or otherwise makes available a certificate for any fraudulent or unlawful purpose shall be guilty of an offense and shall be liable on conviction to imprisonment for a term not exceeding 2 years or a fine not exceeding Rs.1,00,000 or both.

Comments: This section prohibits the publication of a certificate for fraudulent purposes. Under this section use of a certificate for fraudulent purposes is an offense punishable by imprisonment or fine or both.

27. False or Unauthorized Request. Any person who knowingly misrepresents to a certification authority his identity or authorization for the purpose of requesting a certificate or for suspension or revocation of a certificate shall be guilty of an offense and shall be liable on conviction to imprisonment for a term not exceeding 6 months or a fine not exceeding Rs. 50,000 or both.

Comments: This section prohibits misrepresentation when obtaining a digital signature certificate. Under this section obtaining a certificate by misrepresentation is an offense punishable by imprisonment or fine or both.