

ELECTRONIC COMMERCE ACT 1998- SINGAPORE

[Overview](#) | [Contents](#)

Overview

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 repudiable.

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 have 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.

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.

Source: ABA Digital Signature Guidelines §1.3.

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.

Source: ABA Digital Signature Guidelines §1.4.

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.

Source: Singapore Electronic Transactions Act §50.

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.

Source: ABA Digital Signature Guidelines §1.5.

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.

Source: ABA Digital Signature Guidelines §1.6.

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.

Source: ABA Digital Signature Guidelines §1.8.

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.

Source: Malaysia Computer Crimes Act §2(1); Uniform Electronic Transactions Act §102(12)

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.

Source: Uniform Electronic Transactions Act §102.

(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.

Source: Texas Penal Code §33.01.

(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.

Source: Maine Criminal Code §431(9).

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

Source: Singapore Electronic Transactions Act §2.

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.

Source: ABA Digital Signature Guidelines §1.10; Singapore Electronic Transactions Act §2.

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.

Source: United States Code, 18 U.S.C. §1030.

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.

Source: Malaysia Computer Crimes Act §2.

(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.

Source: Singapore Electronic Transactions Act §2.

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.

Source: Illinois Electronic Commerce Security Act §5-105; Uniform Electronic Transactions Act §102(5)(September 1998 draft).

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.

Source: Uniform Electronic Transactions Act §102(6)(September 1998 draft); UCC Article 2B §2B-102(19)(August 1998 draft).

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.

Source: UNCITRAL Model Law, Article 2(a).

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.

Source: Singapore Electronic Transactions Act §2.

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.

Source: Singapore Electronic Transactions Act §2.

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

Source: Singapore Electronic Transactions Act §2.

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.

Source: Uniform Electronic Transactions Act §102(12).

(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.

Source: Singapore Electronic Transactions Act §2.

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.

Source: United States Code, 47 U.S.C. §230(e).

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.

Source: Singapore Electronic Transactions Act §2.

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.

Source: Singapore Electronic Transactions Act §2.

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

Source: Singapore Electronic Transactions Act §2; Illinois Electronic Commerce Security Act §5-105.

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.

Source: Singapore Electronic Transactions Act §2.

(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.

Source: Singapore Electronic Transactions Act §2.

Comments: A repository is a collection of information related to issued 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.

Source: Singapore Electronic Transactions Act §2.

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.

Source: Singapore Electronic Transactions Act §2.

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.

Source: Singapore Electronic Transactions Act §2.

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.

Source: Singapore Electronic Transactions Act §2.

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.

Source: Singapore Electronic Transactions Act §2.

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.

Source: Singapore Electronic Transactions Act §10(3).

(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

Source: Illinois Electronic Commerce Security Act §5-105; See ABA Digital Signature Guidelines §1.35.

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.

Source: Singapore Electronic Transactions Act §2.

(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.

Source: Singapore Electronic Transactions Act §2.

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.

Source: Florida Electronic Signature Act of 1996 §2; Singapore Electronic Transactions Act §3, Utah Digital Signature Act §102.

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.

Source: Singapore Electronic Transactions Act §4; Illinois Electronic Commerce Security Act §5-115.

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.

Source: UNCITRAL Model Law, Article 4; UCC Article 2B §2B-107(b); ABA Digital Signature Guidelines §2.2.

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.

Source: UNCITRAL Model Law, Article 5.

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.

Source: UNCITRAL Model Law, Article 6.

Comments: Statutes and regulations frequently require that certain documents must be "written" or "in writing." The principle of requiring agreements to be memorialized in a 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.

Source: UNCITRAL Model Law, Article 7.

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.

Source: UNCITRAL Model Law, Article 8.

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.

Source: UNCITRAL Model Law, Article 9.

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.

Source: UNCITRAL Model Law, Article 10; Illinois Electronic Commerce Security Act, Section 5-135.

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.

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.

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.

Source: Singapore Electronic Transactions Act §17.

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.

Source: Singapore Electronic Transactions Act §18.

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.

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.

Source: UNCITRAL Model Law, Article 11; UCC Article 2B §2B-204.

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.

Source: UNCITRAL Model Law, Article 13; Uniform Electronic Transactions Act §202; Illinois Electronic Commerce Security Act §306.

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.

Source: UNCITRAL Model Law, Article 14.

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.

Source: UNCITRAL Model Law, Article 15.

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 or 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;

Explanation: 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.

Source: Singapore Electronic Transactions Act §19.

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.

Source: Singapore Electronic Transactions Act §20.

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.

Source: Singapore Electronic Transactions Act §22.

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. Foreseeability 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.

Source: Singapore Electronic Transactions Act §23.

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.

Source: Singapore Electronic Transactions Act §24.

Comments: This section prevents the publication of a certificate if it does not meet the prerequisites 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.

Source: Singapore Electronic Transactions Act §25.

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.

Source: Singapore Electronic Transactions Act §26.

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.

Part VII - Duties of Certification Authorities

28. Trustworthy System. Except as otherwise conspicuously set forth in its certification practice statement, a certification authority and a person maintaining a repository must:

- (a) maintain and utilize trustworthy systems and operate in a trustworthy manner in performing its services;
- (b) possess the reliability necessary for offering certification services;
- (c) employ personnel which possess the expert knowledge, experience and qualifications necessary for the offered services;
- (d) record and retain records of all relevant information concerning a certificate for an appropriate period of time, in particular to be able to provide evidence of certification in the context of a dispute or lawsuit; and

(e) publish all relevant information concerning the proper and secure use of certification services and established procedures for complaints and dispute resolution and settlement.

Source: UNCITRAL Draft Rules, Article 1.

Comments: Maintaining operations and performing services in a trustworthy manner is fundamental to the integrity of the certificate and digital signature process. This section recognizes that the degree of security should be determined according to a reasonableness standard in light of the factors set forth in the definition of trustworthy systems. This section also acknowledges that there may be situations in which persons desire to use certificates not created or maintained pursuant to trustworthy systems, such as for low cost, and allows them to do so as long as appropriate disclosure of that fact is clearly stated in the certification practice statement.

29. Disclosure by Certification Authorities.

(a) A certification authority shall disclose the following:

(i) its certificate that contains the public key corresponding to the private key used by that certification authority to digitally sign another certificate (defined for purposes of this section as a certification authority certificate);

(ii) any relevant certification practice statement;

(iii) notice of any revocation or suspension of its certification authority certificate; and

(iv) any other fact that materially and adversely affects either the reliability of a certificate that the authority has issued or the authority's ability to perform its services.

(b) In the event of an occurrence that materially and adversely affects a certification authority's trustworthy system or its certification authority certificate, the certification authority shall act in accordance with procedures governing such an occurrence specified in its certification practice statement or, in the absence of such procedures, use reasonable efforts to notify any person who is known to be or reasonably foreseeably will be affected by that occurrence.

Source: Singapore Electronic Transactions Act §28.

Comments: This section imposes a disclosure obligation upon a certification authority in order to facilitate the use of digital signatures.

30. Issuing of Certificate. A certification authority may issue a certificate to a prospective subscriber only after the certification authority has received a request for issuance from the prospective subscriber and

(a) if it has a certification practice statement, complied with all of the practices and procedures set forth in such certification practice statement including procedures regarding identification of the prospective subscriber; or

(b) in the absence of a certification practice statement addressing these issues, or if the parties involved have not entered into an agreement specifically providing otherwise, confirmed by itself or through an authorized agent that the following is the case:

(i) the prospective subscriber is the person to be listed in the certificate to be issued;

(ii) if the prospective subscriber is acting through one or more agents, the subscriber authorized the agent to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key;

(iii) the information in the certificate to be issued is accurate;

(iv) the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(v) the prospective subscriber holds a private key capable of creating a digital signature; and

(vi) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber.

Source: Singapore Electronic Transactions Act §29.

Comments: This section imposes only two requirements on the certification authority before issuing a certificate to be used for the purpose of verifying digital signatures: (1) a certificate can be issued only in response to a request from the prospective subscriber; and (2) the certification authority must comply with whatever certificate issuance practices it specifies in its certification practice statement. If a certification authority does not publish a certification practice statement, or enter into a contract with a relying party to address these issues, then Section 30(b) imposes a default standard for subscriber authentication.

The intent of this section is to allow certification authorities maximum flexibility in the efforts they undertake to verify subscriber identity, so long as the verification procedures that will be employed are clearly disclosed in advance.

31. Representations Upon Issuance of Certificate.

(a) By issuing a certificate, a certification authority represents, to any person who reasonably relies on the certificate or a digital signature verifiable by the public key listed in the certificate, that the certification authority has processed, approved and issued, and will manage and if necessary suspend or revoke the certificate, in accordance with any applicable certification practice statement incorporated by reference in the certificate, or of which the relying person has notice.

(b) In the absence of such a certification practice statement, the certification authority represents that it has confirmed the following:

(i) the certification authority has complied with all applicable requirements of this Act and other appropriate authority in issuing the certificate and, if the certification authority has published the certificate or otherwise made it available to such relying person, that the subscriber listed in the certificate has accepted it;

(ii) the subscriber identified in the certificate holds the private key corresponding to the public key listed in the certificate;

(iii) the certification authority has verified the identity of the subscriber to the extent stated in the certificate or its applicable certification practice statement or, in lieu thereof, that the certificate authority has reasonably verified the identity of the subscriber;

(iv) the subscriber's public key and private key constitute a functioning key pair;

(v) all information in the certificate is accurate, unless the certification authority has stated in the certificate or incorporated by reference in the certificate a statement that the accuracy of specified information is not confirmed; and

(vi) that the certification authority has no knowledge of any material fact which if it had been included in the certificate would adversely affect the reliability of the representations in this section.

(c) Where there is an applicable certification practice statement which has been incorporated by reference in the certificate, or of which the relying person otherwise has notice, subsection (b) shall apply to the extent that the representations are not inconsistent with the certification practice statement.

(d) Certification authorities shall keep and maintain as current a publicly accessible electronic register of certificates issued, indicating the time when any individual certificate expires or when it was suspended or revoked.

(e) Notwithstanding subsection (a) through (d), if a certification authority issued the certificate subject to the laws of another jurisdiction, the certification authority makes all warranties and representations, if any, otherwise applicable under the law governing its issuance.

Source: UNCITRAL Draft Rules, Article 10.

Comments: This section recognizes that there will be varying types of certificates based on differing levels of identification and authentication of prospective subscribers, and thus provides that the only representations made are that it has issued the certificate in accordance with any

applicable certification practice statement and any requirements or representations imposed by the law of the state or country under which the certificate was issued.

The reference to laws of another jurisdiction is intended to give relying parties the benefit of any statutory requirements relating to the issuance of the certificate that are imposed by the law of the state or country under which the certificate originally was issued.

32. Fiduciary Relationship.

(a) A certification authority is a fiduciary to a subscriber where a certification authority holds that subscriber's private key or where provided by contract among the parties involved.

(b) A certification authority is not otherwise a fiduciary to a subscriber and is not a fiduciary to any relying party, except where otherwise expressly provided by contract or law.

Source: ABA Digital Signature Guidelines §2.4.

Comments: A certification authority typically provides services at arm's length and does not create a special trusted relationship with its subscribers or relying parties, except where the certification authority holds the private key of a subscriber or where otherwise provided by agreement or law.

33. Financial Responsibility. A certification authority must have sufficient financial resources:

(a) to maintain its operations in conformity with its duties; and

(b) to be reasonably able to bear its risk of liability to subscribers and other relying parties relying on certificates issued by the certification authority and digital signatures verifiable by reference to public keys listed in such certificates.

Source: ABA Digital Signature Guidelines §3.3.

Comments: A certification authority's overall risk of liability largely will be a function of (1) its success in implementing a trustworthy system and utilizing the services of competent, conscientious personnel, (2) the number of certificates outstanding, and (3) the amounts at stake in transactions in which issued certificates are used, all evaluated in light of any applicable limits upon legal liability and recommended reliance limits. The certification authority can manage factors (1) and (2), but can do little in most cases to manage its risk in regard to factor (3).

Financial responsibility may be assured through security arrangements such as surety bonds or standby letters of credit, or perhaps through liability insurance.

34. Suspension of Certificate.

(a) Unless the certification authority and the subscriber agree otherwise, the certification authority that issued a certificate shall suspend the certificate as soon as possible after receiving a request by a person whom the certification authority reasonably believes to be one of the following:

(i) the subscriber listed in the certificate;

(ii) a person duly authorized to act for that subscriber; or

(iii) a person acting on behalf of that subscriber, who is unavailable.

(b) Except as otherwise specifically provided in its certification practice statement, or unless the certification authority and the subscriber agree otherwise, a certification authority that issued a certificate shall suspend the certificate as soon as possible after confirmation by the certification authority that:

(A) a material fact represented in the certificate is false;

(B) a material requirement for issuance of the certificate was not satisfied;

(C) the certification authority's private key or trustworthy system was compromised in a manner materially affecting the certificate's reliability; or

(D) the subscriber's private key has been compromised.

(c) Immediately upon suspension of a certificate by a certification authority, the certification authority shall notify the subscriber and relying parties in accordance with its certification practice statement or, in the absence of such statement, shall promptly notify the subscriber, promptly publish a signed notice of the suspension in the repository specified in the certificate for

publication of notice of suspension, and otherwise disclose the fact of suspension on inquiry by any relying party. Where one or more repositories are specified, the certification authority shall publish signed notices of the suspension in all such repositories.

Source: UNCITRAL Draft Rules Article 14.

Comments: A provision on suspension of certificates was added by the UN Working Group at its thirty-first session.

35. Revocation of Certificate

(a) Except as otherwise specifically provided in its certification practice statement, or unless the certification authority and the subscriber agree otherwise, a certification authority shall revoke a certificate that it issues upon the occurrence of the following:

(i) receiving a request for revocation by the subscriber named in the certificate, and confirming that the person requesting revocation is the subscriber or is an agent of the subscriber with authority to request the revocation;

(ii) receiving a certified copy of the subscriber's death certificate, or upon confirming by other verifiable evidence that the subscriber is dead;

(iii) upon presentation of documents effecting a corporate dissolution of the subscriber or upon confirming by other verifiable evidence that the subscriber has been dissolved or has ceased to exist; or

(iv) confirmation by the certification authority that of the following events has occurred, provided that no such revocation may be made until the subscriber has had a reasonable opportunity for a hearing:

(A) a material fact represented in the certificate is false;

(B) a material requirement for issuance of the certificate was not satisfied;

(C) the certification authority's private key or trustworthy system was compromised in a manner materially affecting the certificate's reliability; or

(D) the subscriber's private key has been compromised.

(b) Upon effecting such a revocation, the certification authority shall immediately provide notice as follows:

(i) immediately upon revocation of a certificate by a certification authority, the certification authority shall promptly notify the subscriber listed in the revoked certificate (if not deceased, dissolved or ceased to exist) and any relying parties in accordance with its certification practice statement or, in the absence of such statement, shall promptly notify the subscriber, promptly publish a signed notice of the revocation in the repository specified in the certificate for publication of notice of revocation, and otherwise disclose the fact of revocation on inquiry by a relying party; and

(ii) where one or more repositories are specified, the certification authority shall publish signed notices of the revocation in all such repositories.

Source: UNCITRAL Draft Rules, Article 13.

Comments: This section and the preceding section set forth a default standard governing suspension and revocation of certificates.

Part VIII -- Duties of Subscribers

36. Generating A Key Pair

(a) If the subscriber generates the key pair whose public key is to be listed in a certificate issued by a certification authority and accepted by the subscriber, the subscriber shall generate that key pair using a trustworthy system.

(b) This section shall not apply to a subscriber who generates the key pair using a system approved by the certification authority.

Source: Singapore Electronic Transactions Act §36.

37. Obtaining A Certificate. All material representations made by the subscriber to a certification authority for purposes of obtaining a certificate, including all information known to the subscriber and represented in the certificate, shall be accurate and complete to the best of the subscriber's knowledge and belief, regardless of whether such representations are confirmed by the certification authority.

Source: Singapore Electronic Transactions Act §37.

Comments: This section sets forth the general obligation of the subscriber to provide accurate and complete information to a certification authority when seeking to obtain a certificate.

38. Acceptance of Certificate.

- (a) A subscriber shall be deemed to have accepted a certificate if that subscriber:
- (i) publishes or authorizes the publication of a certificate in one of the following ways:
 - (A) to one or more persons; or
 - (B) in a repository; or
 - (ii) otherwise demonstrates approval of a certificate while knowing or having notice of its contents.
- (b) By accepting a certificate issued by a certification authority, the subscriber listed in the certificate certifies to all who reasonably rely on the information contained in the certificate as follows:
- (i) that the subscriber rightfully holds the private key corresponding to the public key listed in the certificate;
 - (ii) that all material representations made by the subscriber to the certification authority and material to the information listed in the certificate are true; and
 - (iii) that all information in the certificate that is within the knowledge of the subscriber is true.

Source: Singapore Electronic Transactions Act §38.

Comments: Acceptance of a certificate by a subscriber may be expressed or implied, and can occur in a variety of ways. For example, acceptance can occur when the subscriber publishes the certificate in a repository or when the subscriber provides copies of the certificate to one or more persons. Factors to be considered in determining whether a subscriber has accepted a certificate include whether the subscriber has specifically requested issuance of the certificate; whether the subscriber has expressly approved the certificate, or not acknowledged it in any way; whether the subscriber has knowledge that the certificate is available to potential relying parties; the reasonableness of reliance upon the certificate; and the foreseeability of such reliance.

39. Control of Private Key.

- (a) By accepting a certificate issued by a certification authority, the subscriber identified in the certificate assumes a duty to exercise reasonable care to retain control of the private key corresponding to the public key listed in such certificate and to prevent its disclosure to any person not authorized to create the subscriber's digital signature.
- (b) Such duty shall continue during the operational period of the certificate and during any period of suspension of the certificate.

Source: Singapore Electronic Transactions Act § 39.

Comments: This section imposes a higher duty of care upon a subscriber than is currently imposed on the holder of a credit card, ATM card or other such item. Persons who intentionally or negligently disclose their private keys, with or without fraudulent intent, should be held to a higher standard than those responsible for an involuntary disclosure.

If a private key is compromised, and a certificate has been issued listing the corresponding public key, the appropriate corrective action is to revoke the certificate or to suspend the certificate without delay until revocation or other corrective action can be taken.

40. Initiating Suspension or Revocation. A subscriber who has accepted a certificate shall as soon as possible notify the issuing certification authority and request said authority to suspend or revoke the certificate if the private key corresponding to the public key listed in the certificate has been compromised.

Source: Singapore Electronic Transactions Act § 40.

Comments: A fundamental premise underlying use of a digital signature is that the private key used to create the digital signature is under the control of the subscriber. Because of this, and the fact that a relying party has no ability to determine who actually used the private key to digitally sign an electronic record, this section imposes on the subscriber the obligation to take steps to revoke the certificate promptly in the event the private key is compromised.

Part IX -- Regulation of Certification Authorities and Repositories

41. Appointment of Controller and Other Officers

(a) The Central Government shall appoint a Controller of Certification Authorities for the purpose of this Act and, in particular, for the purposes of licensing, certifying, monitoring and overseeing the activities of certification authorities.

(b) The Controller may, after consultation with the Central Government, appoint such number of Deputy and Assistant Controllers of Certification Authorities and officers as the Controller considers necessary to exercise and perform all or any of the powers and duties of the Controller under this Act or rules made under this Act, except for the Controller's power to direct compliance as set forth in Section 54 of this Act.

(c) The Controller, the Deputy and Assistant Controllers and officers appointed by the Controller under Section 41 shall exercise, discharge and perform the powers, duties and functions conferred on the Controller under this Act or any rules made under this Act, subject to such written directions as may be issued by the Central Government to the Controller and subject to Section 54 of this Act.

(d) The Controller shall maintain a publicly accessible database containing a certification authority disclosure record for each certification authority which shall contain all the particulars required under the rules made under this Act.

(e) The Controller may investigate complaints or other information indicating violations of rules adopted under this Act, and may refer for prosecution any suspected or alleged violations to the appropriate government agency.

(f) In the application of the provisions of this Act to certificates issued by the Controller and digital signatures verified by reference to those certificates, the Controller shall be deemed to be a certification authority.

(g) The Controller, the Deputy, Assistant Controller and officers appointed by the Controller shall be deemed to be public servants for the purposes of the Penal Code.

(h) In exercising any of the powers under this Act, any officer appointed by the Controller shall on demand produce to the person against whom he is acting the authority issued to him by the Controller.

Source: Singapore Electronic Transactions Act §§41 and 50.

42. Recognition of Foreign Certification Authorities

(a) Certificates issued by a foreign certification authority, and signatures and records complying with the laws of another jurisdiction relating to digital or other electronic signatures, are recognized as legally equivalent to certificates issued by certification authorities operating under this Act, and to the signatures and records complying with this Act, if the laws of the other

jurisdiction and the practices of the foreign certification authority require a level of reliability at least equivalent to that required for such certificates, records and signatures under this Act.

(b) Notwithstanding the preceding paragraph, the Controller and parties to commercial and other transactions may specify that a particular certification authority, class of certification authorities or class of certificates must be used in connection with messages or signatures submitted to them.

(c) The determination of equivalence described in subsection (a) may be made by a published determination of the Controller in the Official Gazette or through bilateral or multilateral agreement with other jurisdictions. The determination of equivalence, shall be made with regard to the following factors:

(i) financial and human resources, including existence of assets within jurisdiction;

(ii) trustworthiness of hardware and software systems;

(iii) procedures for processing of certificates and applications for certificates and retention of records;

(iv) availability of information to subscribers identified in certificates and to potential relying parties;

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

(vi) the existence of a declaration by the jurisdiction, an accreditation body or the certification authority regarding compliance with or existence of the foregoing;

(vii) susceptibility to the jurisdiction of the courts of the enacting jurisdiction; and

(viii) the degree of discrepancy between the law applicable to the liability of the certification authority and the law of the enacting jurisdiction.

Source: UNCITRAL Draft Rules, Chapter III, Article 19.

Comments: This section provides maximum flexibility to the Controller to determine which foreign regulatory schemes to recognize, and provides guidelines and criteria to be used in making that determination.

43. Recommended Reliance Limit

(a) A certification authority may, in issuing a certificate to a subscriber, specify a recommended reliance limit in the certificate.

(b) The certification authority may specify different limits in different certificates as it deems appropriate.

Source: Singapore Electronic Transactions Act §44.

Comments: This section provides maximum flexibility to the Controller in setting reliance limits for different certificates issued.

44. Liability Limits for Certification Authorities. Unless a certification authority expressly waives the application of this section, a certification authority shall not be liable for the following:

(a) For any loss caused by reliance on a false or forged digital signature of a subscriber if, with respect to the false or forged digital signature, the certification authority complied with the requirements of this Act and applicable regulations; and

(b) For an amount in excess of the amount specified in the certificate as its recommended reliance limit for either:

(i) a loss caused by reliance on a misrepresentation in the certificate of any fact that the certification authority is required to confirm; or

(ii) intentional or knowing failure to comply with any provisions of this Act in issuing the certificate, unless such failure to comply was done intentionally or knowingly.

Source: Singapore Electronic Transactions Act §45.

Comments: This section limits certification authorities' potential exposure to liability in connection with any losses associated with the use of digital signatures. In particular, it eliminates liability in cases where a false or forged digital signature is executed and relied upon, notwithstanding the certification authorities' compliance with the requirements of this Act.

45. Recognition of Repositories.

(a) The Controller may recognize one or more repositories after determining that a repository to be recognized satisfies the requirements prescribed in the regulations made under this Act.

(b) The Controller shall publish a list of recognized repositories in such form and manner as he may determine.

Source: Malaysia Digital Signature Act §68.

46. Liability of Repositories.

(a) Notwithstanding any disclaimer by the repository or any contract to the contrary between the repository and a certification authority or a subscriber, a repository shall be liable for a loss incurred by a person reasonably relying on a digital signature verified by the public key listed in a suspended or revoked certificate, if loss was incurred more than one business day after receipt by the repository of a request to publish notice of the suspension or revocation, and the repository had failed to publish the notice when the person relied on the digital signature.

(b) Unless waived, a recognized repository or the owner or operator of a recognized repository:

(i) shall not be liable for failure to record publication of a suspension or revocation, unless the repository has received notice of publication and one business day has elapsed since the notice was received;

(ii) shall not be liable under subsection (a) in excess of the amount specified in the certificate as the recommended reliance limit;

(iii) shall not be liable under subsection (a) for:

(A) punitive or exemplary damages; or

(B) damages for pain or suffering;

(iv) shall not be liable for misrepresentation in a certificate published by a certification authority;

(v) shall not be liable for accurately recording or reporting information which a certification authority, a court or the Controller has published as required or permitted under this Act, including information about the suspension or revocation of a certificate; and

(vi) shall not be liable for reporting information about a certification authority, a certificate or a subscriber, if such information is published as required or permitted under this Act or is published by order of the Controller in the exercise of his powers under this Act.

Source: Malaysia Digital Signature Act §69.

Part X – Government use of Electronic Records and Signatures

47. Acceptance of Electronic Filing and Issue of Documents.

(a) Any department or ministry of Central Government, State Government or a statutory corporation under Central or State Government that, pursuant to any enactment:

(i) accepts the filing of documents or requires that documents be created or retained;

(ii) issues any permit, license or approval; or

(iii) provides for the method and manner of payment, may, notwithstanding anything to the contrary in such enactment:

(A) accept the filing of such documents, or the creation or retention of such documents, in the form of electronic records;

(B) issue such permit, license or approval in the form of electronic records; or

(C) make such payment in electronic form.

(b) In any case where a department or ministry of Central Government, State Government or a statutory corporation under Central or State Government decides to perform any of the functions in subsection (a)(i), (ii), or (iii), such agency may specify:

(i) the manner and format in which such electronic records shall be filed, created, retained or issued;

(ii) where such electronic records are required to be signed, the type of electronic signature required (including, if applicable, a requirement that the sender use a secure electronic signature);

(iii) the manner and format in which such signature shall be affixed to the electronic record, and the identity of or criteria that shall be met by any certification authority used by the person filing the document;

(iv) control processes and procedures as appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(v) any other required attributes for electronic records or payments that are currently specified for corresponding paper documents.

(c) Nothing in this Act shall by itself compel any department or ministry of the Central Government, State Government or a statutory corporation under Central or State Government to accept or issue any document in the form of electronic records.

Source: Singapore Electronic Transactions Act §47.

Comment: The section empowers the government to accept the electronic filing of documents. The section also allows a government entity to determine the procedures for filing information electronically. Note that this section does not require government entities to accept electronic filings.

Part XI -- Liability of Network Service Providers

48. Liability of Network Service Providers.

(a) A network service provider shall not be subject to any civil or criminal liability under any rule of law in respect of third party material in the form of electronic records to which such provider merely provides access if such liability is founded on:

(i) the making, publication, dissemination or distribution of such materials or any statement made in such material; or

(ii) the infringement of any rights subsisting in or in relation to such material.

(b) Nothing in this section shall affect:

(i) any obligation of the network service provider founded on principles of contract law;

(ii) the obligation of a network service provider as such under a licensing or other regulatory regime established under any enactment for the time being in force; or

(iii) any obligation imposed under any enactment for the time being in force or by a court to remove, block or deny access to any material;

(iv) the provisions of Section 52 of this Act.

(c) Nothing in clause (a) of this section shall render a network service provider immune from liability for any violation of law for the time being in force (including provisions of this Act) committed intentionally or knowingly.

Source: Singapore Electronic Transactions Act §10.

Comment: The protection afforded by this section is intended to encompass Internet access and service providers, as well as providers of online services and providers of telecommunications services necessary to access the Internet or other interactive computer services. The liability of network service providers has been extremely controversial in the United States and other countries. A statute enacted in the United States in 1996, the "Communications Decency Act,"

included language protecting providers of Internet access from liability as publishers for statements published online by system subscribers or other third-parties. Although the portions of the Communications Decency Act governing indecent material were subsequently found unconstitutional by the United States Supreme Court, the provisions protecting access providers have been held, in several U.S. cases, to protect Internet service and access providers from liability for defamation based upon statements published online by service subscribers. In addition, several statutes currently pending in the United States would, under some circumstances, protect Internet service providers from contributory liability for copyright infringement based on third party activities. In protecting access providers from liability, the courts in the United States have cited the difficulty of screening transmissions on an interactive computer service, as well as the fear of inhibiting the development of Internet communications by imposing liability on network service providers for activities over which they have little control. These principles have been recognized in the International community as well. During the WIPO Diplomatic Convention to adopt new copyright treaties conducted in Geneva in 1996, draft provisions of the treaties that would have imposed liability on Internet service providers and other network operators were deleted from the final drafts of the treaties. Of course, network service providers should not be immunized from intentional acts that are in violation of the law.

Part XII – Computer Crime

49. Computer Crime. For the purpose of this Act, any person who commits any of the following acts is guilty of an offense of computer crime:

- (a) Intentionally accesses, damages or conceals, or attempts to access, damage or conceal, temporarily or permanently, any computer data base, computer, information system or computer network, without permission from the owner, in order to either:
 - (i) wrongfully control, obtain, make use of or prevent others from deriving the benefits of money, property, data or electronic records;
 - (ii) copy or destroy any data or electronic records;
 - (iii) use or disrupt any functions of computers, computer networks or information systems; or
 - (iv) commit any act that is an offense under the Indian Penal Code.
- (b) Knowingly, and with the intent to defraud, obtains or attempts to obtain any computer services by false representation, false statement or unauthorized charging to the account of another, by installing or tampering with any facilities or equipment, or by any other means.
- (c) Intentionally or recklessly introduces or allows the introduction of any computer virus into any computer, computer system or computer network without permission of the owner.

Comments: This section provides for the enumeration of various acts that shall be considered computer crimes. Fundamental to the approach taken in this section is the recognition that the Indian Penal Code, 1860 already enumerates a wide variety of crimes that include acts committed through or in connection with computers. For, example, the Indian Penal Code covers all acts of larceny, without any limitations regarding the means by which the larceny is committed. If the larceny takes the form of manually stealing goods from a store or stealing money from a remote bank account through use of a computer, the law treats either act as the same for purposes of classification as larceny. Thus, the fact that a crime is committed by computer does not limit the applicability of the Indian Penal Code in most instances. This section, therefore, does not attempt to identify all criminal acts involving computers, at least in instances where such acts already would be considered crimes under the Indian Penal Code. Instead, this section merely acknowledges that any act that is considered criminal under the Penal Code may also be called a computer crime when computers are involved.

In addition, this section specifies certain acts as computer crimes when the Indian Penal Code appears not to apply. In particular, the introduction of viruses into computers and the appropriation or disruption of computer services are unique to the computer environment and do not appear to be covered by the Penal Code. It can be argued that the use of fraud in obtaining

computer services could be covered by the Penal Code; however, to the extent that intangible "goods" are being received or altered or the means of access to the services is through cyberspace, the applicability of the Penal Code is unclear. Similarly, although this section makes criminal the act of interfering with another's rights to money or property, which if in a tangible form could be covered by the Penal Code, the advent of cybercash and digital property require new computer crimes to be established. Additionally, the unauthorized copying, controlling or damaging of intangible goods (data, electronic records) appears to be beyond the scope of the Penal Code and, therefore, a provision regarding these acts has been incorporated into this section.

50. Penalties

(a) Any person who commits the offense of computer crime as set forth in the provisions of Section 49(a) of this Act is punishable as follows:

(i) For the first offense that does not result in damage, by imprisonment up to 1 year or by a fine not to exceed Rs. 1,00,000 or both;

(ii) For second or subsequent offenses, or in cases where damage occurs, by imprisonment up to three years or by a fine up to Rs. 2,00,000, or by both, and if government or public property is injured, by imprisonment up to three years or by a fine up to Rs. 5,00,000 or both;

(b) Any person who commits offense as under Section 49(b) of this Act shall be punishable as follows:

(i) For the first offense which does not result in damage, and where the value of the computer services used does not exceed Rs. 10,000, by a fine not exceeding Rs. 1,00,000, or by imprisonment not exceeding one year, or by both.

(ii) For any offense which results in damage of an amount greater than Rs. 1,00,000 or in a damage, or if the value of the computer services used exceeds Rs. 10,000, or for any second or subsequent violation, by a fine not exceeding Rs. 2,00,000, or by imprisonment up to three years, or by both.

(c) Any person who commits offense as per Section 49(c) of this Act is punishable as follows:

(i) For a first offense which does not result in damage, an infraction punishable by a fine not exceeding Rs. 10,000.

(ii) For any offense which results in damage in an amount not greater than Rs. 50,000, or for a second or subsequent violation, by a fine not exceeding Rs. 1,00,000 or by imprisonment not exceeding one year, or by both.

(iii) For any offense which results in damage in an amount greater than Rs. 50,000, by a fine not exceeding Rs. 2,00,000, or by imprisonment up to three years, or by both.

(d) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, all offenses under this Act shall be bailable, nonrecognizable, and triable exclusively by the Chief Metropolitan Magistrate, Additional Chief Metropolitan Magistrate, Chief Judicial Magistrate or Additional Chief Judicial Magistrate.

Comments: This section provides criminal penalties for the offenses enumerated in Section 49. Some leniency was provided in cases of first offenses where no damage occurred as a result of the criminal act. On the other hand, additional fines were imposed in cases where governmental or public property is damaged. As indicated in the commentary to Section 49, the Indian Penal Code already provides for penalties in the case of many criminal acts without regard to whether a computer is involved. Therefore, this section specifies that nothing in this Act should be construed to abrogate any penalties that may be applicable under the Penal Code.

51. Forfeiture.

(a) Any person who commits the offense of computer crime as set forth in Section 49 of this Act shall forfeit, according to the provisions of this section, any monies, profits or proceeds, and any interest or property which the sentencing court determines he has acquired or maintained, directly or indirectly, in whole or in part, as a result of such offense. Such person shall also forfeit any interest in, security, claim against or contractual right of any kind which affords him a source of

influence over any enterprise which he has established, operated, controlled, conducted or participated in conducting, where his relationship to or connection with any such thing or activity directly or indirectly, in whole or in part, is traceable to any item or benefit which he has obtained or acquired through computer fraud.

(b) Any computer, computer system, computer network or any software or data, owned by such person, which is used during the commission of any public offense described in Section 49 or any computer, owned by the person, which is used as a repository for the storage of software or data illegally obtained in violation of Section 49 shall be subject to forfeiture under orders of the Court ordering his conviction.

Comments: This section provides for the forfeiture of any benefits derived by any criminal offended as a result of the commission of any computer crime, as well as the forfeiture of any computers or related apparatus used in the commission of such crime.

Part XIII -- General

52. Confidentiality.

(a) Obligation of Confidentiality.

(i) Except where compelled by any court of law or pursuant to any law for the time being in force, no certification authority, Controller or network service provider, or their respective agents or employees, that have obtained access to any material, shall disclose such material to any other person without the prior consent of the owner of such material, except in cases where such disclosure is being made for the purpose of protecting his interest or for such other purpose as may be prescribed.

(ii) Except where compelled by any court of law or pursuant to any law for the time being in force, no person who has obtained unauthorized access to any electronic record shall intentionally or knowingly disclose such record or its contents to any other person. The provisions of this section shall be without prejudice to any liability which such person may have incurred by reason of the unauthorized access.

(b) Penalty for Breach of Confidentiality.

(i) Any network service provider who intentionally, knowingly or negligently contravenes subsections (a) shall be (A) enjoined by a court from acting as a network service provider for a period not to exceed three (3) months, or (B) liable in damages sustained by the owner, such damages to amount to no less than Rs. 10,000, or (C) both.

(ii) Any person other than a network service provider who intentionally contravenes subsection (a) shall be guilty of an offense and shall be liable upon conviction to imprisonment not to exceed 6 months or fines not to exceed Rs. 50,000 or to both.

Explanation: In this section, "material" includes any electronic record, book, register, correspondence, information or document.

Source: Singapore Electronic Transactions Act §48.

Comments: This section protects the confidentiality of electronic records and related materials obtained pursuant to this Act, and provides for penalties in cases where confidentiality is breached.

53. Offense by Body Corporate. Where an offense under this Act or any rules made under this Act is committed by a body corporate and such offense is proved to have been committed with the consent or connivance of, or is proved to be attributable to, any act or default on the part of any director, manager, secretary or other similar officer of the body corporate, he as well as the

body corporate, shall be guilty of that offense and shall be liable to be proceeded against and punished accordingly.

Source: Singapore Electronic Transactions Act §49.

Comments: This section provides for the criminal liability of corporations and their officers in cases where corporate officers contravene provisions of this Act.

54. Controller May Give Directions for Compliance.

(a) The Controller may direct, by notice in writing, a certification authority or any officer or employee thereof to take such measures or stop carrying on such activities as are specified in the notice, if such action is necessary to ensure compliance with the provisions of this Act or any rules made under this Act.

(b) Any person who fails to comply with any direction specified in a notice issued under subsection(a) shall be guilty of an offense and shall be liable on conviction to imprisonment for a term not exceeding 1 year or a fine not exceeding Rs. 1,00,000 or both.

Source: Singapore Electronic Transactions Act §51.

Comments: This section is designed to provide enforcement authority to the Controller over certification authorities and provide penalties in cases of noncompliance with issued orders.

55. Power to Investigate.

(a) The Controller or an authorized officer may investigate, pursuant to a written order issued by the Controller or the officer, the activities of a certification authority in relation to its compliance with this Act and any rules made under this Act.

(b) For the purposes of subsection (a), the Controller may in writing issue an order to a certification authority to further its investigation.

(c) The Controller or an authorized officer may make reasonable inquiry, pursuant to a written order, of any person reasonably believed to have relevant information in connection with the commission of any offense under this Act.

Source: Singapore Electronic Transactions Act §52.

Comments: This section provides power to the Controller to investigate the activities of certification authorities, essentially for the purpose of compliance auditing.

56. Access to Computers and Data. The Controller or an authorized officer shall:

(a) be entitled at any time reasonable under the circumstances to:

(i) have access to, inspect and check the operation of any information system and any associated apparatus or material which he has reasonable cause to suspect is or has been in use in connection with any offense under this Act;

(ii) use or caused to be used any such information system to search any data contained in or available to such information system; or

(b) be entitled to require:

(i) the person by whom or on whose behalf the Controller or authorized officer has reasonable cause to suspect the computer is or has been so used; or

(ii) any person having charge of, or otherwise concerned with the operation of, the computer, apparatus or material, to provide him with such reasonable technical and other assistance as he may require for the purposes of subsection (a).

Source: Singapore Electronic Transactions Act §53.

Comments: This section empowers the Controller or his agent to have access to and inspect any information system or associated apparatus that is reasonably suspected of having been used in connection with any offenses under this Act. Additionally, it requires technical cooperation from persons having charge of such information system or associated apparatus.

57. Production of Documents, Data, etc. The Controller shall, for the purposes of the implementation of this Act, have power to do all or any of the following:

(a) require, by a written order, the production of records, accounts, data and documents kept by a certification authority and to inspect, examine and copy any of them;

(b) require, by a written order, the production of any document from any person reasonably in relation to any offense under this Act or any regulations promulgated under this Act.

Source: Singapore Electronic Transactions Act §55.

Comments: This section empowers the Controller to request the production of documents for the purpose of auditing a certification authority for compliance, as well as for the purpose of making reasonable inquiry in connection with any offense under this Act.

58. General Penalty. Any person who (a) contravenes any provision of this Act or (b) fails to comply with any notice or written order lawfully issued under this Act, shall be guilty of an offense and, if no penalty is provided in this Act for such offense, shall be punished with imprisonment for a term not exceeding 6 months or a fine not exceeding 1,00,000 or both.

Source: Singapore Electronic Transactions Act §56.

Comments: This section provides for penalties in cases where no penalties otherwise have been provided in this Act or the Penal Code.

59. Sanction for prosecution. No prosecution in respect of any offense under this Act or any rule made under this Act shall be instituted except by or with the previous sanction of the Central Government.

Source: Singapore Electronic Transactions Act §57.

60. Power to Exempt. The Central Government may by notification published in the Official Gazette, exempt, in the public interest, any person or class of persons from all or any of the provisions of this Act or any rules made under this Act.

Source: Singapore Electronic Transactions Act §60.

Comments: This provision allows the Central Government to exempt persons from the Act in cases of public interest.

61. Power of Central Government to make rules.

(a) The Central Government may make rules, by notification in the Official Gazette, to carry out the purposes of this Act.

(b) Without prejudice to the generality of the power conferred by clause (a), the rules made thereunder may provide for all or any of the following matters:

(i) to define when a digital signature qualifies as a secure electronic signature consistent with the provisions of this Act;

(ii) to ensure the quality of repositories and the services they provide;

(iii) licensing of certification authorities and their authorized representatives and matters incidental thereto;

the activities of certification authorities, including the manner, method and place of soliciting business, and the conduct of such solicitation, if any.

- (v) the standards to be maintained by certification authorities;
- (vi) prescribing the appropriate standards with respect to the qualifications, experience and training of applicants for any certification authority or for their employees;
- (vii) prescribing the conditions for the conduct of business by a certification authority;
- (viii) providing for the content and distribution of written, printed or visual material and advertisements that may be distributed or used by a person in respect of a digital certificate or key;
- (ix) prescribing the form and content of a digital certificate or key;
- (x) prescribing the particulars to be recorded in, or in respect of, accounts kept by certification authorities;
- (xi) providing for the appointment and remuneration of an auditor appointed under the regulations and for the costs of an audit carried out under the regulations;
- (xii) providing for the establishment and regulation of any electronic system by a certification authority, whether by itself or in conjunction with other certification authorities, and for the imposition and modification of such requirements, conditions or restrictions as the Controller may deem appropriate;
- (xiii) the manner in which a certification authority conducts its dealings with its customers, conflicts of interest involving the certification authority and its customers, and the duties of the certification authority to its customers with respect to digital certificates;
- (xiv) prescribing any forms for the purposes of the rules; and
- (xv) prescribing fees to be paid in respect of any matter or thing required for the purposes of this Act or the rules.

(a) Rules made under this section may provide that a contravention of a specified provision shall be an offence and may provide penalties not exceeding a fine of Rs. 50,000.

(c) Every rule made by the Central Government under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised of in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or both Houses agree that the rule should not be made, the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule.

(d) All rules made by the Central Government under this Act shall be published in the Official Gazette.

Source: Singapore Electronic Transactions Act §42.

Comments: This section authorizes the Central Government to adopt rules necessary and appropriate to implement the provisions of this Act. In drafting such rules, appropriate consideration should be given to the goal of this Act to be flexible and technologically neutral. Given the rapid pace at which technology develops, overly prescriptive rules are inappropriate. For example, a requirement that Certification Authorities' employees receive training in the use of

specific technologies may not be appropriate, and broader language that permits flexibility in training requirements based upon the available state of technology would be preferred.

In developing rules regarding when a digital signature qualifies as a secure electronic signature, due consideration should be given to making such rules as flexible and technologically neutral as possible in order to accommodate rapidly evolving digital signature technologies.

In developing rules regarding the quality of repositories and their services, due consideration should be given to ensuring that the repositories maintain secure and reliable record management systems. The ISO 9000 guidelines for quality management may be a useful guideline for establishing quality control procedures for repositories.

In developing rules for licensing Certification Authorities, care should be taken to avoid, where possible, imposing specific technical requirements upon applicants. Some key factors, however, that should be considered in licensing Certification Authorities are: the financial capabilities of the applicant, the familiarity of the applicant with digital signatures, the capabilities of the applicant to manage volumes of information (i.e. certificates and related information) effectively, and the integrity of the applicant as a potential fiduciary for subscribers.

In developing rules governing the activities of certification authorities, particularly in regard to solicitation of business, due regard should be given to the provisions in the Advocates Act, 1961 and the Medical Council Act, 1956 regarding solicitation by advocates and members of the medical profession. In general, rules governing the activities and conduct of business of certification authorities should require certification authorities to at all times engage in ethical conduct.

In developing rules governing the standards to be maintained by certification authorities, due consideration should be given to establishing quality control guidelines for all activities of such authorities. The ISO 9000 quality assurance guidelines may be a source of reference.

In developing rules for the content and distribution of materials that may be distributed by a person in respect of a digital certificate or key, due consideration should be given to the need for keeping private keys confidential.

In developing rules prescribing the form and content of a digital certificate or key, consideration should be given to providing flexibility for the use of a variety of available digital signature technologies.

In developing rules for the appointment and remuneration of an auditor, due consideration should be given to the qualifications of an auditor, including the auditor's familiarity with digital signature technology and the need for keeping audited information confidential as appropriate.

In developing rules providing for the establishment and regulation of any electronic system by a certification authority, and for the imposition and modification of such requirements, conditions or restrictions as the Controller may deem appropriate, due consideration should be given to permitting maximum flexibility to the certification authorities so long as basic rules regarding the conduct of certification authorities are followed.

In developing rules prescribing the manner in which a certification authority conducts its dealings with customers, due consideration should be given to the fact that the certification authority will have a fiduciary duty to subscribers with respect to its retention of private keys.

Of course, in the development of other rules, the Central Government should consider those issues that it deems necessary and appropriate. An area in which additional rules may be appropriate relates to the development of licensing requirements for network service providers.

62. Power to remove difficulties. If any difficulty arises in giving effect to the provisions of this Act, the Central Government may by an order published in the Official Gazette make such provisions as necessary for the purpose of removing the difficulty. No such order shall be made after two years from the commencement of this Act.