LEGAL GUIDE TO THE ELECTRONIC TRANSACTIONS ACT

TABLE OF CONTENTS

Overview of the Act

In a non-electronic environment, the document is the record of the parties' agreement, and the signature is the stamp of a person's identity, and marks his intention to commit himself legally. However, in an electronic environment, there is neither paper, pen nor ink, not to mention the fact that parties may not even meet each other. How can these parties "write" a signature on something that is neither physical or tangible in the electronic environment?

The solution is to use an electronic signature on an electronic record. Like written signatures, electronic signatures may be used to establish the identity of the party who "signed" the document, or as proof of his intention to make certain legal commitments. More importantly, a special form of electronic signatures such as digital signatures can be used to guarantee that the electronic document which has been "signed" by way of the electronic signature has not been altered or tampered with. This Act seeks to deal with this problem of affording legal recognition to electronic and digital signatures. It establishes the legal framework that will provide for the setting up of a Public Key Infrastructure. It accords legal sanction for records, files or documents that are retained in electronic form. It also enables public institutions and government departments to accept electronic applications, and in turn permits these institutions and departments to issue electronic licences and permits. And since network intermediaries play such an important role in setting up the electronic infrastructure, the Act also seeks to clarify the liability of network service providers for third party content. Overall, by bringing the law up to date with technological developments, and by putting in place legal standards for the use of electronic transactions, both in the public as well as in the private sector, the Act as a piece of legislation is expected to greatly facilitate and promote electronic commerce in Singapore.

Introduction

The guide is written in the form of a section-by-section commentary, with explanations as to the way each section functions and cross-references to the other relevant sections. The guide is intended for the use of lawyers and lay people who wish to find out more about the Electronic Transactions Act, and its implications for them. It is not intended to be a piece of legal advice to any person, nor is the guide an official interpretation of the Act or a policy statement of the Singapore government or the National Computer Board. Nor is it intended to be a comprehensive restatement of all the legal issues surrounding electronic transactions. However, through the use of the guide, the author hopes that there will be greater awareness of the legal issues surrounding electronic transactions, and greater understanding of the solutions offered in the Act in addressing these issues.

This guide attempts to state the law as of 31 August 1999.

About the Author

This guide was commissioned by the National Computer Board, and is written by Daniel Seng, Partner and Head of the Technology Practice Group in the law firm of Rajah & Tann. Daniel was formerly a Senior Lecturer with the Faculty of Law, National University of Singapore, and was a member of the Singapore Government's Electronic Commerce Hotbed Study Group On Legal, Regulatory and Enforcement Issues. This author wishes to express his thanks to Mr Charles Lim, Deputy Head, Legislation Division, Attorney-General's Chambers, who was the Chairmen of the Study Group, his colleagues on the Study Group, his National Computer Board counterparts and Mr Goh Seow Hiong, Deputy Controller of Certification Authorities, for all their help and assistance with this guide.

The following Act was passed by Parliament on 29th June 1998 and assented to by the President on 3rd July 1998:-

ELECTRONIC TRANSACTIONS ACT 1998

(No. 25 of 1998)

I assent.

ONG TENG CHEONG

President.

3rd July 1998.

An Act to make provisions for the security and use of electronic transactions and for matters connected therewith, and to make related amendments to the Interpretation Act (Chapter 1 of the 1997 Revised Edition) and the Evidence Act (Chapter 97 of the 1997 Revised Edition).

Be it enacted by the President with the advice and consent of the Parliament of Singapore, as follows :

PART I
PRELIMINARY

Short title and commencement

1.—(1) This Act may be cited as the Electronic Transactions Act 1998 and shall come into operation on such date as the Minister may, by notification in the *Gazette*, appoint.

(2) The Minister may appoint different dates for the coming into operation of the different provisions of this Act.

Commentary

The Electronic Transactions Act was passed by the Singapore Parliament on 29th June 1998 and received Presidential assent and became the law of the Republic of Singapore on 3rd July 1998. The whole Act was brought into force by the Minister on 10th July 1998 (S 369/98).

Interpretation

2. In this Act, unless the context otherwise requires —

"asymmetric cryptosystem" means a system capable of generating a secure key pair, consisting of a private key for creating a digital signature, and a public key to verify the digital signature;

"authorised officer" means a person authorised by the Controller under section 50;

"certificate" means a record issued for the purpose of supporting digital signatures which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair;

"certification authority" means a person who or an organisation that issues a certificate;

"certification practice statement" means a statement issued by a certification authority to specify the practices that the certification authority employs in issuing certificates;

"Controller" means the Controller of Certification Authorities appointed under section 41(1) and includes a Deputy or an Assistant Controller of Certification Authorities appointed under section 41(2);

"correspond" , in relation to a private key or public key, means to belong to the same key pair;

"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 —

(a) whether the transformation was created using the private key that corresponds to the signer's public key; and

(b) whether the initial electronic record has been altered since the transformation was made;

"electronic record" means a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or for transmission from one information system to another;

"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;

"hash function" means an algorithm mapping or translating one sequence of bits into another, generally smaller, set (the hash result) such that —

(a) a record yields the same hash result every time the algorithm is executed using the same record as input;

(b) it is computationally infeasible that a record can be derived or reconstituted from the hash result produced by the algorithm; and

(c) it is computationally infeasible that 2 records can be found that produce the same hash result using the algorithm;

"information" includes data, text, images, sound, codes, computer programs, software and databases;

"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;

"licensed certification authority" means a certification authority licensed by the Controller pursuant to any regulation made under section 42;

"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;

"private key" means the key of a key pair used to create a digital signature;

"public key" means the key of a key pair used to verify a digital signature;

"record" means information that is inscribed, stored or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form;

"repository" means a system for storing and retrieving certificates or other information relevant to certificates;

"revoke a certificate" means to permanently end the operational period of a certificate from a specified time;

"rule of law" includes written law;

"security procedure" means a procedure for the purpose of —

(a) verifying that an electronic record is that of a specific person; or

(b) detecting error or alteration in the communication, content or storage of an electronic record since a specific point in time,

which may require the use of algorithms or codes, identifying words or numbers, encryption, answerback or acknowledgment procedures, or similar security devices;

"signed" or "signature" and its grammatical variations includes any symbol executed or adopted, or any methodology or procedure employed or adopted, by a person with the intention of authenticating a record, including electronic or digital methods;

"subscriber" means a person who is the subject named or identified in a certificate issued to him and who holds a private key that corresponds to a public key listed in that certificate;

"suspend a certificate" means to temporarily suspend the operational period of a certificate from a specified time;

"trustworthy system" means computer hardware, software, and procedures that —

(a) are reasonably secure from intrusion and misuse;

(b) provide a reasonable level of availability, reliability and correct operation;

(c) are reasonably suited to performing their intended functions; and

(d) adhere to generally accepted security procedures;

"valid certificate" means a certificate that a certification authority has issued and which the subscriber listed in it has accepted;

"verify a digital signature" , in relation to a given digital signature, record and public key, means to determine accurately —

(a) that the digital signature was created using the private key corresponding to the public key listed in the certificate; and

(b) that the record has not been altered since its digital signature was created.

Commentary

"Asymmetric cryptosystems", "Certificates", "Certification Authority", "Electronic Signature", "Digital Signature"

In the electronic environment, the equivalent of a handwritten signature is the "electronic signature". Like the handwritten signature, the electronic signature takes the form of a certain digital letters or characters which are attached to or logically associated with an electronic record. But electronic signatures, like their handwritten counterparts, can be tampered with or even forged. Similarly, the electronic records which are authenticated by the electronic signatures can also be tampered with or forged. In fact, by their very nature, electronic signatures and electronic records are not secure and can be easily modified or altered.

The solution is to use a more secure form of electronic signatures, known as "digital signatures". Digital signatures work on the basis that there is a third party whom both parties trust, who can verify that the electronic signature applied by the sender to an electronic message is the same electronic signature which the recipient extracts from the received message. This trusted third party is the "certification authority", who is entrusted with the responsibility of verifying the message sender's identity. The sender, who may be a user or an organisation, first registers with the certification authority for an electronic identity. This electronic identity takes the form of a "certificate" issued by the certification authority. This certificate is in turn produced from an electronic key issued to the sender, which is only known to the sender. Like a secret personal code, the sender uses this key, which is normally stored on a secure device such as a smart card, to digitally sign his identity on the message. Upon receipt of the message, the recipient consults a trusted Certification Authority or a trusted repository of these electronic identities to ascertain the sender's electronic identity. This is by way of extracting from the certificate the public or verification key of the alleged sender. Through a mathematical process ("asymmetric

cryptosystems"), the electronic signature of the sender is compared against the public or verification key in the certificate. If they match, the recipient will have the assurance that it was the sender who sent the message, and that the message had not been altered since its transmission. The digital signature on the message will then be the electronic equivalent of a physical signature of the sender.

Purposes and construction

3. This Act shall be construed consistently with what is commercially reasonable under the circumstances and to give effect to the following purposes:

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

(b) to facilitate electronic commerce, 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 electronic filing of documents with government agencies and statutory corporations, and to promote efficient delivery of government services by means of reliable electronic records;

(d) to minimise the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions;

(e) to help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records; and

(f) to promote public confidence in the integrity and reliability of electronic records and electronic commerce, and to foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.

Commentary

This section, similar to the preamble found in laws of civil law countries, uniquely states the objectives to be met by the enactment of the Electronic Transactions Act. These objectives are stated to assist in the judicial interpretation and treatment of the various provisions in the Act. But the Singapore government's overriding philosophy is that laws should not unduly hinder the operation of businesses, which this section reinforces by stating that the legal rules in the Act should only operate in a commercially reasonable manner and consistently with the six enumerated objectives.

Simply put, the six avowed objectives of the Act relate to the use and legal recognition of electronic communications of electronic records, to promote electronic commerce.

In moving the Electronic Transactions Act in Parliament, Mr Lee Yock Suan, the Minister for Trade and Industry, said that the Act seeks to do the following:

(a) Enact a Commercial Code to support e-commerce transactions;

(b) Provide for a Public Key Infrastructure;

(c) Enable Electronic Applications and Licences for the Public Sector; and

(d) Clarify Network Service Providers' liability for third party content.

The organisation of the Electronic Transactions Act largely reflects these objectives. The Commercial Code to support e-commerce transactions is to be found in Part IV of the Act, and Parts II and V relate to the legal recognition and proof of electronic contracts, electronic records and electronic signatures. The provisions governing a public key infrastructure are spelt out in Parts VI, VII, VIII, IX, X and XII of the Act, whereas the provisions governing the use of electronic transactions to provide public sector services are found in Part IX of the Act. Finally, Part III of the Act sets out the position of the liability of network service providers.

Application

4. —(1) Parts II and IV shall not apply to any rule of law requiring writing or signatures in any of the following matters:

(a) the creation or execution of a will;

(b) negotiable instruments;

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

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

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

(f) documents of title.

(2) The Minister may by order modify the provisions of subsection (1) by adding, deleting or amending any class of transactions or matters.

Commentary

Under the Electronic Transactions Act, the general rule is that no discrimination is to be practised between the traditional forms of writing and signatures, and their electronic counterparts. The rules in this regard are to be found in Parts II and IV of the Act. However, there are several laws in Singapore that make it mandatory to effect by way of writing, or to record in writing, or to execute or witness by way of handwritten signatures, certain types of incidents, events or transactions. Writing here refers to non-electronic writings. For instance, the transfer of legal title to building units and to landed property is done in writing. It was felt necessary that these rules (specifically spelt out in this section) should not be changed by the Act. Hence this section preserves these legal rules and sanctions the discrimination, for the purposes of these rules, between traditional forms of writing and signatures, and their electronic counterparts. The list of the affected rules is spelt out in the section.

However, it is also accepted that with changing business environments, coupled with an increased awareness and growing confidence and trust in electronic transactions, writings and signatures, it may no longer be viable to preserve this distinction in these areas of the law. For instance, steps are being undertaken to have electronic bills of lading, which are documents of

title. Thus this section also reserves the power to the Minister to alter this list of affected legal rules as spelt out in the section.

Variation by agreement

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

Commentary

The paramount objective of the Electronic Transactions Act is to promote business practices that are commercially reasonable. The Act thus offers a template of legal rules to give effect to that overall objective. However, there may be circumstances where contracting parties may wish to either revert to non-electronic methods of doing business, or may insist on stricter standards to be observed in transacting electronically. These parties can do so by way of varying by agreement the provisions in Parts II and IV of the Act, that contain rules that concern the generating, sending, receiving, storing or processing of electronic records.

PART II
ELECTRONIC RECORDS AND SIGNATURES GENERALLY

Legal recognition of electronic records

6. For the avoidance of doubt, it is declared that information shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.

Commentary

This section states that a record that is in electronic form shall not have any less legal effect than an equivalent record in non-electronic form. Stated positively, it affirms that an electronic record shall have the same legal effect as a traditional, non-electronic, but otherwise equivalent, record. Hence if merchant A sends to merchant B a written order for goods, merchant B can send the invoice to merchant A in electronic form.

Requirement for writing

7. Where a rule of law requires information to be written, in writing, to be presented in writing or provides for certain consequences if it is not, an electronic record satisfies that rule of law if the information contained therein is accessible so as to be usable for subsequent reference.

Commentary

This section states that where there is any rule of law that requires information to be in writing, the same information can be stored in the form of an electronic record as long as the stored information can be subsequently retrieved. The effect of this section is that an electronic record can be used as a legally recognisable substitute for a document in writing. For instance,

insurance policies and contracts of guarantees can now be made in electronic form, even though the law previously required such documents to be in writing. Similarly, police officers can now record into their computers statements taken from witnesses when previously, they are required to do so in writing.

Electronic signatures

8. —(1) Where a rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law.

(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of such party.

Commentary

If a document is in an electronic form, how does the author of the document, or the parties, or the witnesses, sign the document? If they do so by way of an electronic signature, will this signature be given legal recognition?

This section sets all these doubts to rest by affirming that an electronic signature will be given legal effect as a signature. The legal concept of a signature is already very wide because it is not confined to handwritten signatures – businessmen are undoubtedly familiar with facsimile signatures which are commonly used on cheques, and company seals. This section is merely a logical extension of the same concept into the electronic environment, which is that any symbol or method used by a person with the intention of authenticating a record shall be a signature.

Proof that a signature, electronic or otherwise, has been applied to a document does not prevent parties from subsequent proof that the signature is a forgery, or that the signatory had applied his signature under duress or in ignorance of the true nature of the document.

See section 17 for a definition of a secure electronic signature.

Retention of electronic records

9. —(1) Where a rule of law requires that certain documents, records or information be retained, that requirement is satisfied by retaining them in the form of electronic records if the following conditions are satisfied:

(a) the information contained therein remains accessible so as to be usable for subsequent reference;

(b) 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;

(c) such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained; and

(d) the consent of the department or ministry of the Government, organ of State or the statutory corporation which has supervision over the requirement for the retention of such records has been obtained.

(2) An obligation to retain documents, records or information in accordance with subsection (1)(*c*) shall not extend to any information necessarily and automatically generated solely for the purpose of enabling a record to be sent or received.

(3) A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions in paragraphs (*a*) to (*d*) of that subsection are complied with.

(4) Nothing in this section shall —

(a) apply to any rule of law which expressly provides for the retention of documents, records or information in the form of electronic records;

(b) preclude any department or ministry of the Government, organ of State or a statutory corporation from specifying additional requirements for the retention of electronic records that are subject to the jurisdiction of such department or ministry of the Government, organ of State or statutory corporation.

Commentary

In certain circumstances, the law may require that certain records or information be retained. This could be due to various accounting, reporting or revenue requirements. But these documents or information can just as well be retained in electronic form. This section recognises and gives effect to these measures. However, to prevent any instance of fabrication, falsification or alteration to these electronic records, the retention of these records is subject to conditions, such as ensuring that the electronic record accurately represents the original information, and that identification information such as the origin, destination, date and time of the document are retained. In addition, where the retention of these records comes under the jurisdiction and supervision of a government agency or statutory corporation, it may impose additional requirements to ensure that it can continue to exercise proper supervision over the relevant activities and information which these records capture. Presumably, this will be by way of directives or subsidiary legislation issued by these agencies and corporations.

A person who wishes to comply with these requirements for maintaining electronic records can use the services of any other person to do so. For instance, he may subcontract his document managing operations to a specialist business for this purpose. However, the conditions as set out in subsection (1) must still be complied with.

It should be pointed out that this section goes beyond document imaging: it permits electronic information to be retained, regardless of whether or not the information is in the form of a paper document in the first place.

PART III
LIABILITY OF NETWORK SERVICE PROVIDERS

Liability of network service providers

10. —(1) 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 he merely provides access if such liability is founded on —

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

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

(2) Nothing in this section shall affect —

(a) any obligation founded on contract;

(b) the obligation of a network service provider as such under a licensing or other regulatory regime established under any written law; or

(c) any obligation imposed under any written law or by a court to remove, block or deny access to any material.

(3) For the purposes of this section —

"provides access", in relation to third-party material, means the provision of the necessary technical means by which third-party material may be accessed and includes the automatic and temporary storage of the third-party material for the purpose of providing access;

"third-party" , in relation to a network service provider, means a person over whom the provider has no effective control.

Commentary

By making available for access various types of materials, either from other network service providers or content providers, or from their own subscribers, a network service provider may be potentially subjected to civil or criminal liability to such third-party material. Liability may arise from the service it provides in making available such materials, as a result of which the offending materials or the statements in the materials are made, published, disseminated or distributed, or as a result of which there is an infringement of any rights subsisting in such materials. For instance, the network service provider may be potentially liable in making available material that defames a person. Or the network service provider may unwittingly assist a subscriber in disseminating pornography, or software that infringes copyright. This section absolves the network service provider of all of such liability, provided the network service provider "merely provides access" to such offending materials and their statements. "Providing access" here includes activities such as the automatic and temporary storage of material which is a necessary part of providing access to such materials. However, the network service provider still has to observe its contractual obligations, or any legal obligations under a regime such as the Singapore Broadcasting Authority's licensing rules, or orders of court.

PART IV
ELECTRONIC CONTRACTS

Formation and validity

11. —(1) For the avoidance of doubt, it is declared that in the context of the formation of contracts, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of electronic records.

(2) 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.

Commentary

This section affirms that parties can make a contract, which is legally constituted by an offer and the acceptance of the offer, by means of electronic records. So if A makes B an offer by e-mail to sell to B his second-hand graphics card for $10, and B sends an e-mail back to A, accepting the offer, the contract, which is constituted by the electronic records of the offer and acceptance, has legal effect.

Effectiveness between parties

12. 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.

Commentary

As parties engage in pre-contractual negotiations, they normally make representations and other statements which precede the making of the actual contract. This section states that if such representations and statements take electronic form, they will have similar legal effect as if they were made in the traditional form.

Attribution

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

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

(a) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

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

(3) 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 —

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

(b) 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.

(4) Subsection (3) shall not apply —

(a) 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;

(b) in a case within subsection (3)(*b*), at any time when the addressee knew or ought to have known, had it exercised reasonable care or used any agreed procedure, that the electronic record was not that of the originator; or

(c) 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.

(5) 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.

(6) 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.

(7) 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 another electronic record and the addressee knew or should have known, had the addressee exercised reasonable care or used any agreed procedure, that the electronic record was a duplicate.

(8) Nothing in this section shall affect the law of agency or the law on the formation of contracts.

Commentary

All the previous sections merely have the effect of affirming the application of traditional rules to the electronic environment. But for these rules to operate effectively, there must be additional rules to help the courts and the parties ascertain to whom these rules apply. For instance, section 11 states that an offer can take electronic form. But there may be a dispute as to whether the offer was indeed sent by the offeror, or whether the offeree received the offer. For the rules governing the electronic environment to work, there must be additional rules to allow the courts to attribute these electronic messages to one party or to another.

This section achieves this role with a series of escalating rules that are summarised as follows:

- If A (the party who allegedly sent the electronic message – referred to in the Act as the "originator") did send the message to B (the party who allegedly received the electronic message – referred to as the "addressee"), the message is A's.
- If B receives a message allegedly sent by A, it will be deemed to be A's message if it was sent by A's agent.

- If B receives a message allegedly sent by A, it will be deemed to be A's message if it was sent by a computer system programmed by A, or programmed by A's agent.
- If B receives a message allegedly sent by A, B is entitled to regard it as A's if B applied a procedure, either previously agreed to by A or implemented by someone related to A, for verifying that the message is A's, but not from the point in time when A informed B that the message is not his, and gives B reasonable time to act, or when B knows or ought to know that the message was not A's.

Acknowledgment of receipt

14. —(1) Subsections (2), (3) and (4) 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.

(2) 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 —

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(3) 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.

(4) 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 —

(a) 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

(b) if the acknowledgment is not received within the time specified in paragraph (*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.

(5) 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.

(6) 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.

(7) Except in so far as it relates to the sending or receipt of the electronic record, this Part is not intended to deal with the legal consequences that may flow either from that electronic record or from the acknowledgment of its receipt.

Commentary

However, parties may feel uncomfortable at allowing one party such as B to bind another such as A with an electronic message if A does not have any confirmation that B has received the message. In such a case, this section allows A to require B to acknowledge the receipt of the message. A and B may agree that the acknowledgement be given by B in any form, communicated by B to A upon the receipt of the message, or by B acting on the receipt of the message . If A specifies to B that his message to B is conditional upon receiving this acknowledgement, which B fails to send, A's message will be of no effect. On the other hand, if A fails to tell B that his message is conditional upon receiving an acknowledgement from B, A may reimpose this requirement of an acknowledgements on B.

The effect of these rules is that when parties transact across an electronic transmission medium that cannot guarantee the receipt of messages, parties may wish to impose the requirement that the party who receives a message confirms its receipt with the originator of the message. This is especially important when parties are transmitting critical messages and they need confirmation that the other party has received such messages. A statement in the acknowledgement that the received record met certain technical requirements also leads to the presumption that such requirements have been met. However, the acknowledgement that the message has been received is only a presumption. It can be rebutted if it is proved otherwise. Similarly, the acknowledgement does not imply that the record received has not been altered or tampered with in transit.

Time and place of despatch and receipt

15. —(1) Unless otherwise agreed to between the originator and the addressee, the despatch 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.

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

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

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

(ii) 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; or

(b) if the addressee has not designated an information system, receipt occurs when the electronic record enters an information system of the addressee.

(3) Subsection (2) 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 subsection (4).

(4) Unless otherwise agreed between the originator and the addressee, an electronic record is deemed to be despatched 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.

(5) For the purposes of this section —

(a) 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;

(b) 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

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

(6) This section shall not apply to such circumstances as the Minister may by regulations prescribe.

Commentary

There is some uncertainty as to how the rules applying to the despatch and receipt of paper documents are applicable to their electronic counterparts. This section seeks to resolve this by having rules prescribing when electronic messages are despatched and when they are received, and the places of their despatch and receipt. These rules may be summarised as follows:

- A message is despatched when it enters a computer system that is outside the control of the originator of the message or his agent who sent the message on his behalf.
- The place where the message is despatched is the place where the originator has his place of business.
- A message is received when the message enters a computer system that the addressee designated for receiving messages. If the message is sent to a non-designated computer system, it is received when the addressee retrieves the message. Where no such computer system is designated, the message is received when it enters any computer system of the addressee.
- The place where the message is received is the place where the addressee has his place of business.

These rules ensure that computer mailboxes can be treated as registered offices for the "posting" of electronic messages. These provisions may also be used to avoid disputes between parties who might claim that the messages were never sent to them or they had never read these messages.

PART V
SECURE ELECTRONIC RECORDS AND SIGNATURES

Secure electronic record

16. —(1) If a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved has been properly applied to an electronic record 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.

(2) For the purposes of this section and section 17, whether a security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including —

(a) the nature of the transaction;

(b) the sophistication of the parties;

(c) the volume of similar transactions engaged in by either or all parties;

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

(e) the cost of alternative procedures; and

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

Commentary

Electronic records are by their very nature susceptible to unauthorised modification or tampering. To protect these records against these activities, these records have to be "secured". An electronic record becomes a "secure electronic record" if a security procedure is applied to it. This security procedure makes it possible to determine if the record is that of a specific person, or to detect any alterations or errors in the communication, content or storage of the electronic record since a specific point in time. However, not every security procedure will make an electronic record secure. It has to be a commercially reasonable procedure agreed to by the parties, or, in the absence of such an agreement, a procedure prescribed in the Act, *ie* digital signatures and the use of the public key infrastructure.

Secure electronic signature

17. If, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made —

(a) unique to the person using it;

(b) capable of identifying such person;

(c) created in a manner or using a means under the sole control of the person using it; and

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

such signature shall be treated as a secure electronic signature.

Commentary

If a party signs a record electronically, with the intention of authenticating or approving the record, like their paper-based counterparts, these electronic signatures can be forged. Alternatively, perpetrators can impersonate the electronic signatures of their victims if they have access to them. To protect against such activities, various security procedures can be applied to an electronic signature such that it can be verified that the signature is, at the time it was made, unique to the signatory, capable of identifying such a person as the signatory, and to which no one else has access. In addition, the signature has to be linked to the electronic record to which it is applied, so that any tampering with the electronic record can be detected.

Again, like the previous section, the security procedure has to be one that is a commercially reasonable procedure agreed to by the parties, or, in the absence of such an agreement, a procedure prescribed in the Act, *ie* digital signatures and the use of the public key infrastructure.

Presumptions relating to secure electronic records and signatures

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

(2) In any proceedings involving a secure electronic signature, it shall be presumed, unless evidence to the contrary is adduced, that —

(a) the secure electronic signature is the signature of the person to whom it correlates; and

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

(3) 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.

(4) For the purposes of this section —

"secure electronic record" means an electronic record treated as a secure electronic record by virtue of section 16 or 19;

"secure electronic signature" means an electronic signature treated as a secure electronic signature by virtue of section 17 or 20.

Commentary

Where an electronic record has been rendered secure, as described in section 16, it shall be presumed that the record has not been altered since the point in time when the record is made secure. So parties can act on a secure electronic record on the assumption that it was not tampered with.

Similarly, if an electronic signature, which is a secure signature as described in section 17, is applied, it shall be presumed that the signature is that of the signatory, and that the signatory applied his signature to authenticate or approve of the electronic record. Again, the recipient of

an electronic record signed with a secure electronic signature can presume that based on the secure electronic signature, the sender is the originator of the electronic record, and he cannot easily repudiate his signature on the electronic record.

In the absence of the use of such security procedures, no such presumptions will arise for electronic records and electronic signatures.

PART VI
EFFECT OF DIGITAL SIGNATURES

Secure electronic record with digital signature

19. 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 20.

Commentary

Part VI of the Act deals with the use of digital signatures in the electronic environment generally. In particular, digital signatures can be used as part of the prescribed security procedure to secure electronic records. So if a portion of an electronic record is signed with a digital signature, since the digital signature allows a party to ascertain if the initial electronic record was altered since the signature was applied, that portion of the electronic record is treated as a secure electronic record.

Secure digital signature

20. 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 —

(i) the certificate was issued by a licensed certification authority operating in compliance with the regulations made under section 42 ;

(ii) the certificate was issued by a certification authority outside Singapore recognised for this purpose by the Controller pursuant to regulations made under section 43;

(iii) the certificate was issued by a department or ministry of the Government, an organ of State or a statutory corporation approved by the Minister to act as a certification authority on such conditions as he may by regulations impose or specify; or

(iv) the parties have expressly agreed between themselves (sender and recipient) to use digital signatures as a security procedure, and the digital signature was properly verified by reference to the sender's public key.

Commentary

Digital signatures can themselves be compromised or used in ways to perpetrate forgery. Hence mechanisms ought to be put in place to ensure that a digital signature is unique to the person using it, is capable of identifying such a person, and is created and used under the sole control of the person using it. Similarly, the public key that is stored in a certificate and is used to verify the digital signature can itself be compromised, or may be an unreliable indicator of the subscriber's electronic identity. For this reliance on the certificate to be justified, it must accurately associate the public key which it lists with a person's identity, and be accepted as such by that person, also known as the subscriber. In addition, this information in the certificate must be current – thus the reference to the operational period of a valid certificate. This section sets out all these circumstances. In addition, this section also states that the responsibility for ensuring the trustworthiness of the certificate can be undertaken by licensed, recognised (overseas) or approved certification authorities. Where the approved certification authorities are Government departments, organs of state or statutory corporations, such certification authorities must comply with certain provisions in the Electronic Transactions (Certification Authority) Regulations 1999 as if it were a licensed certification authority. See paragraph 32 of the said Regulations.

See also paragraph 25 of the Electronic Transactions (Certification Authority) Regulations 1999 for the technical treatment of what constitutes a secure digital signature as implemented by way of certificates issued by a licensed certification authority.

Presumptions regarding certificates

21. It shall be presumed, unless evidence to the contrary is adduced, that the information (except for information identified as subscriber information which has not been verified) listed in a certificate issued by a licensed certification authority is correct if the certificate was accepted by the subscriber.

Commentary

Where a certificate is issued by a certification authority, the subscriber has the opportunity of confirming that his identity and other particulars are accurately associated with his public key. Under paragraph 16(6) of the Electronic Transactions (Certification Authority) Regulations 1999, the subscriber has to be given a reasonable opportunity to verify the contents of the certificate before it is accepted. If the subscriber does not accept the certificate, the licensed certification authority must not publish it (paragraph 16(9) of the Electronic Transactions (Certification Authority) Regulations 1999). Hence where the certificate is issued by a licensed certification authority, any party can presume that such information published in the certificate is correct, except in the case of information which is expressly stated as unverified information.

Unreliable digital signatures

22. Unless otherwise provided by 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 electronic 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) any usage of trade, particularly trade conducted by trustworthy systems or other electronic means.

Commentary

Although the recipient of an electronic record that is signed with a secure digital signature is entitled to presume that the record has not been altered, and that the record had been signed by the signatory of the person to whom the digital signature correlates, this is only a presumption which can be rebutted by adducing evidence to the contrary.

In addition, where it is unreasonable to rely on the digital signature to verify the identity of the originator of the message, or to authenticate the electronic record, the risk will be on the person so relying if this reliance turns out to be misplaced. For instance, it may be shown that the security of the repository has been compromised, or that someone had continued to impersonate as the originator even though he had revoked his digital certificate. This section does not spell out the ways in which the electronic record or digital signature can be proven to be invalid. This will vary from situation to situation. Instead, it sets out some of the circumstances in which it will be unreasonable for the recipient to rely on the digital signature. So if the recipient of the electronic record knows that it could not have been possible for the originator to have sent the record, he could not rely on the alleged originator's digital signature. Similarly, if the electronic record is a very important one, it may have been unreasonable for the recipient to have relied on the originator's digital signature without seeking additional means of confirmation. And again, the course of dealing between the parties and the usage of trade may provide the recipient with some indication that the originator's digital signature was unusual, or was executed in unusual circumstances. If having regard to these factors set out in this section, it was unreasonable for the party to have so relied on the originator's digital signature, this party will bear the risk of any losses that flow from his misplaced reliance.

PART VII
GENERAL DUTIES RELATING TO DIGITAL SIGNATURES

Reliance on certificates forseeable

23. It is foreseeable that persons relying on a digital signature will also rely on a valid certificate containing the public key by which the digital signature can be verified.

Commentary

This section confirms the that it is foreseeable that a party who relies on a digital signature will also rely on a valid certificate containing the public key, from which the digital signature can be derived and verified. A certificate is only valid if a certification authority has issued it (see section 29), and the subscriber listed in it has accepted it. This reliance is a matter of necessity because, as is explained in the commentary for section 2, the subscriber's certificate contains the public key which is used to verify the digital signature of the subscriber. Hence the statement in paragraph 21(5) of the Electronic Transactions (Certification Authority) Regulations 1999 that it is the responsibility of any person relying on the certificate to check whether the certificate has been suspended.

Prerequisites to publication of certificate

24. No person may publish a certificate or otherwise make it available to a person 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 that 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.

Commentary

The public key infrastructure system presupposes that not only are the contents of published certificates are accurate, but also that the certificates are properly published. Where the certification authority listed in the certificate has not issued the certificate, or the subscriber listed in the certificate has not accepted it, or where the certificate has been revoked or suspended, this section imposes a duty on the person who knows that that is the case not publish it or make it available.

Publication for fraudulent purpose

25. Any person who knowingly creates, publishes or otherwise makes available a certificate for any fraudulent or unlawful purpose shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 2 years or to both.

Commentary

To ensure that the public key infrastructure system for publishing or making available digital certificates is not abused, this section makes it an offence for a person to create, publish or make available a certificate for a fraudulent or unlawful purpose.

False or unauthorised request

26. Any person who knowingly misrepresents to a certification authority his identity or authorisation for the purpose of requesting for a certificate or for suspension or revocation of a certificate shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 6 months or to both.

Commentary

Similarly, the public key infrastructure system is only as accurate as the information which the subscriber supplies to the certification authority for generation of his certificate for eventual publication. This section makes it an offence for a subscriber to knowingly misrepresent his identity or authorisation for the purpose of requesting for a certificate.

Conversely, a certificate may be removed from the repository without the permission of its subscriber though it is still valid. The integrity of the repository of certificates will be affected. Thus this section also makes it an offence for such a person to seek the suspension or revocation of a certificate by misrepresenting himself as the subscriber, or by misrepresenting himself to be authorised by the subscriber for this purpose.

PART VIII
DUTIES OF CERTIFICATION AUTHORITIES

Commentary

Part VIII of the Act sets out the duties which have to be observed by certification authorities. The Explanatory Statement to the Bill notes that all these duties have to be observed by all certification authorities, regardless of whether or not they are licensed by the Controller of Certification Authorities under section 42 of the Act. The provisions in this Part of the Act only state the duties to be observed by all certification authorities, but do not spell out the legal sanctions if these duties are breached. Presumably, breach of these duties will give rise to an action at common law for breach of statutory duty. In addition, the Controller may, pursuant to his powers under section 51 of the Act, issue a notice in writing to direct the certification authority to comply with these provisions, failing which the certification authority shall be guilty of an offence under section 51.

Trustworthy system

27. A certification authority must utilise trustworthy systems in performing its services.

Commentary

Because users of the public key infrastructure maintained by certification authorities rely on these authorities to provide accurate subscriber information via digital certificates, section 27 of the Act imposes a duty on a certification authority to use trustworthy systems when performing its services. This presumably refers to all aspects of its services related to the issuance, renewal, suspension and revocation of a certificate. A trustworthy system refers to a system comprising hardware, software and procedures that are reasonably secure from intrusion and misuse, provide a reasonable level of availability, reliability and correct operation, are reasonably suited to performing their intended function, and adhere to generally accepted security procedures. A licensed certification authority is subjected to an audit of his security, one of which is an assessment of whether its system is trustworthy. See paragraph 26(3)(c), Electronic Transactions (Certification Authority) Regulations 1999.

Disclosure

28. —(1) A certification authority shall disclose —

(a) its certificate that contains the public key corresponding to the private key used by that certification authority to digitally sign another certificate (referred to in this section as a certification authority certificate);

(b) any relevant certification practice statement;

(c) notice of the revocation or suspension of its certification authority certificate; and

(d) 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.

(2) 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 —

(a) use reasonable efforts to notify any person who is known to be or foreseeably will be affected by that occurrence; or

(b) act in accordance with procedures governing such an occurrence specified in its certification practice statement.

Commentary

Section 28 sets out the disclosure duties to be observed by a certification authority. As is prescribed in paragraph 19(7) of the Electronic Transactions (Certification Authority) Regulations 1999, licensed certification authorities must digitally sign the issued certificates of their subscribers. This is to ensure that the certificates cannot be easily tampered with (see section 19, since the certificate is itself also an electronic record). To support this practice, section 28 requires a certification authority to make publicly available its own certificate (known as a certification authority certificate ('CAC')) that contains the public key that corresponds to the private key used by the certification authority to sign its subscribers' certificates. It also follows that where this CAC is revoked or suspended, *eg* because the certification authority has terminated its services, or because its security or even the private key that corresponds to the CAC has been compromised, the certification authority is required to make a notification on this matter.

Similarly, the certification authority is required to disclose the various practices that it employs in issuing its certificates in the form of a certification practice statement ('CPS'). This statement is vital to both the subscribers of the certification authority's certificates, as well as to those parties who rely on these certificates, because this allows both subscribers and those who rely on the certificates to properly assess and evaluate the trustworthiness and reliability of the certification authority's certificates, based on the nature of the transactions which these parties may be engaged in. The issuance of the CPS also constitutes part of the representation given by the certification authority in relation to the certificates that it issues (see section 30).

Section 28 also sets out the catch-all: to ensure transparency and accountability in its operations, the certification authority is required to disclose "any other fact that materially and adversely affects" the certification authority's issued certificates and its ability to perform its services.

And to whom must these disclosures be made? Paragraph 2 to section 28 imposes a duty on the certification authority to "use reasonable efforts" to notify any person known to be or foreseeably will be affected by any occurrence that will materially and adversely affect its trustworthy system or its CAC. But the certification authority can avoid this more onerous duty and instead choose to act in accordance with the procedure which it has prescribed for this purpose as spelt out in its CPS.

Issuing of certificate

29. —(1) A certification authority may issue a certificate to a prospective subscriber only after the certification authority —

(a) has received a request for issuance from the prospective subscriber; and

(b) has —

(i) 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

(ii) in the absence of a certification practice statement, complied with the conditions in subsection (2).

(2) In the absence of a certification practice statement, the certification authority shall confirm by itself or through an authorised agent that —

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

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

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

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

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

(f) 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.

Commentary

Section 29 sets out the duties to be observed by a certification authority before it issues a subscriber's certificate. Since the certificate is a representation of the subscriber's identity in the digital environment (see definition of "certificate"), the certification authority has to confirm that there has actually been a request for a certificate to be issued from the prospective subscriber. In addition, the certification authority must observe all practices and procedures in relation to the issuing of certificates, in particular, the procedures regarding the identification of the prospective subscriber. These procedures can, for instance, require the prospective subscriber to be physically identified by the certification authority. However, identification by proxy *eg* where the certification authority authorises an agent to verify the identities of the subscribers, is also possible (see section 29(2) – "shall confirm by itself or through an authorised agent"). Where these procedures are set out by the certification authority in its CPS, these must be complied with. In their absence, the procedures spelt out in section 29(2) have to be observed. In summary, these procedures are put in place to confirm that the person listed in the certificate is the prospective subscriber, to require the verification of the reliability of other information included in the certificate, and to ensure that the prospective subscriber holds the private key that corresponds to the public key listed in the certificate, and that both the private and public keys can be used to create and verify digital signatures.

Representations upon issuance of certificate

30. —(1) 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 issued the certificate in accordance with any applicable certification practice statement incorporated by reference in the certificate, or of which the relying person has notice.

(2) In the absence of such certification practice statement, the certification authority represents that it has confirmed that —

(a) the certification authority has complied with all applicable requirements of this Act 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;

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

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

(d) 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

(e) 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 paragraphs (*a*) to (*d*).

(3) Where there is an applicable certification practice statement which has been incorporated by reference in the certificate, or of which the relying person has notice, subsection (2) shall apply to the extent that the representations are not inconsistent with the certification practice statement.

Commentary

As set out in section 23, reliance on a digital signature also connotes foreseeable reliance on a valid certificate containing the public key by which the digital signature can be verified. Section 30 takes this reliance one step further by explicating the content and substance of this reliance. It states that the certification authority by issuing the certificate represents to any person who reasonably relies on the certificate that it has been issued in accordance with the certification authority's CPS, or, in its absence, the representations set out in section 30(2). In a nutshell, the representations are that the certification authority has complied with all applicable requirements of the Act in issuing the certificate, that the subscriber identified in the certificate has accepted it, that he holds the private key corresponding to the public key listed in the certificate, that the public and private key pair are functional, that all the information in the certificate is accurate (unless otherwise excepted) and that the certification authority has no knowledge of any material fact outside the certificate which will materially affect the above representations.

Suspension of certificate

31. 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 —

(a) the subscriber listed in the certificate;

(b) a person duly authorised to act for that subscriber; or

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

Commentary

On the subscriber's authority arising out of his acceptance, the issuance of the certificate by the certification authority is a continuing representation on the subscriber's identity. Thus the subscriber is entitled to take steps to request the certification authority to "suspend" the certificate. The subscriber may wish to suspend his certificate if, for instance, he suspects that his private key has been compromised, or if the subscriber is an employee who is leaving the employment of the firm. The Act defines the "suspension" of a certificate, as the temporary deactivation of the operation of the certificate.

When such a request is made, the certification authority shall take steps to suspend the certificate "as soon as possible", after it has verified the authenticity of this request to suspend the certificate. However, section 31 leaves room for the certification authority and the subscriber to reach an agreement that varies the operation of this section.

Suspension of the certificate is often a precursor to its eventual revocation. See paragraphs 21(7) and (9) of the Electronic Transactions (Certification Authority) Regulations 1999.

Revocation of certificate

32. A certification authority shall revoke a certificate that it issued —

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

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

(c) upon presentation of documents effecting a dissolution of the subscriber, or upon confirming by other evidence that the subscriber has been dissolved or has ceased to exist.

Commentary

As explained above, the certification authority derives its right to represent the subscriber's identity via the issued certificate only upon the continuing authority of the subscriber. The subscriber's authority may however be terminated, leading to a similar termination of the certificate. The "revocation" of a certificate is defined as the permanent ending of the operation of a certificate. The suspension of a certificate is temporary – it will presumably be reinstated and its operation restored, whereas the termination of a certificate is permanent – it will presumably be permanently withdrawn from use.

On the subscriber's authority arising out of his acceptance, the issuance of the certificate by the certification authority is a continuing representation on the subscriber's identity. Thus the subscriber is entitled to withdraw this authority, and when this authority is withdrawn, either expressly (by way of a request made by the subscriber or his agent – section 32(a), or presentation of dissolution documents – section 32(c)), or impliedly (by notice of the death of the subscriber, if the subscriber is a natural person – section 32(b), or confirmation by way of other evidence – section 32(c)).

Revocation without subscriber's consent

33. —(1) A certification authority shall revoke a certificate, regardless of whether the subscriber listed in the certificate consents, if the certification authority confirms that —

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

(b) a 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;

(d) an individual subscriber is dead; or

(e) a subscriber has been dissolved, wound-up or otherwise ceased to exist.

(2) Upon effecting such a revocation, other than under subsection (1)(*d*) or (*e*), the certification authority shall immediately notify the subscriber listed in the revoked certificate.

Commentary

The previous sections impose a duty on the certification authority to suspend or revoke the subscriber's certificate, upon either the subscriber or a third party presenting documents or evidence to substantiate his request. Section 33, however, imposes a duty on the certification authority to revoke a certificate on its own initiative. This is to be done when the certification authority confirms that (a) there is a material misrepresentation in the certificate, (b) a requirement for the issue of the certificate (as set out in section 29) was not satisfied, (c) there has been a compromise to the certification authority's private key (thus negating the CAC) or the trustworthiness of its system (see section 27) which it uses to perform its services, (d) the death of an individual subscriber, or (e) the dissolution or cessation of an artificial persona such as a company as a subscriber.

Notice of suspension

34. —(1) Immediately upon suspension of a certificate by a certification authority, the certification authority shall publish a signed notice of the suspension in the repository specified in the certificate for publication of notice of suspension.

(2) Where one or more repositories are specified, the certification authority shall publish signed notices of the suspension in all such repositories.

Commentary

The procedure to be observed by the certification authority upon the suspension of a certificate is spelt out in this section. Section 34 requires the certification authority to *immediately* publish a signed notice of the suspension in one or all of the relevant repositories. These repositories for publication of notices of suspension have been previously specified in the suspended certificate. Hence before a user relies on the certificate, he should check with the specified repositories to ascertain the validity of the certificate.

Notice of revocation

35. —(1) Immediately upon revocation of a certificate by a certification authority, the certification authority shall publish a signed notice of the revocation in the repository specified in the certificate for publication of notice of revocation.

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

Commentary

The procedure to be observed by the certification authority upon the revocation of a certificate is similar to that for suspension of a certificate.

PART IX
DUTIES OF SUBSCRIBERS

Commentary

The efficacy and reliability of the public key infrastructure depends on the co-operation of the subscribers with the certification authorities in maintaining the certification system. Part IX of the Act imposes certain various legal obligations on the subscribers for this purpose.

Generating key pair

36. —(1) 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.

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

Commentary

One of the most critical aspects of setting up the public key infrastructure is the generation and assignment of a public-private key pair to the subscriber to uniquely identify the subscriber. Like the certification authority (see section 27), the subscriber must use a trustworthy system to generate this key pair. A public-private key pair generated by an untrustworthy system may lead to, for instance, the disclosure of the subscriber's private key, the choice of a key-pair which is too short to be secure because it can too easily be cracked, or the assignment of the same public-private key pair to two or more subscribers. Hence the requirement that either the subscriber uses a trustworthy system to generate this key pair, or uses a certification authority approved system to generate this key pair. As to the latter, the subscriber can generate his key pair on his own personal computer, or have a certificate processor who is approved by the certification authority to generate his key pair for him.

Obtaining certificate

37. 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.

Commentary

Section 37 provides that when the subscriber supplies information to the certification authority for purposes of obtaining a certificate, he shall supply accurate and complete information to the best of his knowledge and belief. This obligation to do so exists independently of the certification authority's duty (see section 29(2)(c)) to confirm that all the information in the certificate to be issued is accurate.

Acceptance of certificate

38. —(1) A subscriber shall be deemed to have accepted a certificate if he —

(a) publishes or authorises the publication of a certificate —

(i) to one or more persons; or

(ii) in a repository; or

(b) otherwise demonstrates approval of a certificate while knowing or having notice of its contents.

(2) By accepting a certificate issued by himself or a certification authority, the subscriber listed in the certificate certifies to all who reasonably rely on the information contained in the certificate

that —

(a) the subscriber rightfully holds the private key corresponding to the public key listed in the certificate;

(b) all representations made by the subscriber to the certification authority and material to the information listed in the certificate are true; and

(c) all information in the certificate that is within the knowledge of the subscriber is true.

Commentary

After the certificate is issued by the certification authority, it has to be accepted by the subscriber before it can be published (see section 24). By publishing it, the publisher is representing that the subscriber listed in the certificate has accepted it (see section 24). In addition, if the certification authority is also the publisher or has made the certificate available to a person who relies on it, the certification authority also represents that the subscriber listed in the certificate has accepted it (see section 30). By section 38(2), the acceptance of a certificate by the subscriber amounts to a certification to all who reasonably rely on the information contained in the certificate that the subscriber is related to the public key listed in the certificate, that the subscriber has made true representations to the certification authority that is material to the information listed in the certificate, and that within the subscriber's knowledge, the information in the certificate is true.

Acceptance of the certificate triggers its publication and subsequent reliance by third parties. A certificate can be accepted by a subscriber in two ways: the subscriber can expressly publish the certificate himself, or authorise its publication (s 38(1)(a)), or he can "demonstrate approval of a certificate while knowing or having notice of its contents", ie publication by acquiescence (s 38(1)(b)).

Control of private key

39. —(1) 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 prevent its disclosure to a person not authorised to create the subscriber's digital signature.

(2) Such duty shall continue during the operational period of the certificate and during any period of suspension of the certificate.

Commentary

Accompanying the subscriber's representation that he holds the private key that corresponds to the public key listed in the published certificate (see section 38(1)) is the subscriber's duty to exercise reasonable care to retain control of the private key so that it is exclusively his. The subscriber is also under a legal duty to prevent its disclosure to an unauthorised person.

This duty subsists during the operational period of the certificate. It also continues during any period of suspension of the certificate. The duty lapses with the termination of the certificate, since it would no longer be valid. Hence it is vitally important for a third party who is relying on the certificate to ascertain that it is current and valid.

Initiating suspension or revocation

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

Commentary

Not only can the private-public key pair be compromised when it is generated; it can also be subsequently compromised *eg* through the disclosure of the private key to unauthorised persons, or breach of confidence or duty on the part of persons entrusted by the subscriber with the private key. Section 40 places an obligation on the subscriber to "as soon as possible" request the issuing certification authority to suspend or revoke the certificate should this happen.

PART X
REGULATION OF CERTIFICATION AUTHORITIES

Commentary

The Act does not require all certification authorities to be licensed. Instead, it adopts a voluntary licensing regime. Certification authorities operating in Singapore can apply to be licensed by the Controller of Certification Authorities ('CCA') pursuant to regulations made by the Minister under section 42. It is not correct to conclude, as the heading for this Part appears to suggest, that certification authorities that are not licensed are unregulated: these certification authorities still have to comply with the other relevant provisions as set out in the Act, for instance, the provisions in Part VIII of the Act that spell out the duties of *all* certification authorities. The list of certification authorities currently licensed by the CCA is published on the CCA website at www.cca.gov.sg.

Besides licensed certification authorities, there are three other groups of certification authorities whose digital certificates can be given legal effect: foreign certification authorities recognised by the CCA (see section 43), Government departments or ministries approved by the Minister (see

section 20(b)(iii)) and those "certification authorities" whose "certificates" the parties have expressly agreed to recognise (see section 20(b)(iv)).

Appointment of Controller and other officers

41. —(1) The Minister shall appoint a Controller of Certification Authorities for the purposes of this Act and, in particular, for the purposes of licensing, certifying, monitoring and overseeing the activities of certification authorities.

(2) The Controller may, after consultation with the Minister, 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 any regulations made thereunder.

(3) The Controller, the Deputy and Assistant Controllers and officers appointed by the Controller under subsection (2) shall exercise, discharge and perform the powers, duties and functions conferred on the Controller under this Act or any regulations made thereunder subject to such directions as may be issued by the Minister.

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

(5) 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 licensed certification authority.

Commentary

This section provides for the appointment of a Controller of Certification Authorities as well as other Deputy and Assistant Controllers and officers. The appointment of the CCA and its Deputy and Assistant Controllers and officers are under the purview of the National Computer Board. The CCA is responsible for the licensing, certifying, monitoring and overseeing of the activities of certification authorities. Its supervision extends beyond licensed certification authorities to include certification authorities that are not licensed (for instance, the various provisions in Part XII that confer power on the CCA to give directions to certification authorities for compliance with the Act, or to investigate the activities of a certification authority in this regard). In turn, the CCA is required to maintain a public database containing a certification authority disclosure record for each certification authority which it licenses, setting out the particulars of the licensed certification authority. Where the CCA issues certificates, the CCA is in turn deemed to be a licensed certification authority. The responsibilities of the CCA are to be found in the Act and the regulations.

Regulation of certification authorities

42. —(1) The Minister may make regulations for the regulation and licensing of certification authorities and to define when a digital signature qualifies as a secure electronic signature.

(2) Without prejudice to the generality of subsection (1), the Minister may make regulations for or with respect to —

(a) applications for licences or renewal of licences of certification authorities and their authorised representatives and matters incidental thereto;

(b) the activities of certification authorities including the manner, method and place of soliciting business, the conduct of such solicitation and the prohibition of such solicitation of members of the public by certification authorities which are not licensed;

(c) the standards to be maintained by certification authorities;

(d) prescribing the appropriate standards with respect to the qualifications, experience and training of applicants for any licence or their employees;

(e) prescribing the conditions for the conduct of business by a certification authority;

(f) 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;

(g) prescribing the form and content of a digital certificate or key;

(h) prescribing the particulars to be recorded in, or in respect of, accounts kept by certification authorities;

(i) 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;

(j) 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 variation of such requirements, conditions or restrictions as the Controller may think fit;

(k) the manner in which a holder of a licence conducts its dealings with its customers, conflicts of interest involving the holder of a licence and its customers, and the duties of a holder of a licence to its customers with respect to digital certificates;

(l) prescribing forms for the purposes of the regulations; and

(m) prescribing fees to be paid in respect of any matter or thing required for the purposes of this Act or the regulations.

(3) Regulations 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 $50,000 or imprisonment for a term not exceeding 12 months or both.

Commentary

This section provides for the Minister to make regulations for the regulation and licensing of certification authorities. It also allows the Minister to define by way of regulations when a digital signature qualifies as a secure electronic signature. Presumably, this allows the Minister to make rules which will render digital signatures secure electronic signatures where they would otherwise not qualify as secure electronic signatures pursuant to section 20. In other words, this section allows the Minister to extend the scope of section 20 of the Act by way of regulations.

Section 42(2) spells out, in detail, the particulars of various regulations that the Minister may make. These are in relation to the administration of licensed certification authorities (eg licence applications and renewals, forms, fees), standards to be observed and maintained by certification authorities (eg prescribing the form and content of a digital certificate or key, establishment and regulation of any electronic system, qualifications of applicants), conduct of business (eg soliciting and advertising, qualifications of the certification authority's employees) and auditing of the certification authority's accounts (eg the particulars to be recorded in and of the various accounts kept).

In exercise of his powers conferred upon him by this section and section 61, the Minister for Trade and Industry has made the Electronic Transactions (Certification Authority) Regulations 1999. The Regulations came into effect on 10th February 1999 and they spell out the licensing criteria for certification authorities as well as the duties and reporting requirements to be observed by them in the conduct of their business. Failure to observe the provisions in the Regulations is a criminal offence. Made pursuant to section 42(3), paragraph 36 of the Electronic Transactions (Certification Authority) Regulations 1999 states that a breach of the provisions in the Regulations is an offence that is punishable with a fine not exceeding $5000 in the case of a first time offender, to a fine not exceeding $10,000 in the case of a second or subsequent conviction. In the case where no penalty is prescribed, section 56 applies (see below).

Recognition of foreign certification authorities

43. The Minister may by regulations provide that the Controller may recognise certification authorities outside Singapore that satisfy the prescribed requirements for any of the following purposes:

(a) the recommended reliance limit, if any, specified in a certificate issued by the certification authority;

(b) the presumption referred to in sections 20(*b*)(ii) and 21.

Commentary

To ensure that the local PKI is able to interface with PKI set up overseas, so that subscribers to the local PKI can rely on and act upon digital signatures and certificates issued by foreign certification authorities for foreign subscribers, this section empowers the Minister to make regulations to allow the Controller to recognise certification authorities outside Singapore, as long as they satisfy the prescribed requirements. No blanket recognition is given to all foreign certification authorities because there may be variations and differences in the laws and standards observed by the foreign certification authorities in their respective countries.

Recommended reliance limit

44. —(1) A licensed certification authority shall, in issuing a certificate to a subscriber, specify a recommended reliance limit in the certificate.

(2) The licensed certification authority may specify different limits in different certificates as it considers fit.

Commentary

One of the main differences between a licensed and an unlicensed certification authority is that a licensed certification authority is legally required to specify a recommended reliance limit in the issued certificate. However, certificates may be used for different purposes by the subscribers. These various classes of uses of certificates will depend on the level of assurance and security required. High value and high security transactions call for very secure environments with guarantees of the identities and creditworthiness of the transacting parties. This section allows the certification authority to offer different services by issuing different classes of certificates, differentiated by the levels of assurance and security they provide. The certificates may be differentiated by their different reliance limits. Of course, they will also be differentiated by their prices.

Liability limits for licensed certification authorities

45. Unless a licensed certification authority waives the application of this section, a licensed certification authority —

(a) shall not be liable 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 licensed certification authority complied with the requirements of this Act;

(b) shall not be liable 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 licensed certification authority is required to confirm; or

(ii) failure to comply with sections 29 and 30 in issuing the certificate.

Commentary

Other differences between a licensed and an unlicensed certification authority are that (i) a licensed certification authority is exempted from any loss caused by reliance on a false or forged digital signature of a subscriber where the certification authority complies with the requirements of the Act, and (ii) a licensed certification authority can limit its liability through the use of certificates that specify a recommended reliance limit. The potential liability of the certification authority arising out of any losses caused by reliance on a misrepresentation in the certificate, or breaches by the certification authority in issuing or making representations upon the issuance of the certificate, is capped at the recommended reliance limit.

Regulation of repositories

46. The Minister may make regulations for the purpose of ensuring the quality of repositories and the services they provide including provisions for the standards, licensing or accreditation of repositories.

Commentary

As explained above, repositories store the certificates issued by the certification authorities and make them available for users of the PKI. Repositories are also required to store and make available the suspension and revocation notices issued by the certification authorities. This section empowers the Minister to make regulations for the purpose of ensuring the quality of repositories and the services they provide. Currently, the Act and the regulations do not require repositories to be licensed.

PART XI
GOVERNMENT USE OF ELECTRONIC RECORDS AND SIGNATURES

Acceptance of electronic filing and issue of documents

47. —(1) Any department or ministry of the Government, organ of State or statutory corporation that, pursuant to any written law —

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

(b) issues any permit, licence or approval; or

(c) provides for the method and manner of payment,

may, notwithstanding anything to the contrary in such written law —

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

(ii) issue such permit, licence or approval in the form of electronic records; or

(iii) make such payment in electronic form.

(2) In any case where a department or ministry of the Government, organ of State or statutory corporation decides to perform any of the functions in subsection (1)(i), (ii) or (iii), such agency may specify —

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

(b) where such electronic records have to be signed, the type of electronic signature required (including, if applicable, a requirement that the sender use a digital signature or other secure electronic signature);

(c) 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;

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

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

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

Commentary

This section of the Act empowers any Government department or ministry, organ of State (such as the judiciary and parliament) or statutory corporation to accept the electronic filing, creation and retention of documents, to issue permits, licences or approvals electronically, and to provide for electronic payment. For instance, the Singapore judiciary's plans to use electronic filing for court documents can be brought within this section. This section, however, does not make it obligatory for these Government departments, State organs and statutory corporations to embark on the use of electronic transactions. But should they choose to do so, they may specify, presumably by way of regulations and directives, the manner and format of these electronic records, and prescribe the standards, processes and procedures to be observed.

PART XII
GENERAL

Obligation of confidentiality

48. —(1) Except for the purposes of this Act or for any prosecution for an offence under any written law or pursuant to an order of court, no person who has, pursuant to any powers conferred under this Part, obtained access to any electronic record, book, register, correspondence, information, document or other material shall disclose such electronic record, book, register, correspondence, information, document or other material to any other person.

(2) Any person who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both.

Commentary

Where the Controller or any authorised person has been granted access, pursuant to the provisions of this Part of the Act, to any electronic records and information, this person is placed under an obligation of confidentiality and shall not disclose such record or information to any other person, unless such a disclosure is for the purposes of the Act, for prosecution of an offence, or made pursuant to a court order. The contravention of this obligation of confidentiality renders the Controller or authorised person criminally liable.

Offence by body corporate

49. Where an offence under this Act or any regulations made thereunder is committed by a body corporate, and it is proved to have been committed with the consent or connivance of, or to be attributable to any act or default on the part of, any director, manager, secretary or other similar

officer of the body corporate, or any person who was purporting to act in any such capacity, he, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

Commentary

This section resolves the problem as to offences committed by bodies corporate. It is usually difficult to render an employee of a body corporate liable for the actions of the corporation, because this employee has to be shown to be the "controlling mind and will" of the body corporate. Section 49 modifies this common law rule. Where a body corporate commits a criminal offence, this section renders the officer of the company or any person who acts in any capacity who has given his consent, who has connived to commit this offence, or who does any act or commits a default for which the offence is attributable, such a person, as well as the body corporate itself, guilty of the offence.

Authorised officer

50. —(1) The Controller may in writing authorise any officer or employee to exercise any of the powers of the Controller under this Part.

(2) The Controller and any such officer shall be deemed to be a public servant for the purposes of the Penal Code (Cap. 224).

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

Commentary

The Controller, in enforcing the Act and the Regulations, may in writing authorise any officer or employee to exercise the powers of the Controller as set out in this Part of the Act. Such an authorised officer shall produce proof of his authority if so demanded.

Controller may give directions for compliance

51. —(1) The Controller may by notice in writing direct 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 they are necessary to ensure compliance with the provisions of this Act or any regulations made thereunder.

(2) Any person who fails to comply with any direction specified in a notice issued under subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 12 months or to both.

Commentary

Section 51 grants the Controller the power to direct a certification authority or its officer or employee to take steps to ensure compliance with the Act and its regulations. A failure to comply with the Controller's direction as specified in the issued notice constitutes a criminal offence.

This section gives the Controller the power to supervise and regulate the activities of certification authorities and their officers and employees to ensure that the provisions of the Act and its regulations are observed.

Power to investigate

52. —(1) The Controller or an authorised officer may investigate the activities of a certification authority in relation to its compliance with this Act and any regulations made thereunder.

(2) For the purposes of subsection (1), the Controller may in writing issue an order to a certification authority to further its investigation or to secure compliance with this Act or any regulations made thereunder.

Commentary

In addition, the Controller is empowered to investigate the activities of a certification authority in relation to its compliance with the Act and its regulations.

Access to computers and data

53. —(1) The Controller or an authorised officer shall —

(a) be entitled at any time to —

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

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

(b) be entitled to require —

(i) the person by whom or on whose behalf the Controller or authorised 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 paragraph (*a*).

(2) Any person who obstructs the lawful exercise of the powers under subsection (1)(*a*) or who fails to comply with a request under subsection (1)(*b*) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 12 months or to both.

Commentary

To supplement its investigative powers, this section empowers the Controller and its authorised officer to access and use any computer system which it has reasonable cause to suspect has been used in connection with an offence committed under this Act. The Controller and its authorised officer are also entitled to require the person who is suspected of committing the offence, or any

person who is in charge of the computer to provide them with such reasonable technical or other assistance. The obstruction of the lawful exercise of the Controller's access powers, and the failure to comply with a request for assistance, constitute criminal offences.

Obstruction of authorised officer

54. Any person who obstructs, impedes, assaults or interferes with the Controller or any authorised officer in the performance of his functions under this Act shall be guilty of an offence.

Commentary

As explained above, the investigative powers of the Controller are supplemented with this section, which renders any person who obstructs, impedes, assaults or interferes with the Controller of authorised officer in the performance of his functions guilty of a criminal offence. Since no punishment is prescribed, section 56 applies.

Production of documents, data, etc

55. The Controller or an authorised officer shall, for the purposes of the execution of this Act, have power to do all or any of the following:

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

(b) require the production of any identification document from any person in relation to any offence under this Act or any regulations made thereunder;

(c) make such inquiry as may be necessary to ascertain whether the provisions of this Act or any regulations made thereunder have been complied with.

Commentary

The investigative powers of the Controller are further supplemented with this section, which empowers the Controller and his authorised officer to require the production of records and documents kept by a licensed certification authority and to inspect, examine and copy any of them.

This section also empowers the Controller to require the production of any identification document from any person. Presumably this can be used to ascertain the true identity of the subscriber to a certificate. It can also be used to ascertain the identity of the offender such as the employee of the certification authority.

Finally, the section also grants the Controller the power to "make such inquiries as may be necessary to ascertain whether the provisions of this Act or any regulations made thereunder have been complied with." This is the catch-all clause to allow inquiries, which may be a precursor to investigations, to be made.

General penalties

56. Any person guilty of an offence under this Act or any regulations made thereunder for which no penalty is expressly provided shall be liable on conviction to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 6 months or to both.

Commentary

Where the Act or its regulations provide that a breach of a provision constitutes a criminal offence, but fails to specify the penalty, section 56 sets out the default penalty, which is a fine not exceeding $20,000 and imprisonment not exceeding 6 months or both.

Sanction of Public Prosecutor

57. No prosecution in respect of any offence under this Act or any regulations made thereunder shall be instituted except by or with the sanction of the Public Prosecutor.

Commentary

The sanction of the Public Prosecutor is required for an offence under the Act or its regulations to be instituted.

Jurisdiction of Courts

58. A District Court or a Magistrate's Court shall have jurisdiction to hear and determine all offences under this Act and any regulations made thereunder and, notwithstanding anything to the contrary in the Criminal Procedure Code (Cap. 68), shall have power to impose the full penalty or punishment in respect of any offence under this Act or any regulations made thereunder.

Commentary

All offences under the Act and its regulations can be heard by a District Court or a Magistrate's Court, and such a court shall have the power to impose the full penalty or punishment.

Composition of offences

59. —(1) The Controller may, in his discretion, compound any offence under this Act or any regulations made thereunder which is prescribed as being an offence which may be compounded by collecting from the person reasonably suspected of having committed the offence a sum not exceeding $5,000.

(2) The Minister may make regulations prescribing the offences which may be compounded.

Commentary

Not all offences committed under the Act and its regulations need to go to trial: the Controller has the discretion to compound any such offence, which is by Ministerial regulations prescribed as an offence which may be compounded, by collecting a composition fine of up to $5,000 from the suspected offender.

Power to exempt

60. The Minister may exempt, subject to such terms and conditions as he thinks fit, any person or class of persons from all or any of the provisions of this Act or any regulations made thereunder.

Commentary

This section empowers the Minister to exempt any person or class of persons from any of the provisions of the Act and its regulations.

Regulations

61. The Minister may make regulations to prescribe anything which is required to be prescribed under this Act and generally for the carrying out of the provisions of this Act.

Commentary

This catch-all provision supplements, among others, sections 42 and 46, by empowering the Minister to make regulations to "prescribe anything which is required to be prescribed under the Act".

Savings and transitional

62. —(1) Where a certification authority has been carrying on or operating as a certification authority before the appointed day and it has obtained a licence in accordance with the regulations made under section 42 within 6 months after the appointed day, all certificates issued by such certification authority before the appointed day, to the extent that they satisfy the requirements under this Act or any regulations made thereunder, shall be deemed to have been issued under this Act by a licensed certification authority and shall have effect accordingly.

(2) In this section, "appointed day" means the date of commencement of this Act.

Commentary

This is a savings and transitional provision, which retrospectively validates all certificates issued by a certification authority that has been in operation before the date of commencement of the Act, if it has obtained a licence in accordance with the regulations within 6 months after this date. Since the Act was brought into force on 10th July 1998, and more than 6 months have lapsed, this section is now obsolete.

Related amendments to Interpretation Act

63. The Interpretation Act (Cap 1) is amended —

(a) by inserting, immediately after the words "*Gazette* published", in the definition of ""*Gazette*" or Government *Gazette*"" in section 2(1), the words "in electronic or other form";

(b) by inserting immediately after subsection (4) of section 2, the following subsection :

"(5) Where a *Gazette* is published in more than one form, the date of publication of that *Gazette* shall be deemed to be the date that *Gazette* is first published in any form."

(c) by deleting the word "and" at the end of sub-paragraph (ii) of paragraph (*a*) of section 20; and

(d) by inserting the word "and" at the end of sub-paragraph (iii) of paragraph (*a*) of section 20, and by inserting immediately thereafter the following sub-paragraph :

"(iv) authority to provide for the manner and method in which any document, record, application, permit, approval or licence may be submitted, issued or served by electronic means, or for the authentication thereof;"

Commentary

This section achieves two things by its related amendments to the Interpretation Act. First, it makes possible the publication of the Government Gazette in electronic form, and it renders the date of publication of the Gazette as the date that the Gazette is first published, either in its traditional form or in electronic form. Secondly, it extends the power to make subsidiary legislation by granting the Government department, ministry or statutory corporation responsible for the making of the subsidiary legislation the power to provide for electronic submissions, applications, approvals or licences, and for their authentication. This part of the section appears to supplement section 47 of the Act.

Related amendment to Evidence Act

64. The Evidence Act (Cap. 97) is amended by renumbering section 69 as subsection (1) of that section, and by inserting immediately thereafter the following subsection :

"(2) This section shall not apply to any electronic record or electronic signature to which the Electronic Transactions Act 1998 applies.".

Commentary

This section makes a related amendment to the Evidence Act by providing that section 69, which deals with proof of signatures and handwriting, has no application where the electronic record or electronic signature is one to which the Electronic Transactions Act applies. Concepts such as proof of a person's handwriting have no application to electronic records and electronic signatures. According to section 18 (see above), where the record is an electronic record, and it is a secure electronic record, it shall be presumed not to have been altered from the time it is made secure. And where the electronic signature is a secure electronic signature, it shall be presumed to be the signature of the person to whom it correlates.