formats or methods. The UK Act aims to be technology-neutral and covers all types of electronic signature, from those based on e-mail exchanges to those using public key cryptography or biometric techniques. The Ordinance is similar to the Singaporean Electronic Transactions Act 1998, which likewise defines digital signatures by reference to the public key-private key signature based on PKI and thereby limits its general application.

In March 2002, the Information Technology and Broadcasting Bureau issued a "Consultation Paper on the Review of the Electronic Transactions Ordinance". The Ordinance was then amended by the Electronic Transactions (Amendment) Ordinance which became effective on 30 June 2004. The main amendments are to:

- revise the definitions in s.2;
- allow for the service of documents to a designated information system (s.5A);
- alter s.6 concerning the use of electronic and digital signatures to accept all types of electronic signatures except in the case of transactions with the Government, where only a technology-specific digital signature is accepted;
- alter certain provisions regarding the consent required from the intended recipient for the service of documents by electronic means; and
- confirm the legal effect of an electronically formed contract under s.17.

Long title

An Ordinance to facilitate the use of electronic transactions for commercial and other purposes, to provide for matters arising from and related to such use, to enable the Postmaster General to provide the services of a certification authority and to provide for connected purposes.

[Part I, ss.4 and 9, Part V (other than in relation to the matters referred to in Sch.1) and Part VI, ss.31 and 33 and Parts IX, X, XI and XII	7 January 2000	
Part VII and s.32	18 February 2000	*L.N. 7 of 2000*
Sections 3, 5, 6, 7, 8 and 10, Part IV, Part V (in relation to the matters referred to in Sch.1) and Schs.1 and 2	7 April 2000	*L.N. 60 of 2000*]

(Originally 1 of 2000)

Section: 1 **Short title** **1 of 2000** **07/01/2000**

PART I

PRELIMINARY

(1) This Ordinance may be cited as the Electronic Transactions Ordinance.
(2)–(3) (Omitted as spent)

Commencement

Part I, ss.4 and 9, Part V (other than in relation to the matters referred to in Sch.1) and Part VI, ss.31 and 33 and Parts IX, X, XI and XII of the Ordinance came into operation on 7 January 2000. **[1.01]**

Part VII and s.32 of the Ordinance came into operation on 18 February 2000.

Sections 3, 5, 6, 7, 8 and 10; Part IV; Part V (in relation to the matters referred to in Sch.1) and Schs.1 and 2 came into operation on 7 April 2000.

Comparative Legislation

The provisions of the Ordinance on electronic records and digital signatures reflect many of the provisions of the United Nations Commission on International Trade Law (UNCITRAL)–Model Law on Electronic Commerce (the "Model Law"). The following provisions and suitable safeguards for these provisions to apply are included: **[1.02]**

(1) where a rule of law requires or permits information to be given or presented in writing, the use of electronic records will satisfy the rule of law;
(2) where a rule of law requires information to be retained, or to be presented or retained in the original form, that requirement is met by retaining or presenting the information in the form of electronic records;
(3) where a rule of law requires a signature of a person, that requirement is met by a digital signature;
(4) contracts shall not be denied legal effect solely on the ground that electronic records are used in their formation; and
(5) electronic records shall not be denied admissibility as evidence in court on the sole ground that they are electronic records.

The Ordinance is also influenced by Singapore's Electronic Transactions Act 1998.

Section: 2 **Interpretation** **L.N. 130 of 2007** **01/07/2007**

Remarks:
For the saving and transitional provisions relating to the amendments made by the Resolution of the Legislative Council (L.N. 130 of 2007), see para (12) of that Resolution.

(1) In this Ordinance, unless the context otherwise requires:

accept (接受), in relation to a certificate:

(a) in the case of a person named or identified in the certificate as the person to whom the certificate is issued, means to:

(i) confirm the accuracy of the information on the person as contained in the certificate;

(ii) authorise the publication of the certificate to any other person or in a repository;

(iii) use the certificate; or

(iv) otherwise demonstrate the approval of the certificate; or

(b) in the case of a person to be named or identified in the certificate as the person to whom the certificate is issued, means to:

(i) confirm the accuracy of the information on the person that is to be contained in the certificate;

(ii) authorise the publication of the certificate to any other person or in a repository; or

(iii) otherwise demonstrate the approval of the certificate; (Added 14 of 2004 s.2)

addressee (收訊者), in relation to an electronic record sent by an originator, means the person who is specified by the originator to receive the electronic record but does not include an intermediary;

asymmetric cryptosystem (非對稱密碼系統) means a system capable of generating a secure key pair, consisting of a private key for generating a digital signature and a public key to verify the digital signature;

certificate (證書) means a record which:

(a) is issued by a certification authority for the purpose of supporting a digital signature which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair;

(b) identifies the certification authority issuing it;

(c) names or identifies the person to whom it is issued;

(d) contains the public key of the person to whom it is issued; and

(e) is signed by the certification authority issuing it; (Amended 14 of 2004 s.2)

certification authority (核證機關) means a person who issues a certificate to a person (who may be another certification authority);

certification authority disclosure record (核證機關披露紀錄), in relation to a recognised certification authority, means the record maintained under s.31 for that certification authority;

certification practice statement (核證作業準則) means a statement issued by a certification authority to specify the practices and standards that the certification authority employs in issuing certificates;

code of practice (業務守則) means the code of practice published under s.33; (Amended 14 of 2004 s.2)

consent (同意), in relation to a person, includes consent that can be reasonably inferred from the conduct of the person; (Added 14 of 2004 s.2)

correspond (對應), in relation to private or public keys, means to belong to the same key pair;

digital signature (數碼簽署), in relation to an electronic record, means an electronic signature of the signer generated by the transformation of the 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 determine:

(a) whether the transformation was generated 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 generated;

electronic record (電子紀錄) means a record generated in digital form by an information system, which can be:

(a) transmitted within an information system or from one information system to another; and

(b) stored in an information system or other medium;

electronic signature (電子簽署) means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted for the purpose of authenticating or approving the electronic record;

government entity (政府單位) means a public officer or a public body; (Added 14 of 2004 s.2)

hash function (雜湊函數) means an algorithm mapping or transforming one sequence of bits into another, generally smaller, set as 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 not feasible for a record to be derived or reconstituted from the hash result produced by the algorithm; and

(c) it is computationally not feasible that two records can be found to produce the same hash result using the algorithm;

information (資訊) includes data, text, images, sound codes, computer programmes, software and databases;

information system (資訊系統) means a system which:

(a) processes information;

(b) records information;

(c) can be used to cause information to be recorded, stored or otherwise processed in other information systems (wherever situated); and

(d) can be used to retrieve information, whether the information is recorded or stored in the system itself or in other information systems (wherever situated);

intermediary (中介人), in relation to a particular electronic record, means a person who on behalf of a person, sends, receives or stores that electronic record or provides other incidental services with respect to that electronic record;

issue (發出), in relation to a certificate, means to:

(a) create the certificate, and then notify the person named or identified in the certificate as the person to

(i) whom the certificate is issued of the information on the person as contained in the certificate; or

(b) notify the person to be named or identified in the certificate as the person to whom the certificate is issued of the information on the person that is to be contained in the certificate, and then create the certificate, and then make the certificate available for use by the person; (Replaced 14 of 2004 s.2)

key pair (配對密碼匙), in an asymmetric cryptosystem, means a private key and its mathematically related public key, where the public key can verify a digital signature that the private key generates;

originator (發訊者), in relation to an electronic record, means a person, by whom, or on whose behalf, the electronic record is sent or generated but does not include an intermediary;

Permanent Secretary (常任秘書長) means the Permanent Secretary for Commerce and Economic Development (Communications and Technology); (Added 14 of 2004 s.2. Amended L.N. 130 of 2007)

Postmaster General (郵政署署長) means the Postmaster General within the meaning of the Post Office Ordinance (Cap.98);

private key (私人密碼匙) means the key of a key pair used to generate a digital signature;

public key (公開密碼匙) means the key of a key pair used to verify a digital signature;

recognised certificate (認可證書) means:

(a) a certificate recognised under s.22;

(b) a certificate of a type, class or description of certificate recognised under s.22; or

(c) a certificate designated as a recognised certificate issued by the certification authority referred to in s.34;

recognised certification authority (認可核證機關) means a certification authority recognised under s.21 or the certification authority referred to in s.34;

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

reliance limit (倚據限額) means the monetary limit specified for reliance on a recognised certificate;

repository (儲存庫) means an information system for storing and retrieving certificates and other information relevant to certificates;

responsible officer (負責人員), in relation to a certification authority, means a person occupying a position of responsibility in relation to the activities of the certification authority relevant to this Ordinance;

rule of law (法律規則) means:

(a) an Ordinance;

(b) a rule of common law or a rule of equity; or

(c) customary law;

Secretary (局長) means the Secretary for Commerce and Economic Development; (Amended L.N. 106 of 2002; L.N. 130 of 2007)

sign and signature (簽、簽署) include any symbol executed or adopted, or any methodology or procedure employed or adopted, by a person with the intention of authenticating or approving a record;

subscriber (登記人) means a person (who may be a certification authority) who:

(a) is named or identified in a certificate as the person to whom the certificate is issued;

(b) has accepted that certificate; and

(c) holds a private key which corresponds to a public key listed in that certificate;

trustworthy system (穩當系統) means computer hardware, software and procedures that:

(a) are reasonably secure from intrusion and misuse;

(b) are at a reasonable level in respect of availability, reliability and ensuring a correct mode of operations for a reasonable period of time;

(c) are reasonably suitable for performing their intended function; and

(d) adhere to generally accepted security principles;

verify a digital signature (核實數碼簽署), in relation to a given digital signature, electronic record and public key, means to determine that:

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

(b) the electronic record has not been altered since its digital signature was generated, and any reference to a digital signature being verifiable is to be construed accordingly.

(2) For the purposes of this Ordinance, a digital signature is taken to be supported by a certificate if the digital signature is verifiable with reference to the public key listed in a certificate the subscriber of which is the signer. (Amended 14 of 2004 s.2; L.N. 131 of 2004)

Enactment History

The following definitions contained in s.2(1) have been amended by virtue of the Electronic Transactions (Amendment) Ordinance (effective 30 June 2004): **[2.01]**

(1) "accept a certificate" was replaced with '"accept" in relation to a certificate. This expanded definition has the effect that a person who has used a certificate is deemed to have accepted the certificate.

(2) "issue" was repealed and substituted by a more detailed definition.

(3) "consent", "government entity" and "Permanent Secretary" were added.

As the position of Secretary for Commerce, Industry and Technology was abolished in 2007 when the Commerce, Industry and Technology Bureau was abolished and its responsibilities merged into that of the Commerce and Economic Development Bureau. Therefore the definitions of "Secretary" and "Permanent Secretary" were amended by substituting "Secretary for Commerce and Economic Development" and "Permanent Secretary for Commerce and Economic Development (Communications and Technology)" respectively, pursuant to L.N. 130 of 2007.

Addressee, originator and intermediary

[2.02] Following art.2 of the Model Law, the definitions of "addressee" and "originator" exclude "intermediary". This is necessary in order to establish a distinction between a person sending electronic data (originator), someone receiving the data (addressee) and a third party in the middle sending and receiving the data on behalf of the other two (intermediary). An example of an intermediary is an internet service provider. Note that the originator and the addressee of an electronic data could be the same person, for example in the case where the data was intended for storage by its author.

Section: 3 Matters to which ss.5, 5A, 6, 7, 8 and 17 are not applicable 14 of 2004 30/06/2004

PART II

APPLICATION

Sections 5, 5A, 6, 7, 8 and 17 do not apply to any (Amended 14 of 2004 s.3):

(a) requirement or permission for information to be or given in writing;

(aa) requirement or permission for a document to be served by personal service or by post; (Added 14 of 2004 s.3)

(b) requirement for the signature of a person;

(c) requirement for information to be presented or retained in its original form;

(d) requirement for information to be retained,

under a rule of law in a matter or for an act set out in Sch.1, unless that rule of law expressly provides otherwise.

Enactment History

[3.01] This section was amended by inserting "5A" after "sections 5" and para (aa) after para (a) pursuant to s.3 of the Electronic Transactions (Amendment) Ordinance, which came into operation on 30 June 2004.

Explanatory Note

[3.02] This section excludes the use of electronic signatures for all documents where a signature is required by law and to those documents specified in Sch.1 of the Ordinance (see ss.5, 5A, 6, 7, 8 and 17 of the Ordinance).

Section: 4 Ordinance to bind Government 1 of 2000 07/01/2000

This Ordinance binds the Government.

Explanatory Note

[4.01] In the Legislative Council Brief on the Bill, it is stated that the proposed Bill applies to a rule of law irrespective of whether the rule of law is applicable to an individual, public body, public authority, private body, organ or any other person or to a transaction executed by means of electronic records to which any such person is a party.

Section: 5 Requirement for writing L.N. 60 of 2000 07/04/2000

PART III

ELECTRONIC RECORDS AND DIGITAL SIGNATURES

(1) If a rule of law requires information to be or given in writing or provides for certain consequences if it is not, an electronic record satisfies the requirement if the information contained in the electronic record is accessible so as to be usable for subsequent reference.

(2) If a rule of law permits information to be or given in writing, an electronic record satisfies that rule of law if the information contained in the electronic record is accessible so as to be usable for subsequent reference.

Explanatory Note

[5.01] This section follows art.6 of the Model Law and s.7 of the Singapore Electronic Transactions Act 1998.

The Ordinance does not define "in writing". Pursuant to s.3 of the Interpretation and General Clauses Ordinance (Cap.1), "writing" and "printing" include writing, printing, lithography, photography, typewriting and any other mode of representing words in a visible form.

Exclusion

[5.02] This section does not apply to documents where a signature is required by law and to those documents specified in Sch.1 of the Ordinance (see s.3 of the Ordinance).

Section: 5A Service of documents 14 of 2004 30/06/2004

(1) Without limiting the generality of s.5, if a rule of law under a provision set out in Sch.3 requires a document to be served on a person by personal service or by post (whether or not there is any further specification as to the address or place at which such service is to be effected), the provision shall be construed as also providing that service of the document in the form of an electronic record to an information system designated by the person satisfies the requirement under the provision if the information contained in the electronic record is accessible so as to be usable for subsequent reference.

(2) Without limiting the generality of s.5, if a rule of law under a provision set out in Sch.3 permits a document to be served on a person by personal service

or by post (whether or not there is any further specification as to the address or place at which such service is to be effected), the provision shall be construed as also providing that service of the document in the form of an electronic record to an information system designated by the person is permitted under the provision if the information contained in the electronic record is accessible so as to be usable for subsequent reference.

(Added 14 of 2004 s.4)

Enactment History

[5A.01] This section was added as a result of the Electronic Transactions (Amendment) Ordinance and took effect from 30 June 2004.

Explanatory Note

[5A.02] This section provides that the service of a document in the form of an electronic record has the same effect as service by post or in person for the purposes of the provisions set out in Sch.3, which are:

(1) Landlord and Tenant (Consolidation) Ordinance (Cap.7) s.119Y(1)(a) and (b);
(2) Rating Ordinance (Cap.116) s.50(1);
(3) Government Rent (Assessment and Collection) Ordinance (Cap.515) s.45(1);
(4) Mass Transit Railway (Land Resumption and Related Provisions) Ordinance (Cap.276) (Added L.N. 151 of 2006) s.21(1);
(5) Roads (Works, Use and Compensation) Ordinance (Cap.370) (Added L.N. 151 of 2006) ss.10(1) and (3) and 29(1);
(6) Railways Ordinance (Cap.519) (Added L.N. 151 of 2006) ss.10(1) and (4), 27(6) and (7) and 34(1);
(7) Electricity Ordinance (Cap.406) (Added L.N. 214 of 2007) s.52;
(8) Inland Revenue Ordinance (Cap.112) (Added L.N. 214 of 2007) s.58(2);
(9) Waterworks Regulations (Cap.102 sub. leg. A) (Added L.N. 249 of 2008) regulation 49(1)(a) and (b); and
(10) Census and Statistics Ordinance (Cap.316) (Added L.N. 83 of 2009) s.12(3)(a) and (b).

(Sch.3 added 14 of 2004 s.28)

The service of the document must be to an information system designated by the intended recipient. Where neither party is a government entity, s.5A will apply only if the person on whom the information or document is to be served consents to it being served in the form of an electronic record.

The definition of "information system" covers systems which process, record and store information. The Guide to Enactment of the Model Law suggests that an "information system" could indicate a range of technical means from a communications network to an electronic mailbox or even a telecopier. The Model

Law does not address the question of whether the information system is located on the premises of the addressee or on other premises, since the location of information systems is not under the Model Law.

Exclusion

This section does not apply to documents where a signature is required by law and to those documents specified in Sch.1 of the Ordinance (see s.3 of the Ordinance). [5A.03]

Section: 6 Electronic signatures, digital signatures, etc. **L.N. 131 of 2004** **01/07/2004**

(1) Where:
(a) a rule of law requires the signature of a person (the first mentioned person) on a document or provides for certain consequences if the document is not signed by the first mentioned person; and
(b) neither the first mentioned person nor the person to whom the signature is to be given (the second mentioned person) is or is acting on behalf of a government entity,

an electronic signature of the first mentioned person satisfies the requirement if:
(c) the first mentioned person uses a method to attach the electronic signature to or logically associate the electronic signature with an electronic record for the purpose of identifying himself and indicating his authentication or approval of the information contained in the document in the form of the electronic record;
(d) having regard to all the relevant circumstances, the method used is reliable, and is appropriate, for the purpose for which the information contained in the document is communicated; and
(e) the second mentioned person consents to the use of the method by the first mentioned person. (Replaced 14 of 2004 s.5)

(1A) Where:
(a) a rule of law requires the signature of a person on a document or provides for certain consequences if the document is not signed by the person; and
(b) either or both of the person mentioned in para (a) and the person to whom the signature is to be given is or are or is or are acting on behalf of a government entity or government entities,

a digital signature of the person mentioned in para (a) satisfies the requirement if the digital signature is:
(i) supported by a recognised certificate;
(ii) generated within the validity of that certificate; and
(iii) used in accordance with the terms of that certificate. (Added 14 of 2004 s.5)

Section: 18 Attribution of electronic record 1 of 2000 07/01/2000

PART VI

ATTRIBUTION OF SENDING AND RECEIVING ELECTRONIC RECORDS

(1) Unless otherwise agreed between the originator and the addressee of an electronic record, an electronic record is that of the originator if it was:

(a) sent by the originator;

(b) sent with the authority of the originator; or

(c) sent by an information system programmed by or on behalf of the originator to operate and to send the electronic record automatically.

(2) Nothing in subs.(1) is to affect the law of agency or the law on the formation of contracts.

Explanatory Note

[18.01] This section specifies that, unless otherwise agreed, the electronic record is considered that of the originator if it was sent by the originator or with his or her authority or by an information system programmed by or on behalf of the originator to send the electronic record automatically. The definitions of "originator", "addressee" and "electronic record" are defined in s.2 of the Ordinance.

[18.02] The relationship between the originator and the authorised person or an information system is still governed by the law of agency and this section does not affect the rule of common law on the formation of contracts between parties. For instance, when a user clicks on a website hyperlink, he sends a message through the Internet to the web server hosting the relevant page; this triggers the sending of the electronic data constituting the desired website back to the user's personal computer. Although the browser electronically solicits the sending of the page, the web server responds to the request and performs the task of sending. Under s.18(1)(c) of the Ordinance, the response of the web server is deemed to be that of the operator of the website, and the electronic record is deemed to have been sent from the operator's place of business and received at the address the browser's place of business or residence.

Section: 19 Sending and receiving electronic records 1 of 2000 07/01/2000

(1) Unless otherwise agreed between the originator and the addressee of an electronic record, an electronic record is sent when it is accepted by an information system outside the control of the originator or of the person who sent the electronic record on behalf of the originator.

(2) Unless otherwise agreed between the originator and the addressee of an electronic record, 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 is accepted by 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 comes to the knowledge of the addressee;

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

(3) Subsections (1) and (2) apply notwithstanding that the place where the information system is located is different from the place where the electronic record is taken to have been sent or received under subs.(4).

(4) Unless otherwise agreed between the originator and the addressee, an electronic record is taken to have been:

(a) sent at the place of business of the originator; and

(b) received at the place of business of the addressee.

(5) For the purposes of subs.(4):

(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 of the originator or the addressee, as the case may be;

(b) if the originator or the addressee does not have a place of business, the place of business is the place where the originator or the addressee ordinarily resides.

(6) Where the originator and the addressee are in different time zones, time refers to Universal Standard Time.

Explanatory Note

Section 19 adopts art.15 of the Model Law and sets out circumstances which constitute sending and receiving an electronic record and when and where it is regarded as sent or received. The location of the information system itself is not relevant to this section. [19.01]

Subsection (2)

Unless otherwise agreed between the parties, an electronic record is considered received: [19.02]

(i) At the time when the electronic record is accepted by the addressee's information system designated for the purpose of receiving electronic records.

(ii) At the time when the electronic record comes to the knowledge of the addressee if:

(a) the addressee does not have a designated information system for the purpose of receiving electronic records, or

(b) the electronic record is sent to an information system of the addressee that is not the designated information system.

"Comes to the knowledge of the addressee" in s.19(2)(a) of the Ordinance is intended to be construed as the point when the addressee becomes aware that information intended for him is available on the system. However, there is no further clarification on whether the addressee comes to the knowledge of the electronic records when the message is received by his server or when he reads the message.

Subsections (4) and (5)

[19.03] The place of sending and receiving an electronic record is primarily the place of business of the originator and the addressee respectively. In situations where there is more than one place of business, it will be the place with the closest connection to the underlying transaction; if there is no underlying transaction, it will be the principal place of business of the originator or the addressee. In the absence of a place of business, the place of sending and receiving will be the place where the originator or the addressee ordinarily resides.

Section: 20 — Certification authority may apply to Government Chief Information Officer for recognition — L.N. 131 of 2004 — 01/07/2004

PART VII

RECOGNITION OF CERTIFICATION AUTHORITIES AND CERTIFICATES BY GOVERNMENT CHIEF INFORMATION OFFICER

(Amended L.N. 131 of 2004)

(1) A certification authority may apply to the Government Chief Information Officer to become a recognised certification authority for the purposes of this Ordinance.

(2) Subject to subs.(4) and s.21(3), an application under subs.(1) must be made in the prescribed manner and in a form specified by the Government Chief Information Officer and the applicant must pay the prescribed fee in respect of the application.

(3) An applicant must furnish to the Government Chief Information Officer (Amended L.N. 131 of 2004):

(a) the relevant particulars and documents specified under s.30; (Amended 14 of 2004 s.12)

(b) a report which:

(i) contains an assessment as to whether the applicant is capable of complying with such provisions of this Ordinance and of

the code of practice as are specified in the code of practice for the purposes of this subparagraph; and

(ii) is made by a person approved by the Government Chief Information Officer as being qualified to make such a report; and (Replaced 14 of 2004 s.12)

(c) a statutory declaration which:

(i) states whether the applicant is capable of complying with such provisions of this Ordinance and of the code of practice as are specified in the code of practice for the purposes of this subparagraph; and

(ii) is made by a responsible officer of the applicant. (Added 14 of 2004 s.12)

(3A) Any report or statutory declaration required to be furnished under subs. (3) must be made at the expense of the applicant. (Added 14 of 2004 s.12)

(4) The Government Chief Information Officer may waive (Amended L.N. 131 of 2004):

(a) the requirements as to manner and form of making the application in subs.(2); or

(b) the requirement of a report or statutory declaration under subs.(3), (Amended 14 of 2004 s.12) in relation to a certification authority, in the circumstances specified in subs.(5).

(5) The Government Chief Information Officer may waive the requirements referred to in subs.(4) only if (Amended L.N. 131 of 2004):

(a) the applicant is a certification authority with a status in a place outside Hong Kong comparable to that of a recognised certification authority (comparable status); and

(b) the competent authority of that place accords to a recognised certification authority a comparable status on the basis of it being a recognised certification authority.

(Amended L.N. 131 of 2004)

Overview

[20.01] This section deals with the procedures that need to be complied with when applying to the Government Chief Information Officer (GCIO) for recognition as a certification authority. For the definition of a certification authority, see s.2 of this Ordinance.

Form and fee

[20.02] The form specified by the GCIO can be downloaded from the Office of the GCIO website.

The current application fee for an application for recognition or an application for renewal of the same is HK$15,000. For a particular certificate or a type, class or description, the fee is HK$1,500 if an application for renewal of recognition was made simultaneously, HK$3,400 otherwise. Pursuant to s.21(3), the whole or part of this fee may be waived upon the certification authority being recognised at the discretion of the GCIO.

Scope of assessment

[20.03] The objective of the assessment is to determine whether the certification authority is capable of, or has been complying with, the requirements under relevant provisions of this Ordinance and the Code of Practice for Recognised Certification Authorities published by the GCIO (the "Code of Practice") (as the case may be) and whether the certification authority has complied with the policies and business practices specified in its certification practice statement(s).

The assessor may cover the following areas in the assessment:

(1) obtain an understanding of the certification authority's policies and business practices and assess whether such information has been properly disclosed;
(2) assess the certification authority's compliance with the requirements concerning the use of a trustworthy system to support its operations;
(3) assess the certification authority's compliance with the requirements regarding the recognition of certificates in accordance with the certification authority's certification practice statement(s) and the Code of Practice; and
(4) review specific information relating to the certification authority's financial projection and ascertain and review specific information relating to cover against potential liabilities arising from the issue of certificates by the certification authority.

Assessment report

[20.04] Pursuant to s.20(3)(b), a certification authority must submit an assessment report to the GCIO when applying for recognition. According to paragraph 12.2 of the Code of Practice, the qualified person referred to in s.20(3)(b)(ii) shall be:

(1) independent of the recognised certification authority under assessment;
(2) accredited by a recognised professional organisation or association; and
(3) proficient in the following:
  (a) the assessment of public key infrastructure and related technologies;
  (b) applying information security tools and techniques;
  (c) performing financial reviews;
  (d) performing security reviews; and
  (e) performing third-party review.

Such qualified person can be an individual, a partnership or an organisation comprising individuals that collectively possess all of the above requirements.

Section: 21 Government Chief Information Officer may on application recognise certification authorities **L.N. 131 of 2004** **01/07/2004**

(1) The Government Chief Information Officer may (Amended L.N. 131 of 2004):
  (a) recognise an applicant under s.20 as a recognised certification authority if the Government Chief Information Officer is satisfied

that the applicant is suitable for such recognition; or (Amended L.N. 131 of 2004)
  (b) refuse the application for recognition.

(2) The Government Chief Information Officer must give reasons in writing to the applicant for refusing an application under subs.(1)(b). (Amended L.N. 131 of 2004)

(3) The Government Chief Information Officer may, in recognising a certification authority referred to in s.20(4), waive the whole or part of the prescribed fee as the Government Chief Information Officer may decide in relation to a particular case. (Amended L.N. 131 of 2004)

(4) In determining whether an applicant is suitable for recognition under subs.(1), the Government Chief Information Officer shall, in addition to any other matter the Government Chief Information Officer considers relevant, take into account the following (Amended L.N. 131 of 2004)
  (a) whether the applicant has the appropriate financial status for operating as a recognised certification authority in accordance with this Ordinance and the code of practice;
  (b) the arrangements put in place or proposed to be put in place by the applicant to cover any liability that may arise from its activities relevant for the purposes of this Ordinance;
  (c) the system, procedure, security arrangements and standards used or proposed to be used by the applicant to issue certificates to subscribers;
  (d) any report or statutory declaration furnished by the applicant under s.20(3); (Replaced 14 of 2004 s.13)
  (e) whether the applicant and the responsible officers are fit and proper persons; and
  (f) the reliance limits set or proposed to be set by the applicant for its certificates.

(5) In determining whether a person referred to in subs.(4)(e) is a fit and proper person, the Government Chief Information Officer shall, in addition to any other matter the Government Chief Information Officer considers relevant, have regard to the following (Amended L.N. 131 of 2004):
  (a) the fact that the person has a conviction in Hong Kong or elsewhere for an offence for which it was necessary to find that the person had acted fraudulently, corruptly or dishonestly;
  (b) the fact that the person has been convicted of an offence against this Ordinance;
  (c) if the person is an individual, the fact that the person is an undischarged bankrupt or has entered into a composition or a scheme of arrangement or a voluntary arrangement within the meaning of the Bankruptcy Ordinance (Cap.6) within the five years preceding the date of the application; and
  (d) if the person is a body corporate, the fact that the person is in liquidation, is the subject of a windingup order or there is a receiver

appointed in relation to it or it has entered into a composition or a scheme of arrangement or a voluntary arrangement within the meaning of the Bankruptcy Ordinance (Cap.6) within the five years preceding the date of the application.

(6) In recognising a certification authority under subs.(1), the Government Chief Information Officer may (Amended L.N. 131 of 2004):

(a) attach conditions to the recognition; or

(b) specify a period of validity for the recognition.

Overview

[21.01] This section sets out different aspects that the GCIO will take into account when deciding whether to recognise a certification authority.

Application Criteria

[21.02] The GCIO will consider the following in deciding whether a certification authority is to be recognised:

(1) the financial status of the certification authority for operating as a recognised certification authority in accordance with the Ordinance and the Code of Practice;

(2) the arrangements put in place or proposed to be put in place to cover the liability that may arise from its activities relevant for the purposes of the Ordinance;

(3) the system, procedure, security arrangements and standards used or proposed to be used to issue certificates to subscribers;

(4) the report prepared pursuant to s.20(3)(b);

(5) whether the applicant and the responsible officers are fit and proper persons; and

(6) the reliance limits set or proposed to be set on the certificates issued or to be issued by the certification authority.

The application form for seeking recognition of the certification authority can be obtained from the Certification Authority Recognition Office (or any other place as it specifies) and is also available on the web site of the Office of the GCIO.

When the completed application form is submitted to the GCIO, the applicant should ensure that the completed application form is supported by the assessment report, the statutory declaration, the application fee(s) and any relevant documents or information.

For more on the application fee, see paragraph [20.02].

Appeal

[21.03] In the circumstances where the GCIO refuses an application, the certification authority concerned may appeal to the Secretary for Commerce and Economic Development against the decision within seven days from the date of the decision made by the GCIO. This is dealt with in s.28 below.

Section: 22 Government Chief Information Officer may recognise certificates **L.N. 131 of 2004** **01/07/2004**

(1) The Government Chief Information Officer may recognise certificates issued by a recognised certification authority as recognised certificates, upon application by that authority.

(2) An applicant under subs.(1) must make the application in the prescribed manner and in a form specified by the Government Chief Information Officer and furnish to the Government Chief Information Officer the relevant particulars and documents specified under s.30.

(3) A recognition under subs.(1) may relate to:

(a) all certificates issued by the recognised certification authority;

(b) certificates of a type, class or description; or

(c) particular certificates.

(4) An applicant must pay the prescribed fee (if any) in respect of an application under subs.(1) unless the Government Chief Information Officer waives it in whole or in part.

(5) In recognizing certificates under this section, the Government Chief Information Officer shall in addition to any other matter the Government Chief Information Officer considers relevant take into account the following (Amended L.N. 131 of 2004):

(a) whether the certificates are issued in accordance with the certification practice statement;

(b) whether the certificates are issued in accordance with the code of practice;

(c) the reliance limit set or proposed to be set for that type, class or description or the particular certificate, as the case may require; and

(d) the arrangements put in place or proposed to be put in place by the certification authority to cover any liability that may arise from the issue of that type, class or description or the particular certificate, as the case may be.

(6) The Government Chief Information Officer may refuse an application under subs.(1).

(7) The Government Chief Information Officer must give reasons in writing to the applicant for refusing an application under subs.(6).

(8) The Government Chief Information Officer may specify a period of validity for a recognition under this section.

(9) The Government Chief Information Officer may upon application renew a recognition under this section.

(10) Subsections (2), (3), (4), (5), (6), (7) and (8) apply to a renewal under subs.(9) as they apply to an application for recognition, subject to necessary modifications. (Amended 14 of 2004 s.14) (Amended L.N. 131 of 2004)

Overview

This section sets out different aspects that the GCIO will take into account when deciding whether to recognise a certificate issued by a recognised certification authority. [22.01]

Overview

[30.01] This section provides that the GCIO may require further particulars or documents to be supplied in addition to the statutory requirements when a certification authority applies for or renews its recognition. The GCIO should publish these requirements by notice in the Gazette.

Section: 31	Government Chief Information Officer to maintain certification authority disclosure record	L.N. 131 of 2004	01/07/2004

PART VIII

CERTIFICATION AUTHORITY DISCLOSURE RECORDS AND CODE OF PRACTICE

(1) The Government Chief Information Officer must maintain for each recognised certification authority an online and publicly accessible record.

(2) The Government Chief Information Officer must publish in the certification authority disclosure record information regarding that certification authority relevant for the purposes of this Ordinance (in addition to the information required to be given in it under other provisions of this Ordinance).

(Amended L.N. 131 of 2004)

Overview

[31.01] This section stipulates that the GCIO has the responsibility to maintain a disclosure record for each recognised certification authority. The GCIO is also required to publish immediately certain information in accordance to s.32, once such information has come to its attention.

Disclosure record

[31.02] A disclosure record is a record maintained by the GCIO for a certification authority. This record allows the public to verify the validity of the recognised certificates issued by a particular certification authority up to least seven years after the concerned certification has terminated its service.

Section: 32	Government Chief Information Officer to notify revocations, suspensions and non-renewals of recognition, etc.	L.N. 131 of 2004	01/07/2004

(1) The Government Chief Information Officer must give notice in the relevant certification authority disclosure record, immediately (Amended L.N. 131 of 2004):

(a) when the Government Chief Information Officer makes a decision to revoke a recognition under s.23(4);
(b) when a revocation has taken effect under s.23(6) or (7);
(c) when the Government Chief Information Officer makes a decision to suspend a recognition under s.24(2);
(d) when a suspension has taken effect under s.24(4) or (5);
(e) when the recognition of a suspended recognition is reinstated;
(f) when the Government Chief Information Officer receives a notice of appeal under s.28(3); or
(g) on becoming aware that the Secretary has confirmed, varied or reversed the decision of the Government Chief Information Officer to revoke or suspend a recognition.

(2) Where the revocation or suspension of a recognition has taken effect, the Government Chief Information Officer must, as soon as practicable, give notice of the revocation or suspension for at least three consecutive days in one English language daily newspaper and one Chinese language daily newspaper in circulation in Hong Kong.

(3) If a recognised certification authority does not apply for renewal before the end of the period during which an application for renewal can be made under s.17(2), the Government Chief Information Officer must, at least 21 days before the expiry of the period of validity of the recognition, give notice (Amended L.N. 131 of 2004):

(a) for at least three consecutive days in one English language daily newspaper and one Chinese language daily newspaper in circulation in Hong Kong; and
(b) in the certification authority disclosure record maintained for the certification authority,

of the date of the expiry of the validity and that the certification authority has not applied for renewal.

(Amended L.N. 131 of 2004)

Overview

[32.01] This section sets out the information the GCIO is required to publish immediately once such information has come to its attention. Thus far, recognitions have been revoked because the recognised certification authorities decided to terminate the service themselves while the reason for revocation of a recognised certificate is usually unspecified.

Revocation, suspension or non-renewal of a recognition

[32.02] In the circumstances of revocation, suspension or a non-renewal of a recognition, the GCIO is further required to publish a notice in one English language daily newspaper and one Chinese language daily newspaper in circulation in Hong Kong for at least three consecutive days.

Section: 33 **Government Chief Information Officer may publish code of practice** **L.N. 131 of 2004** **01/07/2004**

(1) The Government Chief Information Officer may publish in the Gazette a code of practice (Amended L.N. 131 of 2004):

(a) specifying standards and procedures for carrying out the functions of recognised certification authorities;

(b) specifying the provisions of this Ordinance and of the code of practice for the purposes of:

(i) section 20(3)(b)(i) and (c)(i);

(ii) section 27(5A)(b)(i) and (c)(i);

(iii) section 43(1)(a)(i) and (b)(i); and

(iv) section 43A(1)(c)(i) and (d)(i).

(2) The code of practice published under subs.(1) may make different provisions for different circumstances and provide for different cases or classes of cases.

(3) The Government Chief Information Officer may from time to time amend the whole or any part of the code of practice published under subs.(1) in a manner consistent with the power to publish the code under subs.(1), and any reference in this Ordinance to the code shall, unless the context otherwise requires, be construed as a reference to the code as so amended. (Amended L.N. 131 of 2004)

(4) Any code of practice published under subs.(1) is not subsidiary legislation. (Replaced 14 of 2004 s.18)

Explanatory Note

[33.01] This section provides for the GCIO to publish or amend the Code of Practice. The Code of Practice can be accessed on the website of the Office of the GCIO. The latest version was published in December 2004.

[33.02] The Code of Practice specifies standards and procedures to be adopted by recognised certification authorities when discharging their function. The Code of Practice however does not form part of the legislation and should be read in conjunction with the Ordinance. In the circumstances where the Code of Practice is inconsistent with any provision in the Ordinance, the Ordinance shall prevail.

Section: 34 **The Postmaster General as recognised certification authority** **1 of 2000** **07/01/2000**

PART IX

POSTMASTER GENERAL TO BE RECOGNISED CERTIFICATION AUTHORITY

(1) The Postmaster General is a recognised certification authority for the purposes of this Ordinance.

(2) Part VII does not apply to the Postmaster General as a certification authority.

Enactment history

This section was enacted in January 2000. [34.01]

Subsection (1): Definition of "Postmaster General"

According to s.2 of this Ordinance, the definition of the Postmaster General can be found in the Post Office Ordinance (Cap.98). Postmaster General means the Postmaster General of Hong Kong and includes the deputy postmaster general and every assistant postmaster general: s.2 of the Post Office Ordinance (Cap.98). [34.02]

Subsection (2): Part VII does not apply

Part VII sets out the Government's recognition scheme for certificate authorities including the application, renewal and appeal mechanism but the scheme does not apply to the Postmaster General as a certification authority. [34.03]

Section: 35 **Postmaster General may perform functions and provide services of certification authority** **1 of 2000** **07/01/2000**

(1) For the purposes of s.34, the Postmaster General may by himself or by the officers of the Post Office:

(a) perform the functions and provide the services of a certification authority and services incidental or related to the functions or services of a certification authority; and

(b) do anything that is necessary or expedient for the purposes of para (a) and for complying with any provision of this Ordinance relating to a recognised certification authority.

(2) The Postmaster General may determine and charge fees for providing the services of a certification authority or services incidental or related to the functions or services of a certification authority.

(3) The fees determined and charged under subs.(2) shall not be limited by reference to the administrative or other costs incurred or likely to be incurred or recovery of expenditure in the provision of the services of a certification authority or services incidental or related to the functions or services of a certification authority.

(4) The Postmaster General may give particulars of any fees determined under subs.(2) in such manner as the Postmaster General thinks fit.

Enactment history

This section was enacted in January 2000. [35.01]

Subsection (1): Definition of the "officers of the Post Office"

[35.02] According to s.2 of the Post Office Ordinance (Cap.98), officers of the Post Office include the Postmaster General and every other person employed in any business of the Postal Department or on behalf of the Postal Department.

Fees

[35.03] This section empowers the Postmaster General functioning as a recognised certification authority to charge fees for the services of a recognised certification authority and related and incidental services, on a commercial basis. Subsection (3) empowers the Postmaster General to charge service fees which can be above cost.

Subsection (4): Particulars of fees

[35.04] The Postmaster General has the discretion to determine the giving of particulars of the fees for providing services of a certification authority.

Section: 36 Publication of issued and accepted certificates 14 of 2004 30/06/2004

PART X

GENERAL PROVISIONS AS TO RECOGNISED CERTIFICATION AUTHORITIES

Where a person named or identified, or to be named or identified, in a recognized certificate as the person to whom the certificate is issued:

(1) accepts the certificate, the recognised certification authority concerned must publish the certificate in a repository as soon as reasonably practicable after it issues the certificate;
(2) does not accept the certificate, the recognised certification authority concerned must not publish the certificate.

(Replaced 14 of 2004 s.19)

Enactment history

[36.01] This section was substituted pursuant to s.19 of the Electronic Transactions (Amendment) Ordinance 2004 (14 of 2004), commencing on 30 June 2004.

[36.02] The original word "subscriber" in the 2000 version of the Ordinance was substituted by "person named or identified, or to be named or identified in a recognised certificate as the person to whom the certificate is issued". The sentence "as soon as reasonably practicable after it issues the certificate" was added to subs.(a) in 2004 version which emphasises the importance of efficiency.

General Note

[36.03] This section requires a recognised certification authority to publish in a recognised repository the certificate issued to the person named or identified, or to be named or identified, in a recognised certificate.

Definition of a "recognised certificate"

[36.04] As set out in s.2, a "recognised certificate" is a certificate recognised under s.22 or a certificate designated as one issued by the certification authority.

Definition of a "recognised certification authority"

[36.05] As set out in s.2, a "recognised certification authority" is a certification authority recognised under s.21 or one referred to in s.34.

Section: 37 Recognized certification authority to use trustworthy system 14 of 2004 30/06/2004

A recognised certification authority must use a trustworthy system in performing its services:

(a) to issue, revoke or suspend a recognised certificate; or
(b) to publish in a repository or give notice of the issue, revocation or suspension of a recognised certificate.

(Amended 14 of 2004 s.20)

Enactment history

[37.01] This section was amended pursuant to s.20 of the Electronic Transactions (Amendment) Ordinance 2004 (14 of 2004), commencing on 30 June 2004. The original words "or withdraw" and "or withdrawal" in the 2000 version of the Ordinance were substituted by "revoke or suspend" and "revocation or suspension" in 2004 for a broader coverage.

General Note

[37.02] This section requires a recognised certification authority to use a trustworthy system to issue, revoke, suspend or give notice of the issue, revocation or suspension of a certificate.

Section: 38 Presumption as to correctness of information 1 of 2000 07/01/2000

It shall be presumed, unless there is evidence to the contrary, that the information contained in a recognised certificate issued by a recognised certification authority (except information identified as subscriber's information which has not been verified by the recognised certification authority) is correct if the certificate was published in a repository.

Enactment history

[38.01] This section was enacted in January 2000.

General Note

[38.02] This section sets out a rebuttable presumption as to the correctness of information contained in a certificate published in a recognised repository.

No presumption

[38.03] The exception stated in the brackets is to the effect that there is no presumption as to correctness of information if such information was identified as subscriber's information which has not been verified by the recognised certification authority in the recognised certificate.

Section: 39 Representations upon issuance of recognised certificate 1 of 2000 07/01/2000

By issuing a recognised certificate, a recognised certification authority represents to any person who reasonably relies on the information contained in the certificate or a digital signature verifiable by the public key listed in the certificate, that the recognised 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.

Enactment history

[39.01] This section was enacted in January 2000.

Overview

[39.02] This section provides that upon issuance of a recognised certificate the recognised certification authority represents to a person (who reasonably relies on the information contained in it or a digital signature verifiable with reference to a public key listed in that certificate) that the certification authority has issued the certificate in accordance with the applicable certification practice statement.

Definition of "certification practice statement"

[39.03] Section 2(1) defines "certification practice statement" as a statement issued by a certification authority to specify the practices and standards that the certification authority employs in issuing certificates. The relevant standards and procedures can be found in the Code of Practice published by the GCIO under s.33 of the Ordinance.

Section: 40 Representations upon publication of recognised certificate 1 of 2000 07/01/2000

By publishing a recognised certificate, a recognised certification authority represents to any person who reasonably relies on the information contained in the

certificate, that the recognised certification authority has issued the certificate to the subscriber concerned.

Enactment history

This section was enacted in January 2000. [40.01]

Overview

This section states that publication of a certificate in a repository by a recognised certification authority amounts to a representation that the certification authority has issued a certificate to the subscriber concerned. [40.02]

Section: 41 Reliance limit 1 of 2000 07/01/2000

(1) A recognised certification authority may, in issuing a recognised certificate, specify a reliance limit in the certificate.

(2) The recognised certification authority may specify different limits in different recognised certificates or in different types, classes or description of certificates.

Enactment history

This section was enacted in January 2000. [41.01]

Overview

This section permits a recognised certification authority to set a reliance limit on certificates issued by it. [41.02]

Meaning of Reliance Limit

Reliance Limit means the monetary limit specified for reliance on a recognised certification. The recognised certification authority can set the reliance limit; it is however required to maintain suitable insurance or other form of coverage to cover its liability of the Code of Practice. According to para 8.2 of the Code of Practice, the minimum coverage for each claim should be the higher of: [41.03]

(1) 10 times the reliance limit specified by the recognised CA in its certification practice statement(s) in relation to its recognised certificates (where different reliance limits are specified for different recognised certificates that are covered under an insurance policy, the largest of the reliance limits shall be used); or

(2) $200,000.

Section: 42 Liability limits for recognised certification authorities 1 of 2000 07/01/2000

(1) Unless a recognised certification authority waives the application of this subsection, the recognised certification authority is not liable for any loss caused

Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)

PURPOSE OF THIS GUIDE

1. In preparing and adopting the UNCITRAL Model Law on Electronic Commerce (hereinafter referred to as "the Model Law"), the United Nations Commission on International Trade Law (UNCITRAL) was mindful that the Model Law would be a more effective tool for States modernizing their legislation if background and explanatory information would be provided to executive branches of Governments and legislators to assist them in using the Model Law. The Commission was also aware of the likelihood that the Model Law would be used in a number of States with limited familiarity with the type of communication techniques considered in the Model Law. This Guide, much of which is drawn from the *travaux préparatoires* of the Model Law, is also intended to be helpful to users of electronic means of communication as well as to scholars in that area. In the preparation of the Model Law, it was assumed that the draft Model Law would be accompanied by such a guide. For example, it was decided in respect of a number of issues not to settle them in the draft Model Law but to address them in the Guide so as to provide guidance to States enacting the draft Model Law. The information presented in this Guide is intended to explain why the provisions in the Model Law have been included as essential basic features of a statutory device designed to achieve the objectives of the Model Law. Such information might assist States also in considering which, if any, of the provisions of the Model Law might have to be varied to take into account particular national circumstances.

I. INTRODUCTION TO THE MODEL LAW

A. Objectives

2. The use of modern means of communication such as electronic mail and electronic data interchange (EDI) for the conduct of international trade transactions has been increasing rapidly and is expected to develop further as technical supports such as information highways and the INTERNET become more widely accessible. However, the communication of legally significant information in the form of paperless messages may be hindered by legal obstacles to the use of such

messages, or by uncertainty as to their legal effect or validity. The purpose of the Model Law is to offer national legislators a set of internationally acceptable rules as to how a number of such legal obstacles may be removed, and how a more secure legal environment may be created for what has become known as "electronic commerce". The principles expressed in the Model Law are also intended to be of use to individual users of electronic commerce in the drafting of some of the contractual solutions that might be needed to overcome the legal obstacles to the increased use of electronic commerce.

3. The decision by UNCITRAL to formulate model legislation on electronic commerce was taken in response to the fact that in a number of countries the existing legislation governing communication and storage of information is inadequate or outdated because it does not contemplate the use of electronic commerce. In certain cases, existing legislation imposes or implies restrictions on the use of modern means of communication, for example by prescribing the use of "written", "signed" or "original" documents. While a few countries have adopted specific provisions to deal with certain aspects of electronic commerce, there exists no legislation dealing with electronic commerce as a whole. This may result in uncertainty as to the legal nature and validity of information presented in a form other than a traditional paper document. Moreover, while sound laws and practices are necessary in all countries where the use of EDI and electronic mail is becoming widespread, this need is also felt in many countries with respect to such communication techniques as telecopy and telex.

4. The Model Law may also help to remedy disadvantages that stem from the fact that inadequate legislation at the national level creates obstacles to international trade, a significant amount of which is linked to the use of modern communication techniques. Disparities among, and uncertainty about, national legal regimes governing the use of such communication techniques may contribute to limiting the extent to which businesses may access international markets.

5. Furthermore, at an international level, the Model Law may be useful in certain cases as a tool for interpreting existing international conventions and other international instruments that create legal obstacles to the use of electronic commerce, for example by prescribing that certain documents or contractual clauses be made in written form. As between those States parties to such international instruments, the adoption of the Model Law as a rule of interpretation might provide the means to recognize the use of electronic commerce and obviate the need to negotiate a protocol to the international instrument involved.

6. The objectives of the Model Law, which include enabling or facilitating the use of electronic commerce and providing equal treatment to users of paper-based documentation and to users of computer-based information, are essential for fostering economy and efficiency in international trade. By incorporating the procedures prescribed in the Model Law in its national legislation for those situations where parties opt to use electronic means of communication, an enacting State would create a media-neutral environment.

B. Scope

7. The title of the Model Law refers to "electronic commerce". While a definition of "electronic data interchange (EDI)" is provided in article 2, the Model Law does not specify the meaning of "electronic commerce". In preparing the Model Law, the Commission decided that, in addressing the subject matter before it, it would have in mind a broad notion of EDI, covering a variety of trade-related uses of EDI that might be referred to broadly under the rubric of "electronic commerce" (see A/CN.9/360, paras. 28-29), although other descriptive terms could also be used. Among the means of communication encompassed in the notion of "electronic commerce" are the following modes of transmission based on the use of electronic techniques: communication by means of EDI defined narrowly as the computer-to-computer transmission of data in a standardized format; transmission of electronic messages involving the use of either publicly available standards or proprietary standards; transmission of free-formatted text by electronic means, for example through the INTERNET. It was also noted that, in certain circumstances, the notion of "electronic commerce" might cover the use of techniques such as telex and telecopy.

8. It should be noted that, while the Model Law was drafted with constant reference to the more modern communication techniques, e.g., EDI and electronic mail, the principles on which the Model Law is based, as well as its provisions, are intended to apply also in the context of less advanced communication techniques, such as telecopy. There may exist situations where digitalized information initially dispatched in the form of a standardized EDI message might, at some point in the communication chain between the sender and the recipient, be forwarded in the form of a computer-generated telex or in the form of a telecopy of a computer print-out. A data message may be initiated as an oral communication and end up in the form of a telecopy, or it may start as a telecopy and end up as an EDI message. A characteristic of electronic commerce is that it covers programmable messages, the computer programming of which is the essential difference between such messages and traditional paper-based documents. Such situations are intended to be covered by the Model Law, based on a consideration of the users' need for a consistent set of rules to govern a variety of communication techniques that might be used interchangeably. More generally, it may be noted that, as a matter of principle, no communication technique is excluded from the scope of the Model Law since future technical developments need to be accommodated.

9. The objectives of the Model Law are best served by the widest possible application of the Model Law. Thus, although there is provision made in the Model Law for exclusion of certain situations from the scope of articles 6, 7, 8, 11, 12, 15 and 17, an enacting State may well decide not to enact in its legislation substantial restrictions on the scope of application of the Model Law.

10. The Model Law should be regarded as a balanced and discrete set of rules, which are recommended to be enacted as a single statute. Depending on the

situation in each enacting State, however, the Model Law could be implemented in various ways, either as a single statute or in several pieces of legislation (see below, para. 143).

C. Structure

11. The Model Law is divided into two parts, one dealing with electronic commerce in general and the other one dealing with electronic commerce in specific areas. It should be noted that part two of the Model Law, which deals with electronic commerce in specific areas, is composed of a chapter I only, dealing with electronic commerce as it applies to the carriage of goods. Other aspects of electronic commerce might need to be dealt with in the future, and the Model Law can be regarded as an open-ended instrument, to be complemented by future work.

12. UNCITRAL intends to continue monitoring the technical, legal and commercial developments that underline the Model Law. It might, should it regard it advisable, decide to add new model provisions to the Model Law or modify the existing ones.

D. A "framework" law to be supplemented by technical regulations

13. The Model Law is intended to provide essential procedures and principles for facilitating the use of modern techniques for recording and communicating information in various types of circumstances. However, it is a "framework" law that does not itself set forth all the rules and regulations that may be necessary to implement those techniques in an enacting State. Moreover, the Model Law is not intended to cover every aspect of the use of electronic commerce. Accordingly, an enacting State may wish to issue regulations to fill in the procedural details for procedures authorized by the Model Law and to take account of the specific, possibly changing, circumstances at play in the enacting State, without compromising the objectives of the Model Law. It is recommended that, should it decide to issue such regulation, an enacting State should give particular attention to the need to maintain the beneficial flexibility of the provisions in the Model Law.

14. It should be noted that the techniques for recording and communicating information considered in the Model Law, beyond raising matters of procedure that may need to be addressed in the implementing technical regulations, may raise certain legal questions the answers to which will not necessarily be found in the Model Law, but rather in other bodies of law. Such other bodies of law may include, for example, the applicable administrative, contract, criminal and judicial-procedure law, which the Model Law is not intended to deal with.

E. The "functional-equivalent" approach

15. The Model Law is based on the recognition that legal requirements prescribing the use of traditional paper-based documentation constitute the main obstacle to the development of modern means of communication. In the preparation of the Model Law, consideration was given to the possibility of dealing with impediments to the use of electronic commerce posed by such requirements in national laws by way of an extension of the scope of such notions as "writing", "signature" and "original", with a view to encompassing computer-based techniques. Such an approach is used in a number of existing legal instruments, e.g., article 7 of the UNCITRAL Model Law on International Commercial Arbitration and article 13 of the United Nations Convention on Contracts for the International Sale of Goods. It was observed that the Model Law should permit States to adapt their domestic legislation to developments in communications technology applicable to trade law without necessitating the wholesale removal of the paper-based requirements themselves or disturbing the legal concepts and approaches underlying those requirements. At the same time, it was said that the electronic fulfilment of writing requirements might in some cases necessitate the development of new rules. This was due to one of many distinctions between EDI messages and paper-based documents, namely, that the latter were readable by the human eye, while the former were not so readable unless reduced to paper or displayed on a screen.

16. The Model Law thus relies on a new approach, sometimes referred to as the "functional equivalent approach", which is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques. For example, among the functions served by a paper document are the following: to provide that a document would be legible by all; to provide that a document would remain unaltered over time; to allow for the reproduction of a document so that each party would hold a copy of the same data; to allow for the authentication of data by means of a signature; and to provide that a document would be in a form acceptable to public authorities and courts. It should be noted that in respect of all of the above-mentioned functions of paper, electronic records can provide the same level of security as paper and, in most cases, a much higher degree of reliability and speed, especially with respect to the identification of the source and content of the data, provided that a number of technical and legal requirements are met. However, the adoption of the functional-equivalent approach should not result in imposing on users of electronic commerce more stringent standards of security (and the related costs) than in a paper-based environment.

17. A data message, in and of itself, cannot be regarded as an equivalent of a paper document in that it is of a different nature and does not necessarily perform all conceivable functions of a paper document. That is why the Model Law adopted a flexible standard, taking into account the various layers of existing requirements in a paper-based environment: when adopting the "functional-equivalent" approach,

attention was given to the existing hierarchy of form requirements, which provides distinct levels of reliability, traceability and unalterability with respect to paper-based documents. For example, the requirement that data be presented in written form (which constitutes a "threshold requirement") is not to be confused with more stringent requirements such as "signed writing", "signed original" or "authenticated legal act".

18. The Model Law does not attempt to define a computer-based equivalent to any kind of paper document. Instead, it singles out basic functions of paper-based form requirements, with a view to providing criteria which, once they are met by data messages, enable such data messages to enjoy the same level of legal recognition as corresponding paper documents performing the same function. It should be noted that the functional-equivalent approach has been taken in articles 6 to 8 of the Model Law with respect to the concepts of "writing", "signature" and "original" but not with respect to other legal concepts dealt with in the Model Law. For example, article 10 does not attempt to create a functional equivalent of existing storage requirements.

F. Default rules and mandatory law

19. The decision to undertake the preparation of the Model Law was based on the recognition that, in practice, solutions to most of the legal difficulties raised by the use of modern means of communication are sought within contracts. The Model Law embodies the principle of party autonomy in article 4 with respect to the provisions contained in chapter III of part one. Chapter III of part one contains a set of rules of the kind that would typically be found in agreements between parties, e.g., interchange agreements or "system rules". It should be noted that the notion of "system rules" might cover two different categories of rules, namely, general terms provided by communication networks and specific rules that might be included in those general terms to deal with bilateral relationships between originators and addressees of data messages. Article 4 (and the notion of "agreement" therein) is intended to encompass both categories of "system rules".

20. The rules contained in chapter III of part one may be used by parties as a basis for concluding such agreements. They may also be used to supplement the terms of agreements in cases of gaps or omissions in contractual stipulations. In addition, they may be regarded as setting a basic standard for situations where data messages are exchanged without a previous agreement being entered into by the communicating parties, e.g., in the context of open-networks communications.

21. The provisions contained in chapter II of part one are of a different nature. One of the main purposes of the Model Law is to facilitate the use of modern communication techniques and to provide certainty with the use of such techniques where obstacles or uncertainty resulting from statutory provisions could not be avoided by contractual stipulations. The provisions contained in chapter II may,

to some extent, be regarded as a collection of exceptions to well-established rules regarding the form of legal transactions. Such well-established rules are normally of a mandatory nature since they generally reflect decisions of public policy. The provisions contained in chapter II should be regarded as stating the minimum acceptable form requirement and are, for that reason, of a mandatory nature, unless expressly stated otherwise in those provisions. The indication that such form requirements are to be regarded as the "minimum acceptable" should not, however, be construed as inviting States to establish requirements stricter than those contained in the Model Law.

G. Assistance from UNCITRAL secretariat

22. In line with its training and assistance activities, the UNCITRAL secretariat may provide technical consultations for Governments preparing legislation based on the UNCITRAL Model Law on Electronic Commerce, as it may for Governments considering legislation based on other UNCITRAL model laws, or considering adhesion to one of the international trade law conventions prepared by UNCITRAL.

23. Further information concerning the Model Law as well as the Guide and other model laws and conventions developed by UNCITRAL, may be obtained from the secretariat at the address below. The secretariat welcomes comments concerning the Model Law and the Guide, as well as information concerning enactment of legislation based on the Model Law.

International Trade Law Branch, Office of Legal Affairs,
United Nations
Vienna International Centre P.O. Box 500
A-1400, Vienna, Austria
Telephone: (43-1) 26060-4060 or 4061
Telefax: (43-1) 26060-5813 or (43-1) 263 3389
Telex: 135612 uno a
E-mail: uncitral@unov.un.or.at
Internet Home Page: http://www.un.or.at/uncitral

II. ARTICLE-BY-ARTICLE REMARKS

Part one. Electronic commerce in general

CHAPTER I. GENERAL PROVISIONS

Article 1. Sphere of application

24. The purpose of article 1, which is to be read in conjunction with the definition of "data message" in article 2*(a)*, is to delineate the scope of application of the Model Law. The approach used in the Model Law is to provide in principle for the coverage of all factual situations where information is generated, stored or communicated, irrespective of the medium on which such information may be affixed. It was felt during the preparation of the Model Law that exclusion of any form or medium by way of a limitation in the scope of the Model Law might result in practical difficulties and would run counter to the purpose of providing truly "media-neutral" rules. However, the focus of the Model Law is on "paperless" means of communication and, except to the extent expressly provided by the Model Law, the Model Law is not intended to alter traditional rules on paper-based communications.

25. Moreover, it was felt that the Model Law should contain an indication that its focus was on the types of situations encountered in the commercial area and that it had been prepared against the background of trade relationships. For that reason, article 1 refers to "commercial activities" and provides, in footnote ****, indications as to what is meant thereby. Such indications, which may be particularly useful for those countries where there does not exist a discrete body of commercial law, are modelled, for reasons of consistency, on the footnote to article 1 of the UNCITRAL Model Law on International Commercial Arbitration. In certain countries, the use of footnotes in a statutory text would not be regarded as acceptable legislative practice. National authorities enacting the Model Law might thus consider the possible inclusion of the text of footnotes in the body of the Law itself.

26. The Model Law applies to all kinds of data messages that might be generated, stored or communicated, and nothing in the Model Law should prevent an enacting State from extending the scope of the Model Law to cover uses of electronic commerce outside the commercial sphere. For example, while the focus of the Model Law is not on the relationships between users of electronic commerce and public authorities, the Model Law is not intended to be inapplicable to such relationships. Footnote *** provides for alternative wordings, for possible use by enacting States that would consider it appropriate to extend the scope of the Model Law beyond the commercial sphere.