Hong Kong, China

Table of Contents

Hong Kong China

[HC/L] Electronic Transactions Ordinance

2000.1.7 Proclamation

Graunded on		Remarks
cl.num.	Clause	
	Part 1 Preliminary	
	1 Short title and commencement	
HC/L-1.1	**HC/L** may be cited as the Electronic Transactions Ordinance.	
HC/L-1.2	Part 1, **HC/L-4** and **9**, Part 5 (other than in relation to the matters referred to in Schedule 1) and Part 6, **HC/L-31** and **33** and Parts 9, 10, 11 and 12 shall come into operation at the beginning of the day on which **HC/L** is published in the Gazette.	

Graunded on		Remarks
cl.num.	Clause	
HC/L-1.3	**HC/L-3**, **5**, **6**, **7**, **8** and **10**, Part 4, Part 5 (in relation to the matters referred to in Schedule 1) and Part 7, **HC/L-32** and Schedules 1 and 2 shall come into operation on a day to be appointed by the Secretary for Information Technology and Broadcasting by notice in the Gazette.	
	2 Interpretation	
HC/L-2.1	In **HC/L**, unless the context otherwise requires---	
	1) "accept a certificate", in relation to a person to whom a certificate is issued, means that the person while having notice of the contents of the certificate---	
	(a) authorizes the publication of the certificate to one or more persons or in a repository;	
	(b) uses the certificate; or	
	(c) otherwise demonstrates the approval of the certificate;	
	2) "addressee" , 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;	
	3) "asymmetric cryptosystem" 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;	
	4) "certificate" 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;	

Graunded on		Remarks
cl.num.	Clause	
	(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 a responsible officer of the certification authority issuing it; 5) "certification authority" means a person who issues a certificate to a person (who may be another certification authority); 6) "certification authority disclosure record", in relation to a recognized certification authority, means the record maintained under **HC/L-31** for that certification authority; 7) "CPS" means a statement issued by a certification authority to specify the practices and standards that the certification authority employs in issuing certificates; 8) "code of practice" (HC/COP) means the code of practice issued under **HC/L-33**; 9) "correspond", in relation to private or public keys, means to belong to the same key pair; 10) "digital signature", 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; 11) "Director" means the Director of Information Technology Services;	

Graunded on		Remarks
cl.num.	Clause	
	12) "electronic record" 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;	
	13) "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 for the purpose of authenticating or approving the electronic record;	
	14) "hash function" 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 2 records can be found to produce the same hash result using the algorithm;	
	15) "information" includes data, text, images, sound codes, computer programmes, software and databases;	
	16) "information system" 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	

Graunded on		Remarks
cl.num.	Clause	
	(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);	
	17) "intermediary", 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;	
	18) "issue", in relation to a certificate, means the act of a certification authority of creating a certificate and notifying its contents to the person named or identified in that certificate as the person to whom it is issued;	
	19) "key pair", 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;	
	20) "originator", 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;	
	21) "Postmaster General" means the Postmaster General within the meaning of the Post Office Ordinance (Cap. 98);	
	22) "private key" means the key of a key pair used to generate a digital signature;	
	23) "public key" means the key of a key pair used to verify a digital signature;	
	24) "recognized certificate" means---	
	(a) a certificate recognized under **HC/L-22**;	
	(b) a certificate of a type, class or description of certificate recognized under **HC/L-22**; or	
	(c) a certificate designated as a recognized certificate issued by the certification authority referred to in **HC/L-34**;	

Graunded on		Remarks
cl.num.	Clause	
	25) "recognized certification authority" means a certification authority recognized under **HC/L-21** or the certification authority referred to in **HC/L-34**;	
	26) "record" 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;	
	27) "reliance limit" means the monetary limit specified for reliance on a recognized certificate;	
	28) "repository" means an information system for storing and retrieving certificates and other information relevant to certificates;	
	29) "responsible officer", 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 **HC/L**;	
	30) "rule of law" means--- (a) an Ordinance; (b) a rule of common law or a rule of equity; or (c) customary law;	
	31) "Secretary" means the Secretary for Information Technology and Broadcasting;	
	32) "sign" and "signature" 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;	
	33) "subscriber" 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;	

Graunded on		Remarks
cl.num.	Clause	
	34) "trustworthy system" 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;	
	35) "verify a digital signature", 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.	
HC/L-2.2	For the purposes of **HC/L**, 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.	
	Part 2 Application	
	3 Matters to which HC/L-5, 6, 7, 8 and 17 are not applicable	

	Graunded on	Remarks
cl.num.	Clause	
HC/L-3.1	**HC/L-5**, 6, 7, 8 and 17 do not apply to any--- (a) requirement or permission for information to be or given in writing; (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 Schedule 1, unless that rule of law expressly provides otherwise.	
	4 Ordinance to bind Government	
HC/L-4.1	**HC/L** binds the Government.	
	Part 3 Electronic Records and Digital Signatures	
	5 Requirement for writing	
HC/L-5.1	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.	
HC/L-5.2	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.	

Graunded on		Remarks
cl.num.	Clause	
	6 Digital signatures	
HC/L-6.1	If a rule of law requires the signature of a person or provides for certain consequences if a document is not signed by a person, a digital signature of the person satisfies the requirement but only if the digital signature is supported by a recognized certificate and is generated within the validity of that certificate.	
HC/L-6.2	In **HC/L-6.1**, "within the validity of that certificate" means that at the time the digital signature is generated--- (a) the recognition of the recognized certificate is not revoked or suspended; (b) if the Director has specified a period of validity for the recognition of the recognized certificate, the certificate is within that period; and (c) if the recognized certification authority has specified a period of validity for the recognized certificate, the certificate is within that period.	
	7 Presentation or retention of information in its original form	
HC/L-7.1	Where a rule of law requires that certain information be presented or retained in its original form, the requirement is satisfied by presenting or retaining the information in the form of electronic records if--- (a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form; and	

Graunded on		Remarks
cl.num.	Clause	
	(b) where it is required that information be presented, the information is capable of being displayed in a legible form to the person to whom it is to be presented.	
HC/L-7.2	For the purposes of **HC/L-7.1 (a)**--- (a) the criterion for assessing the integrity of the information is whether the information has remained complete and unaltered, apart from the addition of any endorsement or any change which arises in the normal course of communication, storage or display; and (b) the standard for reliability of the assurance is to be assessed having regard to the purpose for which the information was generated and all the other relevant circumstances.	
HC/L-7.3	This section applies whether the requirement in **HC/L-7.1** is in the form of an obligation or whether the rule of law merely provides consequences for the information not being presented or retained in its original form.	
	8 Retention of information in electronic records	
HC/L-8.1	Where a rule of law requires certain information to be retained, whether in writing or otherwise, the requirement is satisfied by retaining electronic records, if--- (a) the information contained in the electronic record remains accessible so as to be usable for subsequent reference; (b) the relevant electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received; and	

Graunded on		Remarks
cl.num.	Clause	
	(c) the information which enables the identification of the origin and destination of the electronic record and the date and time when it was sent or received, is retained.	
HC/L-8.2	This section applies whether the requirement in **HC/L-8.1** is in the form of an obligation or whether the rule of law merely provides consequences for the information not being retained.	
	9 Admissibility of electronic records	
HC/L-9.1	Without prejudice to any rules of evidence, an electronic record shall not be denied admissibility in evidence in any legal proceeding on the sole ground that it is an electronic record.	
	10 Construction of this Part subject to Part 4	
HC/L-10.1	This Part is to be construed subject to Part 4.	
	Part 4 Limitations on Operation of HC/L-5, 6, 7 and 8	
	11 Secretary may make orders excluding application of HC/L-5, 6, 7 or 8	

Graunded on		Remarks
cl.num.	Clause	
HC/L-11.1	The Secretary may by order published in the Gazette exclude an Ordinance or a particular requirement or permission in an Ordinance or a class or description of requirements or permissions in an Ordinance, to which **HC/L** would otherwise apply, from the application of **HC/L-5**, 6, 7 or 8.	
HC/L-11.2	The Secretary may, in relation to an Ordinance to which **HC/L** applies, specify by notice published in the Gazette--- (a) the manner and format in which information in the form of an electronic record is to be given, presented or retained for the purposes of that Ordinance or a particular requirement or permission in that Ordinance or a class or description of requirements or permissions in that Ordinance; and (b) the procedure and criteria for verification of the receipt of that information and for ensuring the integrity and confidentiality of the information.	
HC/L-11.3	The Secretary may specify different requirements under **HC/L-11.2** (a) or (b) in relation to persons or cases of different classes or descriptions.	
HC/L-11.4	An order under **HC/L-11.1** is subsidiary legislation.	
HC/L-11.5	A notice under **HC/L-11.2** is not subsidiary legislation.	
HC/L-11.6	In this section, "manner and format" includes requirements as to software, communication, data storage, how the electronic record is to be generated, sent, stored or received and where a signature is required, the type of signature and how the signature is to be affixed to the electronic record.	

Graunded on		Remarks
cl.num.	Clause	
	12 Electronic record to comply with specified requirements to satisfy HC/L-5, 6, 7 and 8	
HC/L-12.1	If the Secretary has specified any requirement under **HC/L-11.2** in relation to an Ordinance, the information given, presented or retained or the signature made, as the case may require, for the purpose of that Ordinance does not satisfy that Ordinance unless it complies with the specified requirements.	
	13 Rules of court or procedure only to apply where relevant authority provides for application	
HC/L-13.1	**HC/L-**5, 6, 7 or 8 does not apply in relation to information given, presented or retained or signatures required for the purposes of any proceedings set out in Schedule 2, unless any rule of law relating to those proceedings provide for its application.	
HC/L-13.2	**HC/L-13.1** is not to be construed as affecting any provision in a rule of law referred to in that subsection, requiring or permitting, otherwise than by reference to **HC/L**, the use of electronic records or electronic signatures for the purposes of the proceedings to which the rule of law relates.	
HC/L-13.3	Any authority given by a rule of law to make rules (however described) for the purpose of any proceedings set out in Schedule 2 is to be construed as including a power to provide for--- (a) the application of **HC/L-**5, 6, 7 or 8; and (b) the specification of the matters referred to in **HC/L11.2** (a) and (b), by subsidiary legislation or otherwise, consequent to such application.	

Graunded on		Remarks
cl.num.	Clause	
	14 HC/L-5, 6, 7 and 8 not to affect specific provisions as to electronic records in other Ordinances	
HC/L-14.1	If an Ordinance requires or permits giving, presenting or retaining information in the form of an electronic record or the authentication of information by an electronic signature for the purposes of that Ordinance, but contains an express provision which--- (a) specifies requirements, procedures or other specifications for that purpose; (b) requires the use of a specified service; or (c) confers a discretion on a person whether or when to accept electronic records or electronic signatures for that purpose, **HC/L-**5, 6, 7 or 8 is not to be construed as affecting that express provision.	
	15 When HC/L-5, 6 and 7 apply to transactions between persons who are not government entities	
HC/L-15.1	If an Ordinance requires information to be given by a person to another and neither person is or is acting on behalf of a government entity, **HC/L-5.1** applies only if the person to whom the information is to be given consents to it being given in the form of an electronic record.	
HC/L-15.2	If an Ordinance permits information to be given by a person to another and neither person is or is acting on behalf of a government entity, **HC/L-5.2** applies only if the person to whom the information is to be given consents to it being given in the form of an electronic record.	

Graunded on		Remarks
cl.num.	Clause	
HC/L-15.3	If an Ordinance requires the signature of a person ("the signer") and neither the signer 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, **HC/L-6** applies only if the second mentioned person consents to the signer's digital signature being given.	
HC/L-15.4	If an Ordinance requires information to be presented in its original form and neither the person presenting it nor the person to whom it is to be presented ("the second mentioned person") is or is acting on behalf of a government entity, **HC/L-7.1** applies only if the second mentioned person consents to it being presented in the form of an electronic record.	
HC/L-15.5	In this section--- "consent" includes consent that can be reasonably inferred from the conduct of the person concerned; "government entity" means a public officer or a public body.	
	16 HC/L-5, 6, 7 and 8 not to have effect if their operation affects other statutory requirements	
HC/L-16.1	If the effect of **HC/L-**5 on a requirement or permission in an Ordinance for information to be or given in writing ("requirement for writing") is such that any other requirement in that Ordinance or a related Ordinance (that is a requirement other than the requirement for writing) cannot be complied with due to the operation of that section, **HC/L-**5 does not apply to the requirement for writing.	

Graunded on		Remarks
cl.num.	Clause	
HC/L-16.2	If the effect of **HC/L-**6 on a requirement in an Ordinance for the signature of a person is such that any other requirement in that Ordinance or a related Ordinance (that is a requirement other than the requirement for the signature of a person) cannot be complied with due to the operation of that section, **HC/L-**6 does not apply to the requirement for the signature of a person.	
HC/L-16.3	If the effect of **HC/L-**7 on a requirement in an Ordinance for information to be presented or retained in its original form ("requirement for original form") is such that any other requirement in that Ordinance or a related Ordinance (that is a requirement other than the requirement for original form) cannot be complied with due to the operation of that section, **HC/L-**7 does not apply to the requirement for original form.	
HC/L-16.4	If the effect of **HC/L-**8 on a requirement in an Ordinance for information to be retained ("requirement for retention") is such that any other requirement in that Ordinance or a related Ordinance (that is a requirement other than the requirement for retention) cannot be complied with due to the operation of that section, **HC/L-**8 does not apply to the requirement for retention.	
	Part 5 Electronic Contracts	
	17 Formation and validity of electronic contracts	
HC/L-17.1	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 in whole or in part expressed by means of electronic records.	

Graunded on		Remarks
cl.num.	Clause	
HC/L-17.2	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.	
HC/L-17.3	For the avoidance of doubt, it is stated that this section does not affect any rule of common law to the effect that the offeror may prescribe the method of communicating acceptance.	
	Part 6 Attribution of Sending and Receiving Electronic Records	
	18 Attribution of Electronic Record	
HC/L-18.1	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.	
HC/L-18.2	Nothing in **HC/L-18.1** is to affect the law of agency or the law on the formation of contracts.	
	19 Sending and receiving electronic records	

Graunded on		Remarks
cl.num.	Clause	
HC/L-19.1	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.	
HC/L-19.2	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.	
HC/L-19.3	**HC/L-19.1** and 19.2 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 **HC/L-19.4**.	
HC/L-19.4	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.	

Graunded on		Remarks
cl.num.	Clause	
HC/L-19.5	For the purposes of **HC/L-19.4**--- (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.	
HC/L-19.6	Where the originator and the addressee are in different time zones, time refers to Universal Standard Time.	
	Part 7 Recognition of Certification Authorities and Certificates by Director	
	20 Certification authority may apply to Director for recognition	
HC/L-20.1	A certification authority may apply to the Director to become a recognized certification authority for the purposes of **HC/L**.	
HC/L-20.2	Subject to **HC/L-20.4** and **HC/L-21.3**, an application under **HC/L-20.1** must be made in the prescribed manner and in a form specified by the Director and the applicant must pay the prescribed fee in respect of the application.	
HC/L-20.3	An applicant must furnish to the Director--- (a) the relevant particulars and documents specified under **HC/L-**30; and	

Graunded on		Remarks
cl.num.	Clause	
	(b) a report which--- (i) contains an assessment as to whether the applicant is capable of complying with the provisions of **HC/L** applicable to a recognized certification authority and the HC/COP; and (ii) is prepared by a person acceptable to the Director as being qualified to give such a report.	
HC/L-20.4	The Director may waive--- (a) the requirements as to manner and form of making the application in **HC/L-20.2**; or (b) the requirement of a report under **HC/L-20.3**, in relation to a certification authority, in the circumstances specified in **HC/L-20.5**.	
HC/L-20.5	The Director may waive the requirements referred to in **HC/L-20.4** only if--- (a) the applicant is a certification authority with a status in a place outside Hong Kong comparable to that of a recognized certification authority ("comparable status"); and (b) the competent authority of that place accords to a recognized certification authority a comparable status on the basis of it being a recognized certification authority.	
	21 Director may on application recognize certification authorities	
HC/L-21.1	The Director may--- (a) recognize an applicant under **HC/L-**20 as a recognized certification authority if the Director is satisfied that the applicant is suitable for such recognition; or (b) refuse the application for recognition.	

Graunded on		Remarks
cl.num.	Clause	
HC/L-21.2	The Director must give reasons in writing to the applicant for refusing an application under **HC/L-21.1** (b).	
HC/L-21.3	The Director may, in recognizing a certification authority referred to in **HC/L-20.4**, waive the whole or part of the prescribed fee as the Director may decide in relation to a particular case.	
HC/L-21.4	In determining whether an applicant is suitable for recognition under **HC/L-21.1**, the Director shall, in addition to any other matter the Director considers relevant, take into account the following--- (a) whether the applicant has the appropriate financial status for operating as a recognized certification authority in accordance with **HC/L** and HC/COP; (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 **HC/L**; (c) the system, procedure, security arrangements and standards used or proposed to be used by the applicant to issue certificates to subscribers; (d) the report referred to in **HC/L-20.3** (b) (if applicable); (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.	
HC/L-21.5	In determining whether a person referred to in **HC/L-21.4** (e) is a fit and proper person, the Director shall, in addition to any other matter the Director considers relevant, have regard to the following--- (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;	

Graunded on		Remarks
cl.num.	Clause	
	(b) the fact that the person has been convicted of an offence against **HC/L**;	
	(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 5 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 winding-up 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 5 years preceding the date of the application.	
HC/L-21.6	In recognizing a certification authority under **HC/L-21.1**, the Director may---	
	(a) attach conditions to the recognition; or	
	(b) specify a period of validity for the recognition.	
	22 Director may recognize certificates	
HC/L-22.1	The Director may recognize certificates issued by a recognized certification authority as recognized certificates, upon application by that authority.	
HC/L-22.2	An applicant under **HC/L-22.1** must make the application in the prescribed manner and in a form specified by the Director and furnish to the Director the relevant particulars and documents specified under **HC/L-**30.	
HC/L-22.3	A recognition under **HC/L-22.1** may relate to---	
	(a) all certificates issued by the recognized certification authority;	

Graunded on		Remarks
cl.num.	Clause	
	(b) certificates of a type, class or description; or (c) particular certificates.	
HC/L-22.4	An applicant must pay the prescribed fee (if any) in respect of an application under **HC/L-22.1** unless the Director waives it in whole or in part.	
HC/L-22.5	In recognizing certificates under this section, the Director shall in addition to any other matter the Director considers relevant take into account the following--- (a) whether the certificates are issued in accordance with the CPS; (b) whether the certificates are issued in accordance with HC/COP; (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.	
HC/L-22.6	The Director may refuse an application under **HC/L-22.1**.	
HC/L-22.7	The Director must give reasons in writing to the applicant for refusing an application under **HC/L-22.6**.	
HC/L-22.8	The Director may specify a period of validity for a recognition under this section.	
HC/L-22.9	The Director may upon application renew a recognition under this section.	
HC/L-22.10	**HC/L-22.**2, 22.3, 22.4, 22.5, 22.6, 22.7 and 22.8 apply to a renewal under **HC/L-22.9**, subject to necessary modifications.	
	23 Director may revoke recognition	

Graunded on		Remarks
cl.num.	Clause	
HC/L-23.1	The Director may revoke a recognition granted under **HC/L-**21 or 22 or renewed under **HC/L-**22 or 27.	
HC/L-23.2	Before revoking a recognition, the Director must give the certification authority a notice of intention to revoke the recognition specifying the reasons for the intended revocation.	
HC/L-23.3	In a notice under **HC/L-23.2**, the Director must invite the certification authority to make representations as to why the recognition should not be revoked and specify a period for making the representations.	
HC/L-23.4	If the Director decides to revoke a recognition, the Director must immediately give the certification authority notice in writing of the decision specifying the reasons for the decision and the date on which the decision was made.	
HC/L-23.5	A revocation of recognition in relation to certificates may relate to all certificates issued by a recognized certification authority or to a type, class or description of certificates or a particular certificate.	
HC/L-23.6	Subject to **HC/L-23.7**, a revocation takes effect on the expiry of 7 days from the date on which the decision to revoke the recognition is made.	
HC/L-23.7	If the certification authority appeals under **HC/L-**28 against the revocation, the revocation does not take effect until the expiry of 7 days from the date on which the Secretary confirms the revocation on appeal.	
	24 Director may suspend recognition	
HC/L-24.1	The Director may suspend a recognition granted under **HC/L-**21 or 22 or renewed under **HC/L-**22 or 27 for a period not exceeding 14 days.	

Graunded on		Remarks
cl.num.	Clause	
HC/L-24.2	If the Director decides to suspend a recognition, the Director must immediately give the certification authority notice in writing of the decision specifying the reasons for the decision and the date on which the decision was made.	
HC/L-24.3	A suspension of recognition in relation to certificates may relate to all certificates issued by a recognized certification authority or to a type, class or description of certificates or a particular certificate.	
HC/L-24.4	Subject to **HC/L24.5**, a suspension takes effect on the expiry of 7 days from the date on which the decision to suspend the recognition is made.	
HC/L-24.5	If the certification authority appeals under **HC/L-**28 against the suspension, the suspension does not take effect until the expiry of 7 days from the date on which the Secretary confirms the suspension on appeal.	
HC/L-24.6	If the period of suspension expires during the validity of a recognition and the recognition is not revoked, the recognition is taken to be reinstated.	
	25 Matters Director may take into account in revoking or suspending a recognition	
HC/L-25.1	The Director may, in revoking or suspending a recognition under **HC/L-**23 or 24, in addition to any other matter that the Director considers relevant, take into account the following--- (a) any matter set out in **HC/L-21.4**; (b) whether the certification authority has failed--- (i) to operate in accordance with the CPS; (ii) to comply with HC/COP; (iii) to use a trustworthy system; or (iv) to comply with any provision of **HC/L**; and	

Graunded on		Remarks
cl.num.	Clause	
	(c) the relevant report furnished under **HC/L-**43.	
	26 Effect of revocation, suspension of recognition or expiry of validity of recognized certificate	
HC/L-26.1	Where the revocation or suspension of a recognition of a certification authority has taken effect or the period of validity of a recognition specified under **HC/L-**21.6 (b) has expired, the provisions of **HC/L** relating to--- (a) a recognized certification authority do not apply to that certification authority; (b) recognized certificates issued by a recognized certification authority do not apply to the certificates issued by that certification authority; and (c) digital signatures supported by a recognized certificate issued by a recognized certification authority do not apply to the digital signatures supported by the certificates issued by that certification authority.	
HC/L-26.2	Where the revocation or suspension of the recognition of a recognized certificate has taken effect, the provisions of **HC/L** relating to a recognized certificate or digital signatures supported by a recognized certificate do not apply to--- (a) the certificate of which the recognition is revoked or suspended; (b) any certificate of the type, class or description of certificate the recognition of which is revoked or suspended;	

Graunded on		Remarks
cl.num.	Clause	
	(c) digital signatures supported by that certificate or a certificate of that type, class or description, as the case may be.	
HC/L-26.3	Where the validity of a recognized certificate or the period of validity of a recognition specified under **HC/L-**22.8 has expired, the provisions of **HC/L** relating to recognized certificates issued by a recognized certification authority and digital signatures supported by a recognized certificate issued by a recognized certification authority do not apply to the certificate and the digital signatures supported by the certificate.	
HC/L-26.4	The revocation or suspension of the recognition of a certification authority does not affect the valid use of a recognized certificate issued by that certification authority before the revocation or suspension took effect or after the reinstatement of the recognition.	
HC/L-26.5	The revocation or suspension of the recognition of a certificate does not affect the valid use of the certificate concerned before the revocation or suspension took effect or after the reinstatement of the recognition.	
HC/L-26.6	The expiry of the period of validity of the recognition of a certificate specified under **HC/L-**22.8 or the expiry of the period of validity of a recognized certificate does not affect the valid use of the certificate concerned before the expiry of the period of validity of the recognition or the certificate, as the case may be.	
HC/L-26.7	The expiry of the period of validity of the recognition of a certification authority specified under **HC/L-**21.6 (b) does not affect the valid use of a recognized certificate issued by that certification authority during the period of validity of its recognition.	

Graunded on		Remarks
cl.num.	Clause	
	27 Director may renew recognition of certification authority	
HC/L-27.1	A certification authority recognized under **HC/L-**21 may apply to the Director for renewal of a recognition.	
HC/L-27.2	An application for renewal must be made at least 30 days before but not earlier than 60 days before the expiry of the period of validity of the recognition.	
HC/L-27.3	An application for renewal must be sent to the Director as an electronic record or delivered by hand to the Director or left at the office of the Director during the ordinary business hours of that office.	
HC/L-27.4	Subject to **HC/L-27.2**, 27.3 and 27.6, an application for renewal is to be made in the prescribed manner and in a form specified by the Director and if the Director so requires, the applicant must furnish to the Director the relevant particulars and documents specified under **HC/L-**30.	
HC/L-27.5	Subject to **HC/L-27.6**, an applicant must pay the prescribed fee in respect of an application for renewal.	
HC/L-27.6	The Director may, in the circumstances specified in **HC/L-20.5**, waive the requirements in **HC/L-27.4** or the whole or part of the prescribed fee as the Director may decide in relation to a particular case.	
HC/L-27.7	**HC/L-21.4** and 21.6 applies to a renewal of a recognition subject to necessary modifications.	
	28 Certification authority may appeal to Secretary against decision of Director	

Graunded on		Remarks
cl.num.	Clause	
HC/L-28.1	A certification authority aggrieved by a decision of the Director--- (a) refusing an application for recognition under **HC/L-**21 or 22; (b) refusing an application for renewal of a recognition under **HC/L-**22 or 27; or (c) revoking or suspending a recognition under **HC/L-**23 or 24, may appeal to the Secretary against the decision within 7 days from the date on which the relevant decision is made.	
HC/L-28.2	An appeal under **HC/L28.1** must be commenced by sending a notice of appeal to the Secretary as an electronic record or delivering the notice by hand to the Secretary or leaving the notice at the office of the Secretary during the ordinary business hours of that office.	
HC/L-28.3	A certification authority who appeals to the Secretary under this section must also give notice of the appeal to the Director as soon as practicable.	
HC/L-28.4	On appeal under **HC/L28.1**, the Secretary may confirm, vary or reverse the decision of the Director.	
HC/L-28.5	The Secretary must give the appellant notice of the decision on appeal, together with reasons--- (a) by sending it to the appellant as an electronic record; or (b) by sending it by post or registered post to the last known address of the appellant.	
HC/L-28.6	If in a particular case it is not reasonably practicable to give the notice of the decision on appeal by either of the means specified in **HC/L-28.5**, the notice is taken to have been given if the Secretary publishes it in the certification authority disclosure record maintained under **HC/L-**31 for the appellant.	

Graunded on		Remarks
cl.num.	Clause	
	29 How Director may give notices under this Part	
HC/L-29.1	A notice or other document the Director is required to give to a certification authority under this Part is taken to have been given if it is--- (a) sent to the certification authority as an electronic record; or (b) sent by post or registered post to the last known address of the certification authority.	
HC/L-29.2	If in a particular case it is not reasonably practicable to give a notice or other document under this Part by either of the means specified in **HC/L-29.1**, the notice or document is taken to have been given if the Director publishes it in the relevant certification authority disclosure record.	
	30 Director to specify particulars and documents by notice in the Gazette	
HC/L-30.1	The Director must specify by notice published in the Gazette any particulars and documents to be furnished under **HC/L-20.3** (a), 22.2 and 22.10 and 27.4.	
HC/L-30.2	A notice under **HC/L-30.1** is not subsidiary legislation.	
	Part 8 Certification Authority Disclosure Records and Code of Practice	
	31 Director to maintain certification authority disclosure record	

Graunded on		Remarks
cl.num.	Clause	
HC/L-31.1	The Director must maintain for each recognized certification authority an on-line and publicly accessible record.	
HC/L-31.2	The Director must publish in the certification authority disclosure record information regarding that certification authority relevant for the purposes of **HC/L** (in addition to the information required to be given in it under other provisions of **HC/L**).	
	32 Director to notify revocations, suspensions and non-renewals of recognition, etc.	
HC/L-32.1	The Director must give notice in the relevant certification authority disclosure record, immediately--- (a) when the Director makes a decision to revoke a recognition under **HC/L-23.4**; (b) when a revocation has taken effect under **HC/L-23.6** or 23.7; (c) when the Director makes a decision to suspend a recognition under **HC/L-24.2**; (d) when a suspension has taken effect under **HC/L24.4** or 24.5; (e) when the recognition of a suspended recognition is reinstated; (f) when the Director receives a notice of appeal under **HC/L-28.3**; or (g) on becoming aware that the Secretary has confirmed, varied or reversed the decision of the Director to revoke or suspend a recognition.	

Graunded on		Remarks
cl.num.	Clause	
HC/L-32.2	Where the revocation or suspension of a recognition has taken effect, the Director must, as soon as practicable, give notice of the revocation or suspension for at least 3 consecutive days in one English language daily newspaper and one Chinese language daily newspaper in circulation in Hong Kong.	
HC/L-32.3	If a recognized certification authority does not apply for renewal before the end of the period during which an application for renewal can be made under **HC/L-27.2**, the Director must, at least 21 days before the expiry of the period of validity of the recognition, give notice--- (a) for at least 3 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.	
	33 Director may issue code of practice	
HC/L-33.1	The Director may issue a code of practice specifying standards and procedures for carrying out the functions of recognized certification authorities.	
	Part 9 Postmaster General to be Recognized Certification Authority	

Graunded on		Remarks
cl.num.	Clause	
	34 The Postmaster General as recognized certification authority	
HC/L-34.1	The Postmaster General is a recognized certification authority for the purposes of **HC/L**.	
HC/L-34.2	Part 7 does not apply to the Postmaster General as a certification authority.	
	35 Postmaster General may perform functions and provide services of certification authority	
HC/L-35.1	For the purposes of **HC/L-**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 paragraph (a) and for complying with any provision of **HC/L** relating to a recognized certification authority.	
HC/L-35.2	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.	
HC/L-35.3	The fees determined and charged under **HC/L-35.2** 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.	

Graunded on		Remarks
cl.num.	Clause	
HC/L-35.4	The Postmaster General may give particulars of any fees determined under **HC/L-35.2** in such manner as the Postmaster General thinks fit.	
	Part 10 General Provisions as to Recognized Certification Authorities	
	36 Publication of issued and accepted certificates	
HC/L-36.1	Where a subscriber accepts a recognized certificate issued by a recognized certification authority, the certification authority must publish the certificate in a repository.	
HC/L-36.2	If the subscriber does not accept the recognized certificate, the recognized certification authority must not publish it.	
	37 Recognized certification authority to use trustworthy system	
HC/L-37.1	A recognized certification authority must use a trustworthy system in performing its services--- (a) to issue or withdraw a recognized certificate; or (b) to publish in a repository or give notice of the issue or withdrawal of a recognized certificate.	
	38 Presumption as to correctness of information	

Graunded on		Remarks
cl.num.	Clause	
HC/L-38.1	It shall be presumed, unless there is evidence to the contrary, that the information contained in a recognized certificate issued by a recognized certification authority (except information identified as subscriber's information which has not been verified by the recognized certification authority) is correct if the certificate was published in a repository.	
	39 Representations upon issuance of recognized certificate	
HC/L-39.1	By issuing a recognized certificate, a recognized 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 recognized certification authority has issued the certificate in accordance with any applicable CPS incorporated by reference in the certificate, or of which the relying person has notice.	
	40 Representations upon publication of recognized certificate	
HC/L-40.1	By publishing a recognized certificate, a recognized certification authority represents to any person who reasonably relies on the information contained in the certificate, that the recognized certification authority has issued the certificate to the subscriber concerned.	
	41 Reliance limit	
HC/L-41.1	A recognized certification authority may, in issuing a recognized certificate, specify a reliance limit in the certificate.	

Graunded on		Remarks
cl.num.	Clause	
HC/L-41.2	The recognized certification authority may specify different limits in different recognized certificates or in different types, classes or description of certificates.	
	42 Liability limits for recognized certification authorities	
HC/L-42.1	Unless a recognized certification authority waives the application of this subsection, the recognized certification authority is not liable for any loss caused by reliance on a false or forged digital signature of a subscriber supported by a recognized certificate issued by that certification authority, if the recognized certification authority has complied with the requirements of **HC/L** and HC/COP with respect to that certificate.	
HC/L-42.2	Unless a recognized certification authority waives the application of this subsection, the recognized certification authority is not liable in excess of the amount specified in the certificate as its reliance limit, for a loss caused by reliance on any information--- (a) that the recognized certification authority is required to confirm according to the CPS and HC/COP; and (b) which is misrepresented on that recognized certificate or in a repository, if the recognized certification authority has, in relation to that certificate, complied with the requirements of **HC/L** and HC/COP.	
HC/L-42.3	The limitation of liability under **HC/L-42.2** does not apply if the fact was misrepresented due to the negligence of the recognized certification authority or it was intentionally or recklessly misrepresented by the recognized certification authority.	

Graunded on		Remarks
cl.num.	Clause	
	43 Recognized certification authority to furnish report on compliance with Ordinance and code of practice	
HC/L-43.1	At least once in every 12 months, a recognized certification authority must furnish to the Director a report containing an assessment as to whether the recognized certification authority has complied with the provisions of **HC/L** applicable to a recognized certification authority and HC/COP during the report period.	
HC/L-43.2	A report under **HC/L-43.1** must be prepared, at the expense of the certification authority, by a person approved by the Director as being qualified to make such a report.	
HC/L-43.3	The Director must publish in the certification authority disclosure record for the certification authority the date of the report and the material information in the report.	
HC/L-43.4	In **HC/L-43.1** "report period", in relation to a report ("current report"), means the period beginning on--- (a) the date on which recognition is granted under **HC/L-**21 or **HC/L-**34 comes into operation; or (b) the day following the last day of the period for which the last report under that subsection was furnished, as the case may require, and ending on the last day of the period for which the current report is furnished.	
	44 Recognized certification authority to issue a CPS	

Graunded on		Remarks
cl.num.	Clause	
HC/L-44.1	A recognized certification authority must issue and maintain an up to date CPS and notify the Director of changes to the practices of the certification authority as set out in that statement.	
	45 Recognized certification authority to maintain repository	
HC/L-45.1	A recognized certification authority must maintain or cause to be maintained an on-line and publicly accessible repository.	
HC/L-45.2	The Director must publish in the Gazette a list of the repositories maintained under **HC/L-45.1**.	
	Part 11 Provisions as to Secrecy, Disclosure and Offences	
	46 Obligation of secrecy	
HC/L-46.1	Subject to **HC/L-46.2**, a person who has access to any record, book, register, correspondence, information, document or other material in the course of performing a function under or for the purposes of **HC/L** shall not disclose or permit or suffer to be disclosed such record, book, register, correspondence, information, document or other material to any other person.	

Graunded on		Remarks
cl.num.	Clause	
HC/L-46.2	**HC/L46.1** does not apply to disclosure--- (a) which is necessary for performing or assisting in the performance of a function under or for the purposes of **HC/L**; (b) for the purpose of any criminal proceedings in Hong Kong; (c) for the purpose of complying with a requirement made under a rule of law with a view to instituting a criminal proceeding in Hong Kong; or (d) under the direction or order of a magistrate or court.	
HC/L-46.3	A person who contravenes **HC/L-46.1** commits an offence and is liable to a fine at level 6 and in the case of an individual also to imprisonment for 6 months.	
	47 False information	
HC/L-47.1	A person who knowingly or recklessly makes, orally or in writing, signs or furnishes any declaration, return, certificate or other document or information required under **HC/L** which is untrue, inaccurate or misleading commits an offence and is liable in the case of an individual to a fine at level 6 and to imprisonment for 6 months and in any other case, to a fine at level 6.	
	48 Other offences	
HC/L-48.1	A person who makes a false claim that a person is a recognized certification authority commits an offence and is liable in the case of an individual to a fine at level 6 and to imprisonment for 6 months and in any other case, to a fine at level 6.	

Graunded on		Remarks
cl.num.	Clause	
	Part 12 Secretary's Power to Amend Schedules and Make Subsidiary Legislation and Immunity of Public Officers	
	49 Regulations	
HC/L-49.1	The Secretary may make regulations for all or any of the following--- (a) to prescribe the manner of applying to the Director for recognition or renewal of recognition as a recognized certification authority or for recognition or renewal of recognition of certificates and the manner of recognition; (b) to prescribe the fees payable in respect of applications for the recognition of certification authorities, the recognition of certificates or the renewal of such recognition; (c) to prescribe the form of CPSs; (d) to provide for the manner of appealing against a decision of the Director and the procedure for determining appeals; (e) to provide for such other matters as are necessary or expedient to give effect to the provisions of **HC/L**.	
	50 Secretary may amend Schedules	
HC/L-50.1	The Secretary may by order published in the Gazette amend Schedules 1 and 2.	
	51 Protection of public officers	

Graunded on		Remarks
cl.num.	Clause	
HC/L-51.1	No liability is incurred by the Government or a public officer by reason only of the fact that a recognition is granted, renewed, revoked, suspended or reinstated under Part 7.	
HC/L-51.2	Without prejudice to **HC/L-51.1**, no civil liability is incurred by a public officer in respect of anything done or omitted to be done by the public officer in good faith in the performance or purported performance of any function under a Part other than Part 7.	
HC/L-51.3	The protection conferred under **HC/L-51.2** does not in any way affect the liability, if any, of the Government for the act or omission of the public officer in the performance or purported performance of the relevant function.	
	SCHEDULE 1 Matters Excluded from Application of HC/L-5, 6, 7, 8 and 17 under HC/L-3	
	1) The creation, execution, variation, revocation, revival or rectification of a will, codicil or any other testamentary document.	
	2) The creation, execution, variation or revocation of a trust (other than resulting, implied or constructive trusts).	
	3) The creation, execution, variation or revocation of a power of attorney.	
	4) The making, execution or making and execution of any instrument which is required to be stamped or endorsed under the Stamp Duty Ordinance (Cap. 117) other than a contract note to which an agreement under section 5A of that Ordinance relates.	
	5) Government conditions of grant and Government leases.	

Graunded on		Remarks
cl.num.	Clause	
	6) Any deed, conveyance or other document or instrument in writing, judgments, and lis pendens referred to in the Land Registration Ordinance (Cap. 128) by which any parcels of ground tenements or premises in Hong Kong may be affected.	
	7) Any assignment, mortgage or legal charge within the meaning of the Conveyancing and Property Ordinance (Cap. 219) or any other contract relating to or effecting the disposition of immovable property or an interest in immovable property.	
	8) A document effecting a floating charge referred to in section 2A of the Land Registration Ordinance (Cap. 128).	
	9. Oaths and affidavits.	
	9) Oaths and affidavits.	
	10) Statutory declarations.	
	11) Judgments (in addition to those referred to in section 6) or orders of court.	
	12) A warrant issued by a court or a magistrate.	
	13) Negotiable instruments.	
	SCHEDULE 2 Proceedings in Relation to which HC/L-5, 6, 7 and 8 do not Apply under HC/L-13.1	
	roceedings before any of the following---	
	a) the Court of Final Appeal;	
	b) the Court of Appeal;	
	c) the Court of First Instance;	
	d) the District Court;	
	e) the Mental Health Review Tribunal established under the Mental Health Ordinance (Cap. 136);	
	(f) the Lands Tribunal;	
	f) the Lands Tribunal;	

Graunded on		Remarks
cl.num.	Clause	
	g) a coroner appointed under section 3 of the Coroners Ordinance (Cap. 504);	
	h) the Labour Tribunal;	
	i) the Obscene Articles Tribunal established under the Control of Obscene and Indecent Articles Ordinance (Cap. 390);	
	j) the Small Claims Tribunal;	
	k) a magistrate.	

Hong Kong China

[HC/COP] Code of Practice for Recognized Certification Authorities 2000.1.6 v1.0

Graunded on		Remarks
cl.num.	Clause	

1. INTRODUCTION

HC/COP-1.1 This Code of Practice for Recognized Certification Authorities (the Code of Practice) is issued by the Director of Information Technology Services (the Director) pursuant to section 33 of the Electronic Transactions Ordinance (Cap. 553) (the Ordinance).

HC/COP-1.2 This Code of Practice specifies standards and procedures to be adopted by recognized certification authorities (CAs) for carrying out their functions, and should be read in conjunction with the Ordinance.

HC/COP-1.3 The Director shall take into account the ability of a CA to comply with this Code of Practice in determining whether an applicant is suitable for recognition as a recognized CA under section 21 of the Ordinance.

Graunded on		Remarks
cl.num.	Clause	
HC/COP-1.4	The Director shall take into account whether a particular certificate or a type, class or description of certificates is issued or is to be issued by a recognized CA in accordance with this Code of Practice in granting recognition to that particular certificate or that type, class or description of certificates under section 22 of the Ordinance.	
HC/COP-1.5	The Director may take into account the failure of a recognized CA to comply with this Code of Practice in suspending, revoking, or not renewing a recognition granted to that CA or a recognition granted to a particular certificate or a type, class or description of certificates issued or is to be issued by that recognized CA under sections 22, 23, 24 or 27 of the Ordinance, as the case may be.	
HC/COP-1.6	If any part of this Code of Practice is not consistent with any provision in the Ordinance, the relevant provision in the Ordinance will prevail.	
HC/COP-1.7	The Director may from time to time amend this Code of Practice. The Director may consult the industry, including CAs recognized under sections 2l and 34 of the Ordinance, in respect of amendments to this Code of Practice. The primary channel of consultation with the industry bill be through an Advisory Committee on Code of Practice for Recognized Certification Authorities that will be set up and chaired by the Director.	
HC/COP-1.8	If any conflict arises in respect of any difference between the English version and the Chinese version of this Code of Practice, the English version shall prevail.	

2. DEFINITION OF TERMS

HC/COP-2.1	The terms used in this Code of Practice are defined as fo11ows.	

Graunded on		Remarks
cl.num.	Clause	
	1) “certificate” means a record which a) is issued by a CA 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 CA 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 sighed by a responsible officer of the CA issuing it: 2) “certification authority or CA” means a person who issues a certificate to a Person (Who may be another CA); 3) “certification authority certificate or CA certificate” means a certificate issued by or to a CA for the purpose of certifying certificates issued by that CA. This certificate may be issued by a CA for its own use or by one CA to another CA; 4) “certification authority disclosure record” in relation to a recognized CA, means the record maintained under section 31 of the Ordinance for that recognized CA; 5) “certificate policy” means a named set of rules that indicates the applicability of a certificate to a particular community and/or class of usage with common security requirements ; 6) “certification practice statement or CPS” means a statement issued by a recognized CA to specify the practices and standards that the recognized CA employs in issuing certificates; 7) “certificate revocation list” means a list maintained and published by a certification authority to specify the certificates that are issued by it and that have been revoked:	

Graunded on		Remarks
cl.num.	Clause	
	8) “digital signature” 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; 9) “electronic record” means a record generated in digital form by an information system, whicHC/COPn be a) transmitted within an information system or from one information system to another; and b) stored in an information system or other medium; 10) “fit and proper person” in determining whether a person is a fit and proper person, the Director shall, in addition to any other matter the Director considers relevant, have regard to the following: 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 with deception, flaudulently, corruptly or dishonestly; b) the fact that the person has been convicted of an offence against the Ordinance;	

Graunded on		Remarks
cl.num.	Clause	

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 5 years preceding the date of the application for recognition as a recognized CA or for the renewal of such a recognition; and

d) if the person is a body corporate, the fact that the person is in liquidation, is the subject of a winding-up 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 5 years preceding the date of the application for recognition as a recognized CA or for the renewal of such a recognition;

11) “information” includes data, text, images, sound codes, computer programmers, software and databases;

12) “information system” 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) ;

13) “Issue” in relation to a certificate, means the act of a CA of creating a certificate and notif5ring its contents to the person named or identified in that certificate as the person to whom it is issued;

Graunded on		Remarks
cl.num.	Clause	
	14) “key pair” 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 ; 15) “Postmaster General” means the Postmaster General within the meaning of the Post Office Ordinance (Cap.98); 16) “properly authorised Person” means a person who is authorised to act for the subscriber: 17) “private key” means the key of a key pair used to generate a digital signature ; 18) “public key” means the key of a key pair used to verify a digital signature ; 19) “recognized certificate” means a) a certificate recognized under section 22 of the Ordinance ; b) a certificate of a type, class or description of certificate recognized under section 22 of the Ordinance; or c) a certificate designated as a recognized certificate and issued by the Postmaster General; 20) “recognized certification authority or recognized CA” means a CA recognized under section 21 of the Ordinance or the Postmaster General; 21) “record” 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; 22) “reliance limit” means the monetary limit specified for reliance on a recognized certificate; 23) “repository” means an information system for storing and retrieving certificates and other information relevant to certificates;	

Graunded on		Remarks
cl.num.	Clause	
	24) “responsible officer” in relation to a CA, means a person occupying a position of responsibility in relation to the activities of the CA relevant to the Ordinance; 25) “sign and signature” 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; 26) “subscriber” means a person (who may be a CA) 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; 27) “trustworthy system” 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; 28) “verify a digital signature” in relation to a given digital signature, electronic record and public key, means to determine that - a) 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.	

	Graunded on	Remarks
cl.num.	Clause	

3. GENERAL RESPONSIBILITIES OF A RECOGNIZED CERTIFICATION AUTHORITY

HC/COP-3.1	A recognized CA shall comply with the conditions attached by the Director to the recognition granted under section 21 or renewed under section 27 of the Ordinance.	
HC/COP-3.2	A recognized CA may appoint agents or subcontractors to carry out some or all of its operations provided that: + the agents or subcontractors are equally capable of complying with this Code of Practice relevant to their operations, and + the recognized CA is and remains responsible for the activities of its agents or subcontractors in the performance or purported performance by them of the functions, powers, rights and duties of the recognized CA under the Ordinance.	
HC/COP-3.3	A recognized CA shall take all reasonable care in issuing certificates to its subscribers and shall take all reasonable care to persons who may rely upon these certificates.	
HC/COP-3.4	A recognized CA shall furnish the Director with a copy of its certification authority certificate (CA certificate) that it uses to sign its recognized certificates. The Director shall publish the CA certificate in the certification authority disclosure record maintained by the Director for that CA. The disclosure record serves as an additional means for making the CA certificate available to persons who need to verify the validity of the recognized certificates issued by that CA for at least 7 years after the concerned CA has terminated its service.	

Graunded on		Remarks
cl.num.	Clause	
HC/COP-3.5	Where the Code of Practice requires a recognized CA to record, retain or archive information and records, the recognized CA shall do so for a period of at least 7 years or such longer or shorter period as may be specified by the Director and in a manner that ensures the security, integrity and accessibility of the information and records for retrieval and inspection.	
HC/COP-3.6	A recognized CA shall comply with all applicable ordinances and regulations regarding the privacy of personal information.	
HC/COP-3.7	A recognized CA shall refrain from engaging in restrictive practices that impair economic efficiency or free trade.	
HC/COP-3.8	If a recognized CA issues to the public both recognized certificates and certificates not recognized by the Director, the recognized CA shall publicize the fact that it issues these two categories of certificates.	
	4. CPS	
HC/COP-4.1	A recognized CA shall publish for public knowledge and maintain up to date certification practice statement(s) (CPS) for the types, classes or descriptions of recognized certificates that it issues.	
HC/COP-4.2	A recognized CA shall state in its CPS(s) the liabilities, limitations on liability, rights and obligations of the recognized CA, its subscribers and persons who rely on the certificates issued by the recognized CA, and the significance of its reliance limit on its certificates. A recognized CA shall draw the attention of its subscribers and persons who may rely on its certificates to such liabilities, limitations, rights and obligations and the significance of its reliance limits by:	

Graunded on		Remarks
cl.num.	Clause	
	+ specifying separately as appropriate such information in any contract with its subscribers; and + making such information available, both in printed form and in electronic form via an on-line and publicly accessible means.	
HC/COP-4.3	A recognized CA shall provide up to date information in its CPS(s) concerning the recognition status of the types, classes or descriptions of recognized certificates that the recognized CA issues.	
HC/COP-4.4	A recognized CA shall draw the attention of its subscribers and persons who may rely upon those of its certificates which are not recognized certificates to the significance of using and relying upon those certificates.	
HC/COP-4.5	A recognized CA shall draw the attention of its subscribers to the e7(tent that their personal information will become public information when such information is incorporated in recognized certificates issued by the recognized CA to the subscribers and published in a repository of the recognized CA. Its CPS(s) shall state clearly the contents of the relevant recognized certificates.	
HC/COP-4.6	A recognized CA shall submit a copy of its CPS(s) to the Director upon publication of the CPS(s), and notify the Director in writing of any subsequent changes to the CPS(s) as soon as practicable. A recognized CA must also record all changes made to the CPS(s) together with the effective date of each change as soon as practicable.	
HC/COP-4.7	If a recognized CA issues a type, class, or description of recognized certificates that are specified in a certificate policy, then the certificate policy will be considered as part of the CPS.	

Graunded on		Remarks
cl.num.	Clause	
HC/COP-4.8	A recognized CA shall retain a copy of each version of the CPS(s) it has issued, together with the date the CPS(s) come into effect and the date the CPS(s) cease to have effect if applicable.	
HC/COP-4.9	A recognized CA shall, when issuing a type, class or description of recognized certificates, comply with the CPS for that type, class or description of recognized certificates.	
HC/COP-4.10	A recognized CA shall ensure that its CPS(s) are readily available in its on-line and publicly accessible repository. The repository shall be promptly updated when there are changes to the CPS(s).	
HC/COP-4.11	The standards and procedures regarding the contents of a CPS are set out in the Appendix.	
HC/COP-4.12	Before a recognized CA effects any intended material change to its CPS that corresponds to one or more types, classes or descriptions of recognized certificates that the recognized CA issues, the recognized CA shall consult the Director in respect of the effect of the intended material change on the recognition status of the types, classes or descriptions of recognized certificates concerned. The Director may decide whether the intended change will turn the types, classes or descriptions of certificates into new types, classes or descriptions of certificates. That recognized CA may then decide whether it wishes to apply to the Director for recognition of such new types, classes or descriptions of certificates. Examples of material change to a CPS include without limitation: a) changes in the identification process that weaken the reliability of the recognized certificates ; b) changes in the reliance limit of the recognized certificates; or c) changes in the key generation, storage, or usage procedures.	

	Graunded on	Remarks
cl.num.	Clause	
HC/COP-4.13	A recognized CA shall notify any incident that adversely and materially affects the validity of the whole or any part of its CPS to the Director, its subscribers and relying parties immediately. The CA shall take immediate action to address the incident. The resolutions in respect of the incident shall be reflected as soon as practicable in the CPS, published on-line on the recognized CA's repository and reported to the Director.	

5. TRUSTWORTHY SYSTEM

HC/COP-5.1 A recognized CA shall use a trustworthy system in performing its services, including the generation and management of its keys, the generation and management of subscribers' keys if appropriate, the issuance, renewal, suspension or revocation of recognized certificates, the giving of notice of the issuance, renewal, suspension or revocation of recognized certificates, the provision of a repository, and the publication of recognized certificates and other information in the repository.

General Interpretation

HC/COP-5.2 The term 'system' refers to the system itself, i.e. hardware and software, as well as those control and operational procedures moth manual and automated) that are designed to ensure that the system will perform its intended functions in a consistent, reliable and dependable manner.

HC/COP-5.3 For a system to be accepted as trustworthy, a recognized CA shall demonstrate that the mechanisms, procedures, and conditions under which the system operates are adequate for the performance of its intended functions.

HC/COP-5.4 There is no absolute measure of trustworthiness. It can only be assessed against a specific context.

	Graunded on	Remarks
cl.num.	Clause	

Guiding Principles

HC/COP-5.5	In accordance with the technology-neutral and minimalist regulatory approach adopted under the Ordinance, a recognized CA is free to determine the technical solutions to support its operations.
HC/COP-5.6	Where there is a high risk on specific aspects of a recognized CA's operation, for example, those in relation to security sensitive functions, the recognized CA is expected to adopt systems and procedures that meet such standards as are widely accepted or recognized world-wide. h addition, as a matter of good practice, a recognized CA shall perform structured assessments to ascertain the underlying risks of its operations, and implement appropriate counter-measures for managing, mitigating and monitoring such risks.

Specific Areas for Consideration

HC/COP-5.7	A recognized CA operating in a public key infrastructure (PKI) shall make use of any hardware, software and cryptographic components. These components shall be supported by appropriate security policies and procedures in order to ensure that the recognized CA operates in a secure environment.
HC/COP-5.8	The manner in which a recognized CA achieves its objective in maintaining a trustworthy system may vary, depending on the kind of services to be provided by the recognized CA, the state of technology and the business environment. A recognized CA shall adhere to the following generally accepted good practices.

Graunded on		Remarks
cl.num.	Clause	

Generally Accepted Industry Good Practices

HC/COP-5.9 A recognized CA shall develop, establish, maintain and update documented and approved policies, procedures and practices over its operational environment, including but not limited to the areas discussed in the following sub-paragraphs.

Generally accepted security principles

HC/COP-5.9.1 A recognized CA shall develop, establish, maintain, update and enforce adequate and proper security control over its operation in accordance with generally accepted security principles which must cover the following aspects as a minimum:

HC/COP-5.9.1a a) Asset classification and management

(i) recognized CA shall classify its assets properly and identify the owner(s) of its major assets. It shall maintain an up to date and complete inventory of its assets, and establish procedures to safeguard its assets.

(ii) A recognized CA shall treat the information that it maintains as one of its assets and classify such information in accordance with the degree of importance to the business operations, including data privacy considerations. Appropriate controls shall be established to secure such information from unauthorised access or damage.

HC/COP-5.9.1b b) Personnel security

(i) A recognized CA shall develop, establish, maintain and update effective controls over personnel security through mechanisms including without limitation :

Graunded on		Remarks
cl.num.	Clause	
	+ defining roles and responsibilities within formal job descriptions having regard to its security policies; + performing verification checks on its personnel in accordance with its security policies and procedures; and + incorporating confidentiality or similar clauses within formal terms and conditions of employment contracts.	
	(ii) A recognized CA shall provide appropriate and adequate training to its personnel, with the aim of maintaining their competency and ensuring effective implementation of and compliance with its security policies. Training may include without limitation: + appropriate technical training; + organisational policies and procedures; and + procedures to deal with security incidents and notify senior level of management of major security incidents.	
	(iii) A recognized CA shall establish appropriate controls to monitor the performance of its personnel including, for example: + regular performance reviews ; + formal disciplinary procedures; and + formal termination procedures.	
HC/COP-5.9.1c	c) Physical and environmental security (i) A recognized CA shall maintain effective physical and environmental security controls including without limitation :	
HC/COP-5.9.1.c.1-1	+ identifying and defining secure areas, and implementing security controls as appropriate for securing such areas;	
HC/COP-5.9.1.c.1-2	+ establishing formal procedures for access to such areas by staff of the recognized CA as well as by visitors;	

Graunded on		Remarks
cl.num.	Clause	
	+ establish appropriate security and access monitoring mechanisms, with specific attention to those areas where the recognized CA stores its security-sensitive equipment; + establishing appropriate controls to safeguard its equipment against environmental threats and hazards, such as fire, flood, power failures, etc, as well as against opportunity for unauthorised access ; + establishing general security controls, such as clear desk policy and general controls over equipment, information and other assets belonging to the recognized CA; and + ensuring that its environmental control mechanisms are maintained and reviewed on a regular basis. (ii) Where a recognized CA relies on services provided by third parties for the protection of physical and envirornmental security, such services shall be stated in formal service agreements established with these third party suppliers.	
HC/COP-5.9.1d	d) Management over systems access A recognized CA shall develop, establish, maintain and update effective controls and procedures over access to its information systems, including application systems, that are appropriate to the sensitivity and criticality of the systems being protected, including without limitation: + establishing proper business requirements for controlling access to systems; + establishing formal user responsibilities; + establishing formal procedures for the management of user identification profiles and monitoring of access to its systems, including for example:	

Graunded on		Remarks
cl.num.	Clause	
	- allocating, amending and revoking user access rights; and - the monitoring of access attempts through logging or similar means; + establishing proper controls over access to networks, operating systems, and application systems, such as firewalls, router filters, etc; + establishing proper procedures and controls over the monitoring of system access and usage; + establishing proper procedures and controls over mobile computing and teleworking ; + establishing proper procedures and controls against unauthorised or illegal usage of software; and + establishing proper procedures to deal with security incidents concerning access to networks, operating systems, and application systems.	

Operational management

HC/COP-5.9.2	A recognized CA shall maintain effective controls and procedures in respect of its day-to-day operations. Operational policies and standard operating procedures shall be formalised and documented, including without limitation the following aspects: + clear definition of duties and responsibilities of its operational personnel; + regular capacity monitoring procedures to monitor system performance and identify performance bottlenecks ; + proper procedures to protect its computing infrastructure against malicious programs, such as viruses, etc.;	

Graunded on		Remarks
cl.num.	Clause	
	+ proper procedures over systems and network management, including housekeeping tasks such as backup and archiving; + proper procedures over the handling, distribution, storage and disposal of electronic information and media; and + proper procedures for handling and resolving operational problems.	
	Development and maintenance of computer systems	
HC/COP-5.9.3	A recognized CA shall develop, establish, maintain and update effective controls and procedures over system development and maintenance activities, including for example: + establishing proper internal standards to ensure uniformity of development work, whether conducted by the staff of the recognized CA or by outside parties in the case of outsourcing; + procedures to ensure segregation of the production and development environments ; + procedures to ensure segregation of duties between operational and development personnel; + controls over access to data and systems held in its production and development environments ; + controls over change control process, including emergency changes to systems and/or data; and + procedures for the proper management in respect of the acquisition of equipment and services.	

	Graunded on	Remarks
cl.num.	Clause	
	Continuity of business operations	
HC/COP-5.9.4	A recognized CA shall develop, establish, maintain and update a business continuity plan that covers all critical aspects of its operations.	
HC/COP-5.9.5	The continuity plan shall be tested vig6rously on a regular basis, involving relevant key personnel detailed in the plan. Wherever possible, such tests shall be independently observed.	
HC/COP-5.9.6	The continuity plan shall cover contingencies such as recovery from a compromise or suspected compromise of the recognized CA's private key used to sign subscriber certificates, or recovery from major failure of the recognized CA's systems or any of the components of the recognized CA's systems.	
	Maintenance of appropriate event journals	
HC/COP-5.9.7	A recognized CA shall maintain adequate event journals, which includes the retention of documents related to the issuing and managing of recognized certificates by the recognized CA.	
HC/COP-5.9.8	A recognized CA shall archive such event journals. It shall also regularly review the event journals and take action against any exceptions identified.	
HC/COP-5.9.9	A recognized CA shall maintain journals relating to all major events including without limitation: + access to materials and equipment used for key generation; + in respect of keys and certificates, their generation, issuance, distribution, storage, backup, suspension, revocation, withdrawal, archival, destruction, and other related events;	

Graunded on		Remarks
cl.num.	Clause	
	+ security incidents, including key compromise; and	
	+ procurement, installation, implementation, decommission and retirement of cryptographic devices.	
	Compliance monitoring and assurance	
HC/COP-5.9.10	A recognized CA shall develop, establish, maintain and update appropriate controls to ensure compliance with applicable legal, regulatory and technical requirements including without limitation:	
	+ establishing an appropriate function to monitor all aspects of the operations of the recognized CA, and to ensure compliance with applicable requirements ;	
	+ ensuring that its compliance monitoring function meets the current industrial standards and practices; and	
	+ arranging for appropriate review to be conducted over its operational systems.	
	Good Practices Specific to Functions of a Recognized CA	
HC/COP-5.10	A recognized CA shall develop, establish, maintain and update formally documented and approved policies, procedures and practices over specific functions of a recognized CA, including without limitation the areas discussed in the following sub-paragraphs.	
	Management of certification practice statement	

Graunded on		Remarks
cl.num.	Clause	
HC/COP-5.10.1	A recognized CA shall disclose its business practices in its CPS(s) and maintain effective controls over its CPS(s) including without limitation: + forming a management committee with the authority and responsibility for determining and approving the contents of CPS(s), including any certificate policy or policies that are adopted by the recognized CA; + establishing effective procedures for the on-going review and updating of the CPS(s); and + making the CPS(s) available to its subscribers and persons who may rely on the recognized certificates issued by that recognized CA.	
	Legal and regulatory monitoring and compliance in respect of the functions of a recognized CA	
HC/COP-5.10.2	A recognized CA shall maintain effective procedures to monitor and ensure compliance with all legal and regulatory requirements, including relevant provisions in the Ordinance, the Regulations thereunder and this Code of Practice.	
	Key management	
HC/COP-5.10.3	A recognized CA shall maintain effective procedures and controls over the generation, storage, backup, recovery, distribution, use, destruction, and archiving of the recognized CA' s own keys including without limitation:	

Graunded on		Remarks
cl.num.	Clause	
	+ controls over the use of cryptographic modules for key generation, including the adoption of technical solutions with appropriate security standards; + operational controls over key generation including without limitation: - procedures to ensure the integrity of equipment used in the generation of the keys; - procedures to ensure the keys are generated by authorised personnel in a controlled manner; and - where subscriber key pairs are generated by the recognized CA, procedures shall be established to ensure that the private key is delivered to the subscriber in a secure manner without being tampered with; once the private key is delivered to the subscriber, the recognized CA shall not maintain a copy of the subscriber's private key without the written consent of the subscriber; + controls over key storage, backup and recovery including without limitation: - regular and vigorous testing of the recognized CA's recovery procedures ; - procedures to ensure safe custody of the recognized CA's private key, such as by placing it under dual access control. Appropriate measures shall be established to detect any unauthorised attempts to access the key; and - procedures to ensure that the backup of recognized CA's private key is securely performed under dual control, and that backup copies of the recognized CA's private key shall be kept in a secure manner; + controls over security for the key distribution process including without limitation :	

	Graunded on	Remarks
cl.num.	Clause	
	- procedures to ensure the integrity and authenticity of the public key of the recognized CA which the recognized CA provides to the Director for deposit in the CA disclosure record maintained by the Director for that recognized CA; and - procedures to ensure the integrity and authenticity of the recognized CA's own public key; + controls over the usage of the key, including the procedures for activating the key; for example: - more than one responsible officer is required to activate the private key of the recognized CA; and - the recognized CA's private key shall only be activated if proper authority for an intended purpose in a prescribed manner is obtained; + controls to ensure the safe destruction of key pairs and any related devices including procedures that ensure destruction of all copies of private keys (so that they cannot be recovered or reconstructed after destruction) and revocation of the corresponding public keys; and + controls for ensuring that archived keys meet the security and operational requirements stated in the CPS.	
	Management of key generating devices	
HC/COP-5.10.4	A recognized CA shall maintain effective procedures and controls over the procurement, receipt, installation, acceptance tests, commissioning, usage, repair, maintenance, and retirement of key generating devices. Control examples include:	

	Graunded on	Remarks
cl.num.	Clause	
	+ procedures for ensuring the integrity of the cryptographic module;	
	+ procedures for ensuring that the handling of key generating device is under proper supervision by authorised personnel to prevent the device from being tampered with; and control mechanism established to ensure that the cryptographic modules cannot be tampered with without being detected; and	
	+ procedures for ensuring that the strength of keys generated using the cryptographic modules is of the appropriate strength for the purpose of the keys for both the recognized CA and its subscribers.	
	Key management services provided by the recognized CA (where appropriate)	
HC/COP-5.10.5	A recognized CA shall maintain effective procedures and controls over key management services, if any, provided by the recognized CA to its subscribers, such as key generation, storage, backup, recovery, destruction and archival. Such procedures and controls shall be consistent with the principles set out in paragraphs 5.10.3 and 5.10.4 of this Code of Practice.	
	Lifecycle management of tokens (where appropriate)	
HC/COP-5.10.6	A recognized CA shall maintain effective procedures and controls over the preparation, activation, usage, distribution, and termination of any tokens, such as smart cards, used by the recognized CA.	

	Graunded on	Remarks
cl.num.	Clause	

Certificate management

HC/COP-5.10.7 A recognized CA shall maintain effective procedures and controls over the management of certificates, including but not limited to the following examples -

+ before issuing or renewing a recognized certificate, a recognized CA shall verify the identity of the person who applies to the recognized CA for the issuance or renewal of a recognized certificate in accordance with procedures stated in the relevant CPS; the recognized CA shall also verify the uniqueness of the person's distinguished name;

+ there shall be appropriate procedures to notify the subscribers the need to renew their certificates prior to the expiry of their certificates;

+ a recognized CA shall adopt an open and common interface for the issuance of its recognized certificates; the format of the certificate shall be stated in the relevant CPS;

+ there shall be proper policies and procedures to ensure that the performance of the repository of a recognized CA meets the service levels set out by the recognized CA in its CPS in respect of the repository; and

+ a recognized CA shall set out in its CPS the procedures for handling complaints from subscribers.

Management of the certificate revocation list

HC/COP-5.10.8 A recognized CA shall maintain effective procedures and controls over the management of its certificate revocation list. For example:

Graunded on		Remarks
cl.num.	Clause	
	+ a recognized CA shall update its certificate revocation list in accordance with the policies, procedures and arrangements stated in its CPS; and	
	+ there shall be procedures to ensure that only authorised personnel have access to the repository and the certificate revocation list for their maintenance.	
	Key Generation Using a Trustworthy System and Keeping of Records	
HC/COP-5.11	A recognized CA shall provide a trustworthy system to generate the recognized CA's own and the subscriber's key pair.	
HC/COP-5.12	A recognized CA shall separately keep its own private key and the activation data (e.g. PINs, passwords, etc.) in a secure manner.	
HC/COP-5.13	A recognized CA shall make and retain records in respect of:	
	+ activities relating to the issuance, renewal, suspension and revocation of recognized certificates (including the identification documents of any person applying for a recognized certificate from the recognized CA);	
	+ the certificate revocation list;	
	+ the documents relating to the generation of the recognized CA's own key Pair;	
	+ the documents relating to the generation of the subscribers' key pairs; and	
	+ the administration of the recognized CA's computer facilities.	
HC/COP-5.14	A recognized CA shall archive all recognized certificates issued by it and maintain mechanisms to access such certificates. .	

Graunded on		Remarks
cl.num.	Clause	

Digital Signatures

HC/COP-5.15 The technical implementation for the creation of a digital signature shall be such that:

a) the digital signature shall only be created under the direction of the person to whom the digital signature relates; and

b) no other person can reproduce the digital signature and thereby create a valid digital signature without the involvement or the knowledge of the person to whom the digital signature relates.

Matters Affecting a Trustworthy System

HC/COP-5.16 If there is an incident which materially and adversely affects a recognized CA's trustworthy system or the integrity of its recognized certificates, the recognized CA shall:

+ inform the Director immediately in respect of the incident;

+ use all reasonable endeavours to notify all persons who are or who will be affected by that incident; and

+ act in accordance with the procedures, if any, specified in the CPS governing such an incident.

HC/COP-5.17 A recognized CA shall ensure that all its personnel possess the necessary knowledge, technical qualifications and expertise to effectively carry out their duties.

Graunded on		Remarks
cl.num.	Clause	
HC/COP-5.18	A recognized CA shall ensure that all its responsible officers and those officers with trusted roles such as security officers, CA administrators, privileged system operators, registration personnel, and any other personnel that have access to key material, cryptographic modules, or activity event logs shall be fit and proper Persons.	

Security and Risk Management

HC/COP-5.19	A recognized CA shall adopt a security policy in accordance with generally accepted security principles.	
HC/COP-5.20	A recognized CA shall establish a comprehensive security incident reporting and handling procedure, and disaster recovery set-up and procedure for its operation.	
HC/COP-5.21	A recognized CA shall adequately identify and establish procedures to deal with the risks associated with its operation. It shall implement a risk management plan that will provide for the management of, including without limitation, the following incidents : + key compromise; + security breach of the system or network of the recognized CA; + unavailability of the infrastructure of the recognized CA; and + unauthorised generation of certificates and of certificate suspension and revocation information.	

6. CERTIFICATES AND RECOGNIZED CERTIFICATES

Graunded on		Remarks
cl.num.	Clause	
HC/COP-6.1	A recognized CA may issue certificates recognized by the Director under section 22 of the Ordinance or certificates not recognized by the Director. Where a recognized CA issues both recognized certificates and certificates not recognized by the Director, it shall use separate private keys to sign the two streams of certificates respectively.	
HC/COP-6.2	Recognized certificates shall contain the necessary information to facilitate subscribers and persons who rely on the certificates to locate the associated CPS during the conduct of electronic transactions.	

Issuance of Certificates

HC/COP-6.3	A recognized CA may issue a recognized certificate to a person only after the CA: a) has received a request for issuance of the recognized certificate from the person applying for such a certificate; and b) has complied with all of the practices and procedures set out in the CPS including procedures regarding identity verification of the person in respect of that type, class or description of recognized certificates.	
HC/COP-6.4	A recognized CA shall provide a reasonable opportunity for the subscriber to verify the contents of the recognized certificate before accepting the certificate.	
HC/COP-6.5	A recognized CA shall publish recognized certificates that it issues and that are accepted by its subscribers in the on-line and publicly accessible repositories maintained by it or maintained for it by one or more third parties.	

Graunded on		Remarks
cl.num.	Clause	
HC/COP-6.6	A recognized CA shall obtain the consent of the subscriber in respect of any personal information of the subscriber which the CA intends to include in the certificate that is to be issued to the Subscriber and to be listed in an on-line and publicly accessible repository.	
HC/COP-6.7	Once a recognized certificate has been issued by the recognized CA and accepted by the subscriber, the recognized CA shall notify the subscriber through all reasonable channels within a reasonable time of any fact known to the recognized CA that affects the validity or reliability of the recognized certificate.	
HC/COP-6.8	A recognized certificate shall state when its validity expires.	
HC/COP-6.9	By issuing a recognized certificate, a recognized CA represents to any person who reasonably relies on the recognized certificate or a digital signature verifiable by a public key listed in the recognized certificate that the recognized CA has issued the recognized certificate in accordance with its applicable CPS.	
HC/COP-6.10	All transactions related to the issuance of a recognized certificate including the date and time shall be recorded.	

Suspension and Revocation of Recognized Certificates

HC/COP-6.11	A recognized CA shall be able to revoke and may also be able to suspend recognized certificates in accordance with the following paragraphs.	
HC/COP-6.12	A recognized certificate shall contain or incorporate by reference necessary information to locate or identify the repository or repositories in which suspension or revocation notices of the recognized certificate will be published.	

Graunded on		Remarks
cl.num.	Clause	
HC/COP-6.13	Unless a recognized CA and its subscriber otherwise agree, the recognized CA that issues a recognized certificate to the subscriber shall suspend or revoke the certificate within a reasonable time after receiving a request from: a) the subscriber named or identified in the recognized certificate; or b) a properly authorised person.	
HC/COP-6.14	Within a reasonable time following suspension or revocation of a recognized certificate by a recognized CA, the recognized CA shall publish a signed notice of the suspension or revocation (e.g. certificate revocation list) in a repository maintained by it or by an outside organisation for the recognized CA.	
HC/COP-6.15	The exact time of the revocation or suspension by the recognized CA as well as the allocation of liability for transactions using die Certificate in the period between the receipt of the request for revocation or suspension and the time when the certificate is revoked or suspended shall be agreed between the recognized CA and the subscriber.	
HC/COP-6.16	A recognized CA may temporarily suspend a recognized certificate that it has issued if the recognized CA has reasonable grounds to believe that the recognized certificate is unreliable, regardless of whether the subscriber consents to the suspension; but the recognized CA shall complete its investigation regarding the reliability of the recognized certificate and decide within a reasonable time period whether to reinstate the certificate or to revoke the certificate.	
HC/COP-6.17	If the recognized CA considers that an immediate revocation of a recognized certificate issued by it is justified in the light of all the information available to it, the certificate shall be revoked, regardless of whether the subscriber has given consent to the revocation.	

Graunded on		Remarks
cl.num.	Clause	
HC/COP-6.18	In the case of suspension requested by the subscriber or a properly authorised person, the recognized CA shall check with the subscriber or that properly authorised person whether the recognized certificate to be suspended shall be revoked or reinstated after suspension. The relevant CPS shall state the action to be taken in the event that it is not possible for the recognized CA to contact the subscriber or the properly authorised person for his instruction of whether the suspended certificate shall be revoked or reinstated after suspension.	
HC/COP-6.19	Whenever a recognized CA suspends or revokes a recognized certificate which is issued by it, the recognized CA shall, within a reasonable time, notify the suspension or revocation of the recognized certificate and provide a record to the subscriber of the recognized certificate or the properly authorised person.	
HC/COP-6.20	A recognized CA shall provide hotline or other facilities for subscribers to report to the recognized CA incidents affecting their certificates or private keys, for example, keys having been lost or compromised.	
HC/COP-6.21	All transactions, including the date and time, in relation to suspension or revocation of certificates shall be recorded.	

Renewal of Recognized Certificates

HC/COP-6.22	A recognized certificate is subject to renewal upon expiry of its validity at the request of the subscriber and the discretion of the recognized CA.	
HC/COP-6.23	All transactions including the date and time in relation to the renewal of a recognized certificate shall be recorded.	

Graunded on		Remarks
cl.num.	Clause	

7. VERIFICATION OF SUBSCRIBER'S IDENTITY

HC/COP-7.1	A recognized CA shall specify in the relevant CPS that corresponds to a particular type, class or description of recognized certificates the procedure to verify the identity of a person who applies for such a recognized certificate from the recognized CA.
HC/COP-7.2	A recognized CA shall retain copies of the documentary evidence that identifies its subscribers.

8. RELIANCE LIMIT

HC/COP-8.1	In issuing a type, class or description of recognized certificates to subscribers, a recognized CA may specify in the relevant CPS that corresponds to that type, class or description of certificates a reliance limit on the certificates. A recognized CA shall specify in the relevant CPS the significance of the reliance limit on the use of the recognized certificates.
HC/COP-8.2	A recognized CA shall arrange suitable insurance or other forms of cover to ensure that it is capable of covering its liability for claims up to the reliance limit set for the recognized certificates that it issues.

9. REPOSITORIES

Graunded on		Remarks
cl.num.	Clause	
HC/COP-9.1	A recognized CA shall make available at least one on-line and publicly accessible repository for the publication of recognized certificates and related information. It shall ensure that its repository or repositories are implemented through trustworthy systems. The recognized CA shall state in its CPS(s) the service levels in respect of the operation of its repository or repositories.	
HC/COP-9.2	A recognized CA, in maintaining and managing a repository, shall not carry out any activity in a manner that creates an unreasonable risk to persons relying on the recognized certificates or other information contained in the repository.	
HC/COP-9.3	A repository of a recognized CA shall contain: + recognized certificates issued by the recognized CA; + suspension or revocation notices of its recognized certificates (including certificate revocation lists as appropriate); + the CA disclosure record for that recognized CA; and + other information as specified by the Director.	
HC/COP-9.4	A repository of a recognized CA shall not contain any information which the recognized CA knows to be inaccurate or unreliable.	
HC/COP-9.5	A recognized CA shall keep in its repository an archive of recognized certificates that have been suspended or revoked, or that have expired within at least the Previous Seven years.	

10. DISCLOSURE OF INFORMATION

HC/COP-10.1	A recognized CA shall publish in its repository or repositories:	

Graunded on		Remarks
cl.num.	Clause	
	a) its CA certificate that contains the public key corresponding to the private key used by the recognized CA to digitally sign recognized certificates it issues;	
	b) the suspension, revocation or non-renewal notice of its CA certificate or recognition granted by the Director; and	
	c) any other fact that materially and adversely affects either the reliability of a recognized certificate that the recognized CA has issued or its ability to perform its services relevant under the Ordinance.	
HC/COP-10.2	A recognized CA shall inform the Director of any changes in the appointment of responsible officers Or any Person Who performs functions equivalent to that of a responsible officer Within 3 working days from the date of appointment of that person.	
HC/COP-10.3	A recognized CA shall submit progress reports to the Director at 6-month intervals containing information with regard to:	
	a) the number of its subscribers classified by type, class or description of certificates ;	
	b) the number of certificates issued, suspended, revoked, expired and renewed by type, class or description of certificates;	
	c) its performance compared with its stated service levels;	
	d) new types, classes or descriptions of certificates issued;	
	e) changes in its organisational structure or systems;	
	f) actions taken by the recognized CA to address recommendation(s) made in the assessment report which is prepared and submitted to the Director under section 20(3)(b) or 43(1) of the Ordinance, and .	

Graunded on		Remarks
cl.num.	Clause	
	g) any changes related to the above items since the preceding progress report was submitted or since the application for recognition or renewal as a recognized CA.	
HC/COP-10.4	A recognized CA shall report to the Director immediately any material changes in the above information. The Director may also call for such report as well as other information relevant under the Ordinance at any time by giving a reasonable notice.	
HC/COP-10.5	A recognized CA shall report to the Director immediately when the recognized CA realises that there is an event which may or will lead to potential conflict of interest in respect of the operation of the recognized CA.	
HC/COP-10.6	A recognized CA shall report any incident that materially and adversely affects its operation to the Director immediately.	
	11. TERMINTION OF SERVICE	
HC/COP-11.1	A CA shall submit to the Director a termination plan when the CA applies for recognition as a recognized CA. A recognized CA shall submit to the Director a termination plan when it applies for renewal of its recognition.	
HC/COP-11.2	The termination plan shall specify the arrangements for the termination of the recognized CA's service, especially the arrangement for its records, including the certificates which it has issued and its CA certificate, to be archived for not less than 7 years.	

Graunded on		Remarks
cl.num.	Clause	
HC/COP-11.3	The termination plan shall cover both voluntary and involuntary termination of the recognized CA's service including the expiry or revocation of the recognition granted by the Director to the recognized CA. The termination plan shall also include measures to ensure that the interests of the subscribers are safeguarded upon termination of the recognized CA's service.	
HC/COP-11.4	Any CPS published by a recognized CA must refer to the termination plan of the CA.	
HC/COP-11.5	Before a recognized CA's service is terminated , the recognized CA shall	
	a) inform the Director of its intention to terminate service at least 90 days before the termination of its service;	
	b) inform all its subscribers of its intention at least 60 days before the termination of its service;	
	c) advertise such intention in one English language daily newspaper and one Chinese language daily newspaper in circulation in the Hong Kong Special Administrative Region for at least three consecutive days at least 60 days before the termination of its service;	
	d) if considered necessary by the Director, make arrangements to revoke all certificates which remain not revoked or expired, regardless of whether the subscribers have requested for the revocation, when it terminates its service; and	
	e) make appropriate arrangements to effect an orderly transfer of information contained in the recognized CA's repository, including details of certificates issued by the recognized CA and the recognized CA's public key(s).	

	Graunded on	Remarks
cl.num.	Clause	

12. ASSESSMENT OF COMPLIANCE WITH THE ORDINANCE AND THIS CODE OF PRACTICE

HC/COP-12.1 At least once in every 12 months, a recognized CA shall submit to the Director a report containing an assessment as to whether the recognized CA has complied with all the provisions of the Ordinance applicable to a recognized CA, the Regulations there under and this Code of Practice during the report period for which the report is prepared.

HC/COP-12.2 A recognized CA shall ensure that the report is prepared, at the expense of the recognized CA, by a qualified person approved by the Director for this purpose. In order to be considered as being qualified for preparing the assessment report, the person shall be:

+ independent of the recognized CA under assessment;

+ accredited by a recognized professional organisation or association; and

+ proficient in:

- the assessment of public key infrastructure and related technologies, such as digital signature and certificate, etc;

- applying information security tools and techniques;

- performing financial reviews ;

- performing security reviews; and

- performing third-party reviews.

Graunded on		Remarks
cl.num.	Clause	
HC/COP-12.3	The qualified person may be an individual possessing all of the above requirements, or a partnership or an organisation comprising individuals that collectively possess all of the above requirements. The individual signing the assessment report shall: + be a registered member of the recognized professional organisation or association, e.g. holding a valid practising certificate or attaining a similar status ; + have overall responsibility for ensuring that the person(s) performing the assessment possess sufficient knowledge of the subject matter, such as digital signature and certificate, public key infrastructure, financial matters, etc.; and + have overall responsibility for ensuring the quality of the assessment and adherence to any standards or practices adopted for the purpose of performing such assessments.	
HC/COP-12.4	For illustrative purposes, a Certified Public Accountant, i.e. a professional accountant with a practising certificate issued under the Professional Accountants Ordinance (Cap.50) who possesses or has available the technical expertise in information technology as set out in paragraph 12.2, or alternatively a professional in the field of information technology who possesses or has available the technical expertise as set out in paragraph 12.2, is considered acceptable for approval by the Director as the person to conduct the assessment. The Director is also prepared to assess the suitability of other persons as being qualified to conduct the assessment.	
HC/COP-12.5	The professional organisation or association referred to in paragraph 12.2 must have an established system to properly admit and regulate its members.	

Graunded on		Remarks
cl.num.	Clause	
	+ rules and regulations that govern membership admission requirements, such as in respect of training, competency testing, fitness for membership;	
	+ rules and regulations that govern professional and ethical standards and guidelines to members that govern the performance of their professional services, such as in respect of conflict of interest, undertaking and accepting instructions ;	
	+ mechanism for enforcing the professional and ethical standards and monitoring the conduct of members including without limitation formal disciplinary procedures, quality assurance measures such as peer reviews; and	
	+ mandatory continuing professional education requirement.	
HC/COP-12.6	A copy of the assessment report shall be submitted to the Director by the recognized CA within 4 weeks of the completion of the assessment, together with management's response to any recommendation raised by the assessor to the recognized CA as a result of the assessment. h the event that a recognized CA applies for renewal of recognition to the Director, the recognized CA shall submit a complete report of such assessment which is completed within three months prior to the date of the application for renewal by the recognized CA.	
HC/COP-12.7	Failure to meet the requirements as stated in the Ordinance, the Regulations thereunder and the Code of Practice may be a ground for suspending or revoking the recognition granted by the Director to a recognized CA or for rejecting a recognized CA's application for renewal of its recognition by the Director.	

13. ADOPTION OF STANDARDS AND TECHNOLOGY

Graunded on		Remarks
cl.num.	Clause	
HC/COP-13.1	A recognized CA shall continuously review and, where appropriate, improve and update its standards and technology in order to uphold the confidence that its subscribers place in it and to protect the interests of the subscribers.	
	14. INTER-OPERABILITY	
HC/COP-14.1	To reduce barriers for digital signatures supported by recognized certificates to be widely accepted, a recognized CA shall, wherever applicable, adopt an open and common interface to facilitate the verification by others of digital signatures supported by its recognized certificates.	
HC/COP-14.2	A recognized CA shall state in its CPS(s) the open and common interfaces that it supports and any inter-operability that it has established with other CAs.	
	15. CONSUMER PROTECTION	
HC/COP-15.1	The advertisement of services by a recognized CA shall be decent, honest and truthful. Comparative advertising shall be fair and not misleading. All claims shall be capable of independent substantiation.	