Consultation on the Draft Code of Practice for Recognised Certification Authorities

The Government is committed to promoting the development of electronic commerce in Hong Kong. In order to facilitate the conduct of safe and secure electronic transactions, the Government will establish a framework for the operation of certification authorities (CAs). While there will not be any compulsory licensing requirements on CAs operating in Hong Kong, the Government has proposed to establish a voluntary recognition scheme for CAs to protect consumer interest. The proposed framework has been set out in detail in an Electronic Transactions Bill, which has been introduced into the Legislative Council. Under the Bill, the Director of Information Technology Services (the Director) will be the authority for granting Government recognition to CAs.

2. CAs which intend to be recognised by the Director must achieve a trust standard acceptable to the Government in its operation and should adopt a common and open interface to facilitate inter-operability with other recognised CAs. CAs recognised under the voluntary scheme have to follow a Code of Practice to be issued by the Director, which spells out the general responsibilities of the CAs and the standards and procedures for their operation. Failure of recongised CAs to comply with the requirements of the Code of Practice may result in suspension or revocation of the recognition granted.

3. The Government now publishes the draft Code of Practice for public consultation and would welcome comments on the draft. Comments should be sent to the Information Technology Services Department on or before 15 November 1999 through the following means:

By Post	Information Technology Services Department 15/F, Wan Chai Tower 12 Harbour Road Wan Chai, Hong Kong
Fax	2802-4549
E-mail	enquiry@itsd.gcn.gov.hk

4. The Government reserves the right to make public all, or parts, of any comments made in response to this consultation exercise. Any material claimed to be commercially confidential would need to be clearly marked. The Government would take such marking into account in making its decision on whether or not to release the material.

Information Technology Services Department
25 October 1999

CODE OF PRACTICE

FOR RECOGNISED

CERTIFICATION AUTHORITIES

(Draft)

25 October 1999

The Government of the Hong Kong Special Administrative Region

CONTENTS

1. INTRODUCTION

1.1 Section 39 of the Electronic Transactions Ordinance (hereinafter referred to as "the Ordinance") provides that the Director of Information Technology Services (hereinafter referred to as "the Director") may issue a Code of Practice specifying standards and procedures for recognised certification authorities (CAs) to carry out their functions.

1.2 This Code of Practice is issued by the Director under Section 39 of the Ordinance. It specifies the standards and procedures for carrying out the functions of recognised CAs. It should be read in conjunction with the Ordinance.

1.3 The Director shall take into account the capability of a CA in complying with this Code of Practice in granting recognition to the CA under Section 20 of the Ordinance.

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 recognised 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 21 of the Ordinance.

1.5 The Director may take into account the failure of a recognised 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 CA under section 21, 22, 23 or 26 of the Ordinance, as the case may be.

2. DEFINITION OF TERMS

The terms used in this Code of Practice are defined as follows -

certificate	means a record which – is issued by a CA for the purpose of supporting a digital signature which purports to confirm the identify or other significant characteristics of the person who holds a particular key pair; – identifies the CA issuing it; – names or identifies the person to whom it is issued; – contains the public key of the person to whom it is issued; and – is signed by a responsible officer of the CA issuing it
certification authority	means a person who issues a certificate to a person (who may be another CA)
certification authority disclosure record	in relation to a recognized CA, means an on-line and publicly accessible record maintained by the Director in respect of that CA, which contains information relevant for the purposes of the Ordinance, regarding that CA
certification practice statement	means a statement issued by a CA to specify the practices and standards that the CA employs in issuing certificates
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 – whether the transformation was generated using the private key that corresponds to the signer's public key; and – whether the initial electronic record has been altered since the transformation was generated

fit and proper person	in relation to a CA, means a person -- who does not have a conviction in Hong Kong or elsewhere for an offence for which it was necessary to find that the person has acted fraudulently, corruptly or dishonestly; -- the person has not been convicted of an offence against the Ordinance; -- if the person is an individual, the person is not an undischarged bankrupt or has not 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 of the CA to become a recognised CA; and -- if the person is a body corporate, the person is not in liquidation, not a subject of a winding-up order, nor there is a receiver appointed in relation to it, and it has not 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 of the CA to become a recognised CA.
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
private key	means the key of a key pair used to generate a digital signature
public key	means the key of a key pair used to verify a digital signature
recognised certification authority	means a CA recognised by the Director under section 20 of the Ordinance or the CA referred to in section 28 of the Ordinance
recognised certificate	means a certificate recognised by the Director under section 21 of the Ordinance or a certificate of a type, class or description of certificates recognised by the Director under section 21 of the Ordinance or a certificate issued by the recognised CA referred to in section 28 of the Ordinance and is designated as a recognised certificate by the recognised CA.

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
recognised repository	means a repository recognised by the Director under section 40 of the Ordinance
reliance limit	means the monetary limit specified for reliance on a recognised certificate
repository	means an information system for storing and retrieving certificates and other information relevant to certificates
subscriber	means a person (who may be a CA) who – is named or identified in a certificate as the person to whom the certificate is issued; – has accepted that certificate; and – holds a private key which corresponds to a public key listed in that certificate
trustworthy manner	in relation to the logging, retention or archiving of information and records, means the procedures and arrangements which shall ensure the accuracy, security, confidentiality, integrity and accessibility for retrieval and inspection of the information and records, and which are fit for the intended purpose in respect of the information and records to be logged, retained or archived
trustworthy system	means computer hardware, software and procedures which – are reasonably secure from intrusion and misuse, ensuring that information is accessible only by authorised persons in authorised ways; – are at a reasonable level in respect of availability and reliability, ensuring a correct mode of operations for a reasonable period of time; – are consistent and accurate in maintaining data and records on the system; – are reasonably suitable for performing their intended functions; and – adhere to generally accepted security principles.

3. RESPONSIBILITIES OF A RECOGNISED CERTIFICATION AUTHORITY (CA)

3.1 General Responsibilities

3.1.1 A recognised CA shall comply with all the conditions of recognition including the conditions attached by the Director to the recognition granted under section 20 of the Ordinance.

3.1.2 A recognised CA shall comply with the legislation currently in force in the Hong Kong Special Administrative Region.

3.1.3 A recognised CA shall not conduct its business in a manner that gives rise to an unreasonable risk to its subscribers or persons who may rely on the recognised certificates issued by the recognised CA.

3.1.4 Whenever in this Code of Practice a recognised CA is required to log, retain or archive information and records, the CA shall log, retain or archive the information and records concerned for a period of not less than 7 years except where otherwise specified.

3.2 Certification Practice Statement

3.2.1 A recognised CA must publish for public knowledge and maintain an up to date certification practice statement for each type, class or description of recognised certificates that it issues. It shall submit a copy of the certification practice statement to the Director when it is published and notify the Director of any subsequent changes to the statement as soon as practicable.

3.2.2 A recognised CA shall keep in a trustworthy manner a copy of each version of the certification practice statement, together with the date the statement comes into effect and the date the statement ceases to have effect. The recognised CA shall also log all changes to the statement together with the effective date of each change.

3.2.3 A recognised CA shall, in the issuance of a type, class or description of recognised certificates, comply with the published certification practice statement for that type, class or description of certificates.

3.2.4 A recognised CA shall highlight in the certification practice statement to its subscribers any limitation of its liability, and in particular, it shall draw the subscribers' attention to the implication of the reliance limits set on its recognised certificates.

3.2.5 The subscriber identity verification procedure for the issuance and renewal of a type, class or description of recognised certificates shall be specified in the certification practice statement for that type, class or description of recognised certificates.

3.3 Trustworthiness

3.3.1 A recognised CA must use a trustworthy system in performing its services, including the issuance, renewal, suspension or revocation of a recognised certificate, the giving of notice of the issuance, renewal, suspension or revocation of a recognised certificate, or the publication of a recognised certificate in a recognised repository.

3.3.2 A recognised CA shall make and keep in a trustworthy manner the records relating to -

a. activities in the issuance, renewal, suspension and revocation of recognised certificates (including the identification documents of any person applying for a recognised certificate from the recognised CA);

b. the documents relating to the generation of the recognised CA' s own and the subscribers' key pairs; and

c. the administration of the recognised CA' s computer facilities.

A recognised CA shall archive all recognised certificates issued by it and maintain mechanisms to access such certificates. A recognised CA shall retain all records required to be kept under this paragraph and all logs of the creation of the archive of certificates in a trustworthy manner so as to ensure that they are accurate, complete, legible and accessible if they are to be reproduced to the Director or to a person who audits the operation of the recognised CA.

3.3.3 If there is an incident which materially and adversely affects a recognised CA's trustworthy system or its recognised certificates issued, the recognised CA shall

a. use reasonable efforts to notify any person who is known to be or foreseeably will be affected by that incident;

b. act in accordance with the procedures governing such an incident if such procedures have been specified in the certification practice statement; and

c. inform the Director immediately in respect of the incident.

3.3.4 A recognised CA shall provide a trustworthy system for the generation of the CA' s own and the subscriber' s key pairs.

3.3.5 A recognised CA must separately keep its own private key and activation data (e.g. PINs, passwords, etc.) in a trustworthy manner.

3.3.6 A recognised CA shall ensure that all its responsible officers and those who have direct responsibilities for the day-to-day operations, security and performance of the activities of the recognised CA and those who have duties directly relating to the issuance, renewal, suspension or revocation of recognised certificates (including the identification of any person applying for a recognised certificate from the

recognised CA), creation of private keys or administration of the recognised CA' s computer facilities are

a. fit and proper persons; and

b. persons who possess the relevant knowledge, technical qualifications and expertise to effectively carry out their duties.

3.4 Certificates

3.4.1 A recognised CA may issue certificates recognised by the Director under Section 21 of the Ordinance or certificates not recognised by the Director.

3.4.2 The recognised CA must associate a distinct certification practice statement with each type, class or description of recognised certificates issued.

3.4.3 The recognised CA must draw the attention of subscribers and parties who rely on the certificates issued by it to the effect of using and relying on the certificates which it issues but which are not recognised by the Director.

3.5 Reliance Limit

3.5.1 In issuing a recognised certificate to a subscriber, a recognised CA may specify a reliance limit in the recognised certificate in accordance with the provisions of the Ordinance.

3.5.2 A recognised CA shall specify in the certification practice statement for a type, class or description of recognised certificates the implications of the reliance limit on that type, class or description of recognised certificates.

3.5.3 A recognised CA shall make suitable arrangements to ensure that it is capable of covering its liability for claims up to the reliance limits set for the recognised certificates that it issues.

3.6 Identification

3.6.1 A recognised CA shall specify in the certification practice statement for a type, class or description of recognised certificates the procedure to verify the identity of a person who applies for that type, class or description of recognised certificates from the recognised CA. The procedure shall specify the steps of identity verification to be performed by the recognised CA for that type, class or description of recognised certificates, which shall be fit for the intended purpose and conform to relevant legislation and regulations.

3.6.2 The recognised CA shall keep an archive of the documentary proof that substantiates the identification of the applicant.

3.7 Disclosure of Information

3.7.1 A recognised CA shall publish in the recognised repositories maintained by it

a. its certificate that contains the public key corresponding to the private key used by that recognised CA to digitally sign another certificate;

b. notice of the suspension, revocation or non-renewal 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 recognised certificate that the recognised CA has issued or its ability to perform its CA services.

3.7.2 A recognised 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.

3.7.3 A recognised CA shall submit progress reports to the Director, at a frequency to be specified by the Director, containing information on -

a. the number of its subscribers 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. performance against its stated service levels;

d. new type, class or description of certificates issued;

e. changes in its organisational structure; and

f. changes in the above items since the preceding progress report was submitted or since the application for recognition.

The recognised CA also has the obligation to disclose to the Director any changes in the above information immediately when such changes warrant the attention of the Director. The Director may also call for such report at any time by giving a reasonable notice as and when necessary.

3.7.4 A recognised CA shall report any extraordinary incident which affects its trustworthiness to the Director immediately.

3.7.5 A recognised CA shall report to the Director immediately any event which may or will lead to potential conflict of interest in respect of the operation of the CA.

3.8 Issuance of Certificates

3.8.1 A recognised CA may issue a recognised certificate to an applicant only after the CA -

a. has received a request for issuance of the recognised certificate from the applicant; and

b. has complied with all of the practices and procedures set out in the certification practice statement associated with that type, class or description of recognised certificates including the procedures regarding identification of the applicant for that type, class or description of recognised certificates.

3.8.2 A recognised CA shall maintain a repository of issued recognised certificates. It shall publish recognised certificates which it issues and which are accepted by the subscribers in the recognised repositories maintained by it.

3.8.3 A recognised certificate must contain or incorporate by reference such information as is sufficient to locate or identify one or more recognised repositories in which notification of the suspension or revocation of the recognised certificate will be listed if the recognised certificate is suspended or revoked.

3.8.4 A recognised CA shall provide a reasonable opportunity for the subscriber to verify the contents of the recognised certificate before accepting the certificate.

3.8.5 Once a recognised certificate has been issued by the recognised CA and accepted by the subscriber, the recognised CA shall notify the subscriber within a reasonable time of any fact known to the recognised CA that significantly affects the validity or reliability of the recognised certificate.

3.8.6 A recognised certificate must state the date on which its validity expires.

3.8.7 All transactions, including the date and time, in relation to the issuance of a recognised certificate must be logged and kept in a trustworthy manner.

3.8.8 By issuing a recognised certificate, a recognised CA represents to any person who reasonably relies on the recognised certificate or a digital signature verifiable by the public key listed in the recognised certificate that the recognised CA has issued the recognised certificate in accordance with any applicable certification practice statement incorporated by reference in the recognised certificate, or of which the relying person has notice.

3.9 Suspension and Revocation of Certificates

3.9.1 A recognised CA shall support revocation of recognised certificate. It may also support suspension of recognised certificate.

3.9.2 Unless a recognised CA and the subscriber agree otherwise, the recognised CA that issues a recognised certificate to the subscriber shall suspend (if suspension is supported) or revoke the certificate within a reasonable time after receiving a request from

a. the subscriber named in the recognised certificate; or

b. a person who is authorised to act for that subscriber.

3.9.3 Within a reasonable time upon suspension (if suspension is supported) or revocation of a recognised certificate by a recognised CA, the recognised CA shall publish a signed notice of the suspension or revocation in a recognised repository specified in the certificate.

3.9.4 A recognised CA may suspend (if suspension is supported) a recognised certificate that it has issued if the recognised CA has reasonable grounds to believe that the recognised certificate is unreliable, regardless of whether the subscriber consents to the suspension; but the recognised CA shall complete its investigation into the reliability of the recognised certificate and decide within a reasonable time whether to reinstate the certificate or to revoke the certificate.

3.9.5 If the recognised CA considers that the immediate revocation of a recognised certificate which was issued by it is justified in the light of all the evidence available to it, the certificate shall be so revoked, regardless of whether the subscriber consents to the revocation.

3.9.6 In the case of suspension (if suspension is supported) requested by the subscriber or a person who is authorised to act for him, the recognised CA shall check with the subscriber or the authorised person as to whether the certificate suspended should be revoked or reinstated after suspension.

3.9.7 All transactions, including the date and time, in relation to suspension or revocation of recognised certificates must be logged and kept in a trustworthy manner.

3.9.8 Whenever a CA suspends (if suspension is supported) or revokes a recognised certificate issued by it, the CA shall within a reasonable time notify the subscriber of the recognised certificate or the person who is authorised to act for him of the suspension or revocation of the recognised certificate.

3.10 Renewal of recognised certificate

3.10.1 A recognised certificate is subject to renewal upon expiry of its validity.

3.10.2 All transactions, including the date and time, in relation to the renewal of a recognised certificate must be logged and kept in a trustworthy manner.

3.11 Inter-operability

3.11.1 A recognised CA shall, wherever applicable, adopt an open and common interface to facilitate the verification by others of digital signatures supported by the recognised certificates which it issues.

3.12 Adoption of Standards and Technology

3.12.1 A recognised CA shall continuously review and update its standards and technology in respect of the trustworthiness of its system and procedures in order to protect the interest of its subscribers.

3.12.2 The technical implementation for the creation of a digital signature shall ensure that

a. the creation of the digital signature is under the direction of the person to whom the digital signature correlates; 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 correlates.

3.13 Auditing

3.13.1 The operation of a recognised CA shall be audited in accordance with the provisions in the Ordinance and this Code of Practice. The audit shall also cover the compliance of the operation of the CA with the certification practice statements which the CA has published for its recognised certificates.

3.13.2 All audits must be conducted by a qualified and independent auditor approved by the Director for this purpose.

3.13.3 The result of every audit shall be submitted to the Director within 4 weeks of the completion of the audit. In the event that a recognised CA applies for renewal of recognition, the CA shall submit to the Director the result of such an audit which is completed within the three months preceding the date of the application of renewal.

3.13.4 Failure to pass an audit may be a ground for revocation of the recognition granted to the recognised CA or for rejecting the application of the CA for renewal of the recognition granted.

3.13.5 A recognised CA shall establish an internal audit function within its organisation for

ensuring compliance of its operation with the provisions in the Ordinance, this Code of Practice and the certification practice statements published by the CA for its recognised certificates.

3.14 Termination Plan

3.14.1 A CA shall submit for approval by the Director a termination plan when the CA applies for recognition or for renewal of the recognition granted to the CA.

3.14.2 The termination plan shall specify the arrangements for the termination of the CA's services, especially the arrangement for its records including the certificates which it has issued to be archived in a trustworthy manner for not less than seven years and the measures to ensure that the interest of its subscribers are properly taken care of.

3.14.3 If a recognised CA intends to terminate its services, it shall

a. inform the Director of its intention no later than 90 days before the termination of its services as a CA;
b. inform all its subscribers of its intention no later than 60 days before the termination of its services as a CA;
c. advertise such intention in one English language daily newspaper and one Chinese language daily newspaper for at least three consecutive days no later than 60 days before the termination of its services as a CA; and
d. if considered necessary by the Director, make arrangements to revoke all certificates which remain not revoked or expired when it terminates its services as a CA.

3.15 Security and Risk Management

3.15.1 A recognised CA shall adopt a security policy which shall be developed in accordance with generally accepted security principles and standards and which shall cover at least the aspects of physical control, procedural control, personnel control, technical security control and security audit procedures in respect of its operation.

3.15.2 A recognised CA shall have a comprehensive security incident reporting and handling procedure, and disaster recovery setup and procedure for its operation.

3.15.3 A recognised CA shall adequately identify and establish procedures to deal with the risks associated with its operation. The CA shall implement a risk management plan that must provide for the management of, but shall not be limited to, the following types of incident -

a. key compromise;
b. intrusion of the system or network of the CA;
c. unavailability of the infrastructure of the CA; and
d. fraudulent generation of certificates and of certificate suspension and revocation

information.

4. REPOSITORIES

4.1 Repositories

4.1.1 A recognised CA shall maintain one or more repositories which is recognised by the Director.

4.2 Trustworthiness

4.2.1 A recognised CA shall maintain a recognised repository through a trustworthy system.

4.2.2 A recognised CA, in maintaining a recognised repository, shall not carry out any activity in a manner that creates an unreasonable risk to persons who may rely on the recognised certificates or other information contained in the recognised repository.

4.2.3 A recognised CA shall have a comprehensive security incident reporting and handling procedure, and disaster recovery setup and procedure for maintaining a recognised repository.

4.3 Operation

4.3.1 A recognised repository of a recognised CA shall include a database containing:

a. recognised certificates published in the repository;
b. notices of suspension and revocation of recognised certificates published by the recognised CA ;
c. CA disclosure records for the recognised CA;
d. all orders or advisory statements published by the Director in respect of the recognition of the CA; and
e. other information as specified by the Director

4.3.2 A recognised repository shall contain no information which is untrue, inaccurate, or not reasonably reliable.

4.3.3 A recognised CA shall keep in a recognised repository an archive of recognised certificates that have been suspended or revoked, or that have expired within at least the past seven years.

5. AMENDMENT TO THE CODE OF PRACTICE

5.1 The Director may from time to time amend this Code of Practice and will notify the CAs recognised under sections 20 and 28 of the Ordinance of the amendment made accordingly.