LC Paper No. CB(1)559/99-00(07)

Revised Draft Code of Practice
for Recognised Certification Authorities

Introduction

This paper presents to Members of the Bills Committee on the Electronic Transactions Bill (ETB) the revised draft code of practice for recognised certification authorities.

Background

2. According to Clause 27D of the ETB, the Director of Information Technology Services (the Director) may issue a code of practice (COP) specifying standards and procedures for carrying out the functions of recognised certification authorities (CA). The Information Technology Services Department (ITSD) published the first draft of the COP for public consultation between 25 October 1999 and 15 November 1999, and received written comments from the following 8 organisations and 1 individual –

- British Computer Society (Hong Kong Section);
- Cable & Wireless HKT;
- Consumer Council;
- Hong Kong Bar Association;
- Hong Kong Computer Society;
- Hong Kong Institution of Engineers (IT Division);
- Office of the Privacy Commissioner on Personal Data;
- Tradelink Electronic Commerce Limited; and
- An individual.

The ITSD has also discussed and exchanged views on the draft COP with other bodies, e.g. the Hong Kong Society of Accountants, etc.

3. We briefed Members on the major comments received in the consultation exercise and our initial response at the eighth meeting of the Bills Committee held on 29 November 1999.

The Revised Draft COP

4. Taking into account comments received in the consultation exercise and Members' views, ITSD has revised the draft COP and has substantially expanded its contents. The revised draft COP is at the Annex. Major changes are highlighted below –

- a provision is added to the effect that if any part of the code is not consistent with any provision under the Electronic Transactions Ordinance (when enacted), the relevant provision under the Ordinance will prevail (section 1.6 of the revised draft);

- a provision is added to the effect that the Director will consult the industry in respect of future amendments to the COP (section 1.7 of the revised draft);

- detailed guidelines for the implementation of a trustworthy system are provided, including a set of generally accepted security principles and a set of good practices specific to certification authority functions which recognised certification authorities should adhere to; and

- the following 3 annexes are added -

    - Annex 1 : Recognition of Certification Authorities and Certificates, which outlines the recognition criteria and the process for obtaining recognition for certification authorities and certificates;

- Annex 2 : Guidelines on the Contents of Certification Practice Statements of recognised certification authorities; and

- Annex 3 : Compliance Assessment on Certification Authorities, which sets out the minimum qualifications of the persons for preparing compliance assessment reports and the scope of the report.

Further Consultation

5. The ITSD has forwarded the revised draft COP to those organisations which have expressed specific views on the first draft and have sought discussion with them on the revised draft. All the organisations which have been contacted support the approach which ITSD has taken in preparing the revised draft COP. They also consider the principles and framework set out in the revised draft appropriate. They will provide further comments on points of detail, if any, shortly but these comments should not affect the approach of the COP or the principles and framework set out in it. ITSD will finalise the COP in the light of these comments.

Information Technology and Broadcasting Bureau

December 1999

ITS

Information Technology
Services Department

資訊科技署

Code of Practice for Recognised Certification Authorities

(Second Draft)

The Government of the Hong Kong Special Administrative Region

TABLE OF CONTENTS

INTRODUCTION

1.1 This Code of Practice is issued by the Director of Information Technology Services (hereinafter referred to as "the Director") in accordance with the Electronic Transactions Ordinance (hereinafter referred to as "the Ordinance").

1.2 This Code of Practice provides guidelines on standards and procedures to be adopted by recognised Certification Authorities (CAs) in carrying out their functions, and should be read in conjunction with the Ordinance.

1.3 The Director will 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 will 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.

1.6 If any part of this Code of Practice is not consistent with any provision under the Ordinance, the relevant provision under the Ordinance will prevail.

1.7 The Director may from time to time amend this Code of Practice. The Director will consult the industry, including CAs recognised under sections 20 and 28 of the Ordinance, in respect of future amendments to the Code of Practice.

2 DEFINITION OF TERMS

2.1 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 identity 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 certificate means a certificate issued to a CA for the purpose of certifying certificates issued by the CA (which may be a certificate issued by a certification authority to itself, i.e. a ‘self-signed’ certificate);

certification authority disclosure record in relation to a recognised CA, means an on-line and publicly accessible record maintained by the Director for the CA;

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;

certification practice statement means a statement issued by a CA to specify the practices and standards that the CA employs in issuing certificates;

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;

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 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 determining whether a person is a fit and proper person, in addition to any other relevant matter, there must be regard to

- 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;
- the fact that the person has been convicted of an offence against the Ordinance;
- 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 preceding 5 years; and
- 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 preceding 5 years;

information system means a system which

- processes information;
- records information;
- can be used to cause information to be recorded, stored or otherwise processed in other information systems (wherever situated); and
- can be used to retrieve information, whether the information is recorded or stored in the system itself or in other information systems (wherever situated);

issue in relation to a certificate, means the act of a CA 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;

key pair in an asymmetric cryptosystems, 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 a key of a key pair used to verify a digital signature;

recognised certificate means

- a certificate recognised under section 21 of the Ordinance;
- a certificate of a type, class or description of certificate recognised under section 21 of the Ordinance; or
- a certificate designated as a recognised certificate issued by the CA referred to in section 28 of the Ordinance;

recognised certification authority
means a CA recognised under section 20 of the Ordinance or the CA referred to in section 28 of the Ordinance;

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;

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 system
means computer hardware, software and procedures that

- are reasonably secure from intrusion and misuse;
- are at a reasonable level in respect of availability, reliability and ensuring a correct mode of operations for a reasonable period of time;
- are reasonably suitable for performing their intended functions; and
- adhere to generally accepted security principles.

3 GENERAL RESPONSIBILITIES OF A RECOGNISED CERTIFICATION AUTHORITY

3.1 A recognised CA has to comply with the conditions attached by the Director to the recognition granted under section 20 of the Ordinance. Annex 1 outlines the conditions and the process for the recognition of CAs and certificates.

3.2 A recognised 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 CA is ultimately responsible for the activities of its agents or subcontractors relevant under the Ordinance.

3.3 A recognised CA must not issue certificates in a manner that gives rise to an unreasonable risk to its subscribers or persons who rely on the recognised certificates issued by the recognised CA.

3.4 A recognised CA has to furnish the Director with a copy of its certification authority certificate (CA certificate) which the Director will publish 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 certificates issued by that recognised CA up to 7 years after the concerned recognised CA has terminated its service.

3.5 Where the Code of Practice requires a recognised CA to log, retain or archive information and records, the CA has to log, retain or archive the information and records concerned for a period of not less than 7 years except where otherwise specified.

3.6 A recognised CA has to comply with all applicable regulations regarding the privacy of personal information.

4 CERTIFICATION PRACTICE STATEMENT

4.1 A recognised CA has to publish for public knowledge and maintain one or more up to date certification practice statements (CPS) for the types, classes or descriptions of recognised certificates that it issues. It may publish separate CPSs to be associated with different types, classes or descriptions of recognised certificates or a combined CPS to be associated with all recognised certificates that it issues.

4.2 A recognised CA has to define in its CPS(s) the liabilities, limitations of liability and obligations of the CA, its subscribers and persons who rely on the certificates issued by the CA, and the implications of reliance limits set by the CA on its certificates. A recognised CA has to draw the attention of its subscribers and persons who rely on its certificates to such liabilities, limitations, obligations and implications by:

- specifying separately as appropriate such information in any contract or agreement with its subscribers; and

- making such information available as appropriate, both in printed form and in electronic form via an on-line and publicly accessible means.

4.3 A recognised CA has to provide up to date information in its CPS(s) concerning the recognition status of the types, classes or descriptions of recognised certificates that the CA issues.

4.4 A recognised CA has to draw the attention of its subscribers and persons who rely on its recognised certificates to the effect of using and relying on the certificates which it issues but which are not recognised by the Director.

4.5 A recognised CA has to draw the attention of its subscribers to the fact that their personal information will become public information when such information is incorporated in recognised certificates issued by the CA to the subscribers and published in a repository of the CA. The relevant CPS(s) have to define precisely the contents of the recognised certificates associated with the CPS(s).

4.6 A recognised CA has to submit a copy of the CPS(s) to the Director upon publication of the CPS(s), and notify the Director of any subsequent changes as soon as practicable. The recognised CA must also log all changes made to the CPS(s) together with the effective date of each change.

4.7 If a recognised CA issues a type, class, or description of recognised certificates that are specified in a certificate policy, then reference can be made from the CPS associated with the certificates to such certificate policy. The certificate policy concerned will then be considered as part of the CPS.

4.8 A recognised CA has to 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. Retention of copies of the CPS(s) has to be made having due regard to the aspects of security, integrity and accessibility for subsequent retrieval and inspection.

4.9 A recognised CA has to, when issuing a type, class or description of recognised certificates, comply with the CPS for that type, class or description of recognised certificates.

4.10 A recognised CA has to ensure that its CPS(s) are readily available in its on-line and publicly accessible repository. The repository has to be promptly updated when there are changes to the CPS(s).

4.11 Further guidelines in respect of the contents of a CPS are set out in Annex 2.

5 TRUSTWORTHY SYSTEM

5.1 A recognised CA has to 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 (if supported) or revocation of recognised certificates, the giving of notice of the issuance, renewal, suspension or revocation of recognised certificates, the provision of a repository, and the publication of recognised certificates and other information in the repository.

General Interpretation

5.2 The term ‘system’ refers not just to computer hardware and software, but also to the supporting procedures, both manual and automated, security arrangements and standards with which the system operates.

5.3 A trustworthy system is a system that offers sufficient assurances that it will perform the intended functions in a consistent, reliable, and dependable manner. For a system to be accepted as trustworthy, a recognised CA has to be able to demonstrate that the mechanisms, procedures, and conditions under which the system operates are adequate for the performance of its intended functions.

5.4 There is no absolute measure of trustworthiness; it can only be assessed against a specific context. “Reasonableness” will be assessed as fit and appropriate to the end in view, having regard to all the relevant circumstances.

Guiding Principles

5.5 In adherence to the technology-neutral and minimalist regulatory approach adopted under the Ordinance, a recognised CA is free to determine the specific technical solutions that it wishes to implement in order to support its operations.

5.6 However, where the risk of specific aspects of a recognised CA’s operation is high, such as in relation to security sensitive functions, the recognised CA is expected to adopt systems and procedures that adhere to standards widely accepted or recognised worldwide. In addition, as a matter of good practice, a recognised CA has to perform structured assessments of the underlying risks of its operations, and implement appropriate counter-measures for managing, mitigating and monitoring such risks.

Specific Areas for Consideration

5.7 A recognised CA operating in a public key infrastructure (PKI) will make use of a complex integration of hardware, software and cryptographic components. These components need to be supported by appropriate security policies and procedures in order to provide assurance that the CA operates in a secure environment.

5.8 The manner in which a recognised CA achieves the objective of maintaining a trustworthy system may vary, depending on the specific services to be provided by the CA, the state of available technology and the business circumstances. However, it is expected that a recognised CA should adhere to the following generally accepted good practices.

Generally Accepted Industry Good Practices

5.9 A recognised CA has to establish documented and approved policies, procedures and practices over its operational environment, including but not limited to the areas discussed in the following paragraphs.

Generally accepted security principles

5.9.1 A recognised CA has to maintain 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:

- Asset classification and management;
- Personnel security;
- Physical and environmental security; and
- Management over systems access.

Assets classification and management

5.9.2 A recognised CA has to divide its assets into logical and proper classifications and identify the owner(s) of its major assets. The CA has to maintain an up to date and complete inventory of its assets, and establish procedures to safeguard its assets.

5.9.3 The CA has to treat the information that it maintains as one of its assets and classify such information in accordance with its importance to the business operations. Appropriate controls has to be established to secure such information against unauthorised assess or damage.

Personnel security

5.9.4 A recognised CA has to maintain effective control over personnel security through mechanisms, including but not limited to:

- 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 agreements within formal terms and conditions of employment contracts.

5.9.5 A recognised CA has to provide appropriate training to its personnel, with the aim of maintaining their competency and ensure effective implementation of, and compliance with, its security policies. Areas to be addressed in such training may include, but not limited to:

- appropriate technical training;
- organisational policies and procedures; and
- procedures on incident response and escalation.

5.9.6 A recognised CA has to establish appropriate controls to monitor the performance of its personnel, including for example:

- regular performance reviews;
- formal disciplinary procedures; and
- formal termination procedures.

Physical and environmental security

5.9.7 A recognised CA has to maintain effective physical and environmental security controls, including but not limited to:

- the identification and definition of secure areas, and the implementation of security controls as appropriate for securing such areas;
- establishing formal procedures for access to such areas by staff of the CA as well as by visitors;
- establishing appropriate security and access monitoring mechanisms, with specific attention to those areas where the 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 CA; and
- ensuring that its environmental control mechanisms are maintained and reviewed on a regular basis.

5.9.8 Where a recognised CA relies on services provided by third parties, such as through outsourcing agreements, the requirements for the protection of physical and environmental security have to be specified, as appropriate, in formal service level agreements established with these third parties suppliers.

5.9.9 Where a recognised CA relies on outside building management services to protect its physical and environmental surroundings, appropriate formal service level agreements have to be established with the service providers.

Management over systems access

5.9.10 A recognised CA has to establish and maintain 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 but not limited to :

- establishing business requirements for controlling access to systems;
- establishing formal definition of user responsibilities;
- defining formal procedures for the management of user-ids and monitoring of access to its systems, including for example:
  - the allocation, variation and revocation of user access rights; and
  - the monitoring of access attempts through logging or similar means;
- establishing controls over access to networks, operating systems, and application systems, such as firewalls, router filters, etc;
- establishing procedures and controls over the monitoring of system access and usage;
- establishing procedures and controls over mobile computing and teleworking;
- establishing procedures and controls against unauthorised or illegal usage of software; and
- establishing procedures to deal with security incidents concerning access to networks, operating systems, and application systems.

Operational management

5.9.11 A recognised CA has to maintain effective controls and procedures in respect of its day to day operations. Operational policies and standard operating procedures have to be formalised and documented, covering but not limited to 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.;

- 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

- formal problem escalation procedures for raising critical issues for follow up and resolution.

Development and maintenance of computer systems

5.9.12 A recognised CA has to maintain 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 CA’s personnel 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.

Continuity of business operations

5.9.13 A recognised CA has to develop and maintain a business continuity plan that covers all critical aspects of its operations.

5.9.14 The continuity plan has to be tested on a regular basis, involving relevant key personnel detailed in the plan. Wherever possible, such tests have to be independently observed.

5.9.15 The continuity plan has to cover contingencies such as recovery from a compromise or suspected compromise of the CA’s private key used to sign subscriber certificates, or recovery from major failure of the CA's systems or any of its components.

Maintenance of appropriate event journals

5.9.16 A recognised CA has to maintain adequate event journals, which includes the retention of documentation for activities related to the issuance and management of the recognised certificates of the CA.

5.9.17 A recognised CA has to archive such event journals in a manner that ensures the security, integrity and accessibility of the journals for retrieval and inspection. The CA has to also periodically review the event journals and take action against any exceptions identified.

5.9.18 A recognised CA has to maintain journals relating to all major events, including but not limited to:

- 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;
- security sensitive incidents, including key compromise; and
- procurement, installation, implementation, decommission and retirement of cryptographic devices;

Compliance monitoring and assurance

5.9.19 A recognised CA has to establish appropriate controls to ensure compliance with applicable legal, regulatory and technical requirements, including but not limited to:

- establishing an appropriate function to monitor all aspects of the CA operations, and to ensure compliance with applicable requirements;

- ensuring that its compliance monitoring function are up to date having regard to current issues in the industry; and

- arranging for appropriate review to be conducted over its operational systems.

Good Practices Specific to CA Functions

5.10 A recognised CA has to establish documented and approved policies, procedures and practices over specific CA functions, including but not limited to the areas discussed in the following paragraphs.

Management of certification practice statement

5.10.1 A recognised CA has to disclose its business practices in its CPS and maintain effective controls over its CPS, including but not limited to:

- the setting up of a management group with the authority and responsibility for specifying and approving CPS, including any certificate policy or policies that are adopted by the CA;

- establishing effective procedures for the on-going review and update of the CPS; and

- making the CPS available to its subscribers and persons who rely on the recognised certificates that the CA issues.

Legal and regulatory monitoring and compliance in respect of the CA functions

5.10.2 A recognised CA has to maintain effective mechanism to monitor and ensure compliance with legal and regulatory requirements, including relevant provisions under the Ordinance and this Code of Practice.

Key management

5.10.3 A recognised CA has to maintain effective procedures and practices covering the generation, storage, backup, recovery, distribution, use, destruction, and archiving of the CA’s own keys, covering areas of but not limited to:

- controls over the secure use of cryptographic modules for key generation, including the adoption of technical solutions with appropriate security standards.

- operational controls over key generation, including but not limited to:

  - procedures to ensure the integrity of equipment used in the generation of the keys;

  - procedures to ensure that keys are generated by authorised personnel in a controlled manner; and

  - where subscriber key pairs are generated by the CA, procedures have to 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 CA will not maintain a copy of the subscriber's private key without the consent of the subscriber.

- controls over key storage, backup and recovery, including but not limited to:

  - regular testing of the CA's recovery procedures;

  - procedures to ensure safe custody of the CA's private key, such as by placing it under dual access control. Appropriate measures have to be established to detect any unauthorised attempts to access the key; and

  - procedures to ensure the backup of CA's private keys is performed securely under dual control, and backup copies of the CA's private key have to be kept in a secure manner.

- controls over security for the key distribution process (e.g. mechanism to ensure integrity and authenticity of the key and to detect modifications to the key), including but not limited to:

  - procedures to ensure the integrity and authenticity of the public key of the recognised CA which the CA provides to the Director for deposit in the CA disclosure record maintained by the Director for that CA; and

  - procedures to ensure the integrity and authenticity of the CA's own public key.

- controls over the usage of the key, including the procedures for activating the key; examples include but not limited to:

  - the activation of the CA's private key has to be under multi-party control and may be performed using two factors authentication. (e.g. a physical token plus a password); and

  - the CA's private key can only be activated under proper authority for an intended purpose in a prescribed manner.

- controls over the secure destruction of key pairs, including any related devices, encompassing procedures to ensure the complete destruction of all copies of a private key (so that it cannot be recovered or reconstructed after destruction) and the revocation of the public key corresponding to the destroyed private key.

- controls for ensuring that archived keys meet the security and operational requirements set out in the CPS.

Management of key generating devices

5.10.4 A recognised CA has to maintain effective policies, procedures and controls over the procurement, receipt, installation, acceptance tests, commissioning, usage, repair, maintenance, and retirement of key generating devices. Control examples include but not limited to:

- procedures for ensuring the integrity of the cryptographic module that could result in leakage of information;

- procedures for ensuring that the handling of key generating device is under proper control 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 are of the appropriate strength for the purpose of the keys for both the CA and its subscribers.

Key management services provided by the CA (where appropriate)

5.10.5 A recognised CA has to maintain effective policies, procedures and controls over key management services, if any, that the CA provides to its subscribers, such as key generation, storage, backup, recovery, destruction and archival. Such policies, procedures and controls have to be consistent with the principles set out in sections 5.10.3 and 5.10.4 of this Code of Practice.

Lifecycle management of tokens (where appropriate)

5.10.6 A recognised CA has to maintain effective policies, procedures and controls over the manufacture, preparation, activation, usage, distribution, and termination of any tokens, such as smart cards, used by the CA.

Certificate management

5.10.7 A recognised CA has to maintain effective policies, procedures and controls over the management of certificates, including but not limited to the following examples -

- a recognised CA has to verify the identity of the person who applies to the CA for the issuance or renewal of a recognised certificate in accordance with procedures set out in the associated CPS; the CA also has to verify the uniqueness of the person's distinguished name;

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

- a recognised CA has to adopt an open and common interface for the issuance of its recognised certificates; the format of the certificate has to be specified in the associated CPS;

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

- a recognised CA has to set out in its CPS the procedures for handling complaints from subscribers.

Management of the certificate revocation list

5.10.8 A recognised CA has to maintain effective policies, procedures and controls over the management of its certificate revocation list; examples include but not limited to:

- a recognised CA has to update its certificate revocation list in accordance with the arrangements set out in its CPS; and

- there has to 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

5.10.9 A recognised CA must provide a trustworthy system for the generation of the CA's own and the subscriber's key pair.

5.10.10 A recognised CA must separately keep its own private key and the activation data (e.g. PINs, passwords, etc.) in a manner that ensures the security, integrity and accessibility of the private key and the activation data for retrieval and inspection.

5.10.11 A recognised CA has to make and keep records in respect of:

- activities relating to 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);

- the certificate revocation list;

- the documents relating to the generation of the recognised CA's own key pair;

- the documents relating to the generation of the subscribers' key pairs; and

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

Such records have to be kept in a manner which ensures the security, integrity and accessibility of the records for retrieval and inspection.

5.10.12 A recognised CA has to archive all recognised certificates issued by it and maintain mechanisms to access such certificates. A recognised CA has to retain all records required to be kept under this paragraph in a manner which ensures that the records are accurate, complete, legible and accessible if they are to be made available to the Director or to a person who assesses the operation of the recognised CA.

Digital Signatures

5.10.13 The technical implementation for the creation of a digital signature has to ensure that:

(a) the creation of the digital signature must be 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.

Matters Affecting a Trustworthy System

5.10.14 If there is an incident which materially and adversely affects a recognised CA's trustworthy system or the recognised certificates it has issued, the recognised CA has to -

- inform the Director immediately in respect of the incident;

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

- act in accordance with the procedures governing such an incident if such procedures have been specified in the CPS.

5.10.15 Recognised CAs must ensure that all its personnel possess the necessary knowledge, technical qualifications and expertise to effectively carry out their duties.

5.10.16 Recognised CAs must 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 must be fit and proper persons.

Security and Risk Management

5.10.17 A recognised CA has to adopt a security policy that has to be developed in accordance with generally accepted security principles.

5.10.18 A recognised CA has to establish a comprehensive security incident reporting and handling procedure, and disaster recovery setup and procedure for its operation.

5.10.19 A recognised CA has to adequately identify and establish procedures to deal with the risks associated with its operation. The CA has to implement a risk management plan that must provide for the management of, but not limited to, the following incidents:

- key compromise;

- intrusion of the system or network of the CA;

- unavailability of the infrastructure of the CA; and

- unauthorised generation of certificates and of certificate suspension and revocation information.

6 CERTIFICATES AND RECOGNISED CERTIFICATES

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

6.2 Recognised certificates should 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

6.3 A recognised CA may issue a recognised certificate to a person only after the CA:

(a) has received a request for issuance of the recognised 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 recognised certificates.

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

6.5 A recognised CA has to publish recognised 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 outside organisations.

6.6 A recognised CA has to 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.

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

6.8 A recognised certificate must state when its validity expires.

6.9 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 CPS incorporated by reference in the recognised certificate, or of which the relying person has notice.

6.10 All transactions related to the issuance of a recognised certificate, including the date and time, must be logged and kept in a manner that ensures the security, integrity and accessibility of the information for retrieval and inspection.

Suspension and Revocation of Certificates

6.11 A recognised CA has to support revocation of recognised certificates. It may also support suspension of recognised certificates.

6.12 A recognised certificate has to contain or incorporate by reference such information as is sufficient to locate or identify the repository or repositories in which notification of the suspension (if supported) or revocation of the recognised certificate will be listed if the recognised certificate is suspended (if supported) or revoked.

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

(a) the subscriber named or identified in the recognised certificate; or

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

6.14 Within a reasonable time upon suspension (if suspension is supported) or revocation of a recognised certificate by a recognised CA, the recognised CA has to publish a signed notice of the suspension or revocation (e.g. certificate revocation list) in a repository maintained by it or maintained for it by an outside organisation.

6.15 The time for the recognised CA to revoke or suspend (if suspension is supported) a recognised certificate as well as the allocation of liability for transactions using the certificate in between the time when revocation or suspension is requested by the subscriber or a person who is authorised to act for the subscriber, and the time when the certificate is actually revoked or suspended must be a matter of service arrangement to be agreed between the CA and the subscriber. Such a service arrangement has to be specified in the associated CPS.

6.16 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 has to 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.

6.17 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 will be so revoked, regardless of whether the subscriber consents to the revocation.

6.18 In the case of suspension (if suspension is supported) requested by the subscriber or a person who is authorised to act for the subscriber, the recognised CA has to check with the subscriber or the authorised person whether the recognised certificate that was suspended should be revoked or should be reinstated after suspension. The associated CPS has to define the expected time period within which this check has to be made and the action to be taken in the event that it is not possible for the recognised CA to contact the subscriber or the authorised person.

6.19 Whenever a CA suspends (if suspension is supported) or revokes a recognised certificate which is issued by it, the CA has, within a reasonable time, to 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.

6.20 A recognised CA must provide hotline or other facilities for subscribers to report to the CA incidents affecting their certificates or private keys, such as keys having been lost or compromised.

6.21 All transactions, including the date and time, in relation to suspension or revocation of certificates must be logged and kept in a manner that ensures the security, integrity and accessibility of the information for retrieval and inspection.

Renewal of Recognised Certificates

6.22 A recognised certificate is subject to renewal upon expiry of its validity at the request of the subscriber and the discretion of the recognised CA.

6.23 All transactions, including the date and time, in relation to the renewal of a recognised certificate must be logged and kept in a manner that ensures the security, integrity and accessibility of the information for retrieval and inspection.

7 VERIFICATION OF SUBSCRIBER'S IDENTITY

7.1 A recognised CA has to specify in the CPS associated with a type, class or description of recognised certificates the procedure to verify the identity of a person who applies for such a recognised certificate from the recognised CA.

7.2 A recognised CA has to retain copies of the documentary evidence that substantiates the identification of its subscribers.

8 RELIANCE LIMIT

8.1 In issuing a type, class or description of recognised certificates to subscribers, a recognised CA may specify in the CPS associated with that type, class or description of certificates a reliance limit on the certificates. The CA has to specify in the CPS the implication of the reliance limit on the use of the certificates.

8.2 A recognised CA has to make suitable arrangements to ensure that it is capable of covering its liability for claims up to the reliance limit set for the recognised certificate that it issues.

9 REPOSITORIES

9.1 A recognised CA has to make available at least one on-line and publicly accessible repository for the publication of recognised certificates and related information. The recognised CA has to ensure that its repository is implemented through a trustworthy system. The recognised CA has to define in its CPS the service levels in respect of the operation of its repository.

9.2 A recognised CA, in maintaining and managing a repository, may not carry out any activity in a manner that creates an unreasonable risk to persons relying on the recognised certificates or other information contained in the repository.

9.3 A repository of a recognised CA has to contain :

- recognised certificates issued by the CA;
- notices of suspension (if supported) or revocation of recognised certificates (including certificate revocation lists as appropriate);
- the CA disclosure record for the recognised CA; and
- other information as specified by the Director.

9.4 A repository of a recognised CA must not contain any information which is known to the CA to be inaccurate or not reasonably reliable.

9.5 A recognised CA has to keep in its repository an archive of recognised certificates that have been suspended or revoked, or that have expired within at least the past seven years.

10 DISCLOSURE OF INFORMATION

10.1 A recognised CA has to publish in its repository, :

(a) its CA certificate that contains the public key corresponding to the private key used by that recognised CA to digitally sign recognised certificates it issues;

(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.

10.2 A recognised CA has to 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.

10.3 A recognised CA has to submit progress reports to the Director at 6-month interval 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 or systems; and

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

10.4 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 as well as other information relevant under the Ordinance at any time by giving a reasonable notice as and when necessary.

10.5 A recognised CA has to 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.

10.6 A recognised CA has to report any incident that materially and adversely affects its operation to the Director immediately.

11 TERMINATION OF SERVICE

11.1 A CA has to submit to the Director a termination plan when the CA applies for recognition as a recognised CA. A recognised CA also has to submit to the Director a termination plan when it applies for renewal of its recognition.

11.2 The termination plan has to specify the arrangements for the termination of the CA's service, especially the arrangement for its records, including the certificates which it has issued and its CA certificate, to be archived for no less than 7 years in a manner that ensures the security, integrity and accessibility of the records for retrieval and inspection.

11.3 The termination plan has to cover both voluntary and involuntary termination of the CA's service, as well as the expiry or revocation of the recognition granted by the Director to the CA. The termination plan also has to include measures to ensure that the interests of the subscribers are properly taken care of upon termination of the CA's service.

11.4 The termination plan forms part of the CPS of the CA.

11.5 If a recognised CA intends to terminate operation, it has to

(a) inform the Director of its intention at least 90 days before the termination of its services as a CA;

(b) inform all its subscribers of its intention at least 60 days before the termination of its services as a CA;

(c) advertise such intention in one local English language daily newspaper and one local Chinese language daily newspaper for at least three consecutive days at least 60 days before the termination of its services as a CA;

(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 services as a CA; and

(e) make appropriate arrangements to effect an orderly transfer of information contained in the CA’s repository, including details of certificates issued by the CA and the CA’s public key.

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

12.1 At least once in every 12 months, a recognised CA must furnish to the Director a report containing an assessment as to whether the recognised CA has complied with the provisions of the Ordinance applicable to a recognised CA and this Code of Practice during the period for which the report is prepared.

12.2 All assessments must be conducted by a qualified person approved by the Director for this purpose. Certified Public Accountants, i.e. professional accountants with practising certificates issued under the Professional Accountants Ordinance (Cap. 50), who are supported by technical expertise in IT as necessary, are considered acceptable for approval by the Director as the person to prepare the report. The Director may also consider the suitability of other persons as being qualified to prepare the report.

12.3 A copy of the assessment report has to be submitted to the Director by the recognised CA within 4 weeks of the completion of the assessment. In the event that a recognised CA applies for renewal of recognition to the Director, the CA has to submit the report of such an assessment which is completed within the three months preceding the date of the application of renewal by the CA.

12.4 Failure to pass an assessment may be a ground for suspension or revocation of the recognition granted by the Director to the CA or for rejecting the application by the CA for renewal of its recognition.

12.5 Further information in respect of the assessment is set out in Annex 3.

13 ADOPTION OF STANDARDS AND TECHNOLOGY

13.1 A recognised CA has to continuously review and, where appropriate, update its standards and technology in order to uphold the trust that its subscribers place in it and to protect the interest of the subscribers.

14 INTER-OPERABILITY

14.1 To reduce barriers for digital signatures supported by recognised certificates to be widely accepted, a recognised CA has to, wherever applicable, adopt an open and common interface to facilitate the verification by others of digital signatures supported by the recognised certificates which are issued by the CA.

14.2 A recognised CA has to specify 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

15.1 Advertising of services by recognised CAs has to be honest and truthful. Comparative advertising has to be fair and not misleading. All claims have to be capable of substantiation.

Recognition of Certification Authorities and Certificates

Introduction

1 A CA seeking recognition from the Director must be capable of complying with the provisions under the Ordinance applicable to recognised CAs and with the Code of Practice. A recognised CA may also apply to the Director for recognition of its certificates.

2 This annex outlines the conditions and the process for the recognition of CAs and certificates.

Recognition of Certification Authorities

3 In accordance with subsection 20(3) of the Ordinance, the Director has to consider, in addition to any other matters, the following matters in determining whether the applicant is suitable for recognition:

(a) the financial status of the applicant for operating as a recognised CA in accordance with relevant provisions of the Ordinance and the Code of Practice;

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

(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 which contains an assessment as to whether the applicant is capable of complying with relevant provisions of the Ordinance and the Code of Practice;

(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 on its certificates.

Financial Considerations

4 Items (a), (b) and (f) in subsection 20(3) of the Ordinance all relate to the financial aspects of the applicant's operation.

5 The applicant has to provide evidence that:

(a) it has assessed the business and financial risks that will arise or have arisen from its operation as a CA; that it has made arrangements to adequately cover itself for its operation and against potential claims which it will be subjected to. Where the CA issues certificates with specific reliance limits, the insurance coverage should be sufficient to enable the CA to meet its potential liability under the circumstances; and

(b) the CA intends to be, and will remain, a going concern. Such intention can be demonstrated in various ways, including but not limited to:

– maintaining adequate financing to support its operation;

– having installed, or contracted to install systems and equipment which are required to support the operation of the CA and have made the necessary financial arrangements; and

– having the availability of appropriate level of personnel, both in terms of quality (skill set) and quantity (number of staff), to support the CA's operation and have made the necessary financial arrangements.

Systems, Procedures, Security Arrangements and Standards

6 Government will grant recognition only to those CAs which have achieved a trust standard acceptable to Government. Therefore, the applicant must be able to demonstrate that its systems, procedures, security arrangements and standards will work together to form a trustworthy system with which the applicant issues certificates to subscribers and carry out related services.

7 Guidelines on a trustworthy system are described in section 5 of the Code of Practice.

Assessment Report

8 At least once in every 12 months, a recognised CA must furnish to the Director a report containing an assessment as to whether the recognised CA has complied with the provisions of the Ordinance applicable to a recognised CA and this Code of Practice during the period for which the report is prepared.

9 All assessments must be conducted by a qualified independent person approved by the Director for this purpose. Certified Public Accountants, i.e. professional accountants with practicing certificates issued under the Professional Accountants Ordinance (Cap. 50), who are supported by technical expertise in IT as necessary, are considered acceptable for approval by the Director as the person to prepare the report. The Director may also consider the suitability of other persons as being qualified to prepare the report.

Fit and proper person

10 As set out in subsection 20(3)(e) the applicant and its responsible officers have to be fit and proper persons. The criteria for determining whether a person is a fit and proper person is set out in subsection 20(4) of the Ordinance, and the applicant, in making the

application for recognition, has to make a declaration to confirm that the applicant and its responsible officers are fit and proper persons.

Validity period of recognition of a CA

11 The validity period for the recognition of a CA will normally be for 2 years. The CA may apply to the Director for the renewal of the recognition at least 30 days before but not earlier than 60 days before the expiry of the validity of the recognition.

Recognition of certificates

12 A recognised CA may apply to the Director for recognition of some or all of its certificates. If the CA is not yet a recognised CA, the CA can submit an application of recognition both for itself as well as for its certificates. The recognition of the certificates will be considered after the Director has granted recognition to the CA concerned.

13 In general, so long as a CA maintains its recognition status, the recognition status of a certificate issued by the CA will not change provided that the CPS, including the relevant certificate policy (if supported) that governs the recognised certificate, has not materially changed.

14 Material changes that may affect the recognition status of the certificate may include:

(a) changes in the identification process that weaken the reliability of the certificate;

(b) changes in the reliance limit of the certificate; or

(c) changes in the key generation, key storage, key usage requirements.

Certificate recognition criteria

15 For the recognition of a type, class or description of certificates, the recognised CA has to demonstrate that:

(a) the certificates are issued in accordance with the CA's CPS;

(b) the certificates are issued in accordance with the Code of Practice; and

(c) the arrangements put in place or proposed to be put in place by the CA to cover liability that may arise from the issue of that type, class or description of certificates are sufficient.

Guidelines on the Contents of Certification Practice Statements

Introduction

1 The Ordinance and the Code of Practice (the Code) require, among other requirements, that a recognised CA must:

- issue and maintain an up to date CPS[1]; and
- notify the Director of changes to the CPS.

2 This Annex provides guidelines on the contents of a CPS, which recognised CAs must as a minimum consider.

3 It is important to note that CPSs are tailored to the organisational structure, operating procedures, facilities, and computing environment of specific CAs and the particular certificate policies that the CA intends to issue certificates under. As such the level of details of a CPS as well as the specific attributes of each section in the CPS may vary from CA to CA.

4 The primary source of these guidelines was the IETF (The Internet Engineering Task Force) RFC 2527 “Certificate Policy and Certification Practices Framework”, commonly referred to as “IETF PKIX Part 4”. Nevertheless, it is not intended that this should be the only relevant source for guidelines on the contents of CPS.

[1] The concept of a CPS was first articulated in the American Bar Association (ABA) Digital Signature Guidelines. The ABA Guidelines define the CPS as “a statement of the practices which a certification authority employs in issuing the certificates”. The term was chosen, in part, to avoid ambiguity or confusion in the usage of the word “policy”. CPS should not be confused with Certificate Policies (CP) because they tend to differ in terms of authorship, purpose, level of specificity, and approach.

Appendix: Suggested Coverage of a CPS

1 Summary of Attributes

Under this section, the CA has to consider providing a summary of the key attributes relating to the type, class or description of certificates that the CA issues. The purpose of this section is to enable users of the CA to quickly gain an understanding of the relevant factors of the certificates issued under the CPS.

Such attributes has to include, for example, the recognition status of each type, class or description of certificates, their respective reliance limit, and other significant attributes, such as the form of identification required, that may otherwise impact the level of confidence or trust that subscribers or relying parties may place on the certificates. This section should also include a reference to a web site or other source where the CA maintains information about the status of its recognition and its CA disclosure record maintained by the Director.

2 Introduction

2.1 Overview

A high level summary of the purpose and scope of the CPS, including the scope of its recognition, such as whether any conditions have been attached, and a general description of what that recognition means for both subscribers and relying parties. This section may also highlight the scope and the terms and conditions of the CAs services.

2.2 Identification

A CA that is not seeking recognition of the certificates it issues need not identify any supported certificate policies (CPs). Nevertheless a CA that supports specific CPs and that is seeking recognition of any of the certificates it issues has to identify those policies here and provide the appropriate object identifier of the CP. In addition it has to ensure that the full text of the policies identified is posted in a location accessible on-line to subscribers and prospective subscribers.

2.3 Community and applicability

This section has to identify all known groups or functions that form part of, or participate in, the operation and maintenance of the CA. Examples may include the CA function, the registration function, repositories, and target end users (i.e. subscribers). Where one or more of the core CA functions are outsourced, such as the use of a third party registration function, this must be clearly stated.

Where applicable, this section also has to set out the limitations on the applicability of each type, class or description of certificates issued by the CA, covering for example:

- usage for which the issued certificates are suitable, e.g. electronic mail, retail transactions, contracts, etc.;

- restricted usage of the issued certificates; and

- prohibited usage of the issued certificates.

2.4 Contact details

The CPS has to identify at least one point of contact for communication with the CA that can address subscriber, regulatory and other inquiries. Typically the CPS would state at least a telephone number, postal address and email address for subscribers and relying parties to contact the CA. The CPS should also provide information on reporting or hotline facilities for subscribers where provided, e.g. for reporting lost key.

3 General Provisions

3.1 Obligations

3.1.1 CA obligations

This section has to clearly state the obligations the CA assumes as part of its service offerings, encompassing specific requirements set out in the Ordinance, including any conditions for its recognition, and the Code of Practice. Examples of such obligations may include:

- notification (including the timing of such notification) of issuance of a certificate to the subscriber who is the subject of the certificate being issued; and

- notification (including the timing of such notification) of revocation or suspension of a certificate to the subscriber whose certificate is being revoked or suspended.

Where the recognised CA has outsourced any of its functions, then the respective obligations of these functions have to be separately described.

3.1.2 Subscriber obligations

This section has to describe the duties and obligations assigned to their subscribers in accordance with the CPs that the CA supports, for example:

- ensuring accuracy of representations in certificate application;

- protection of the subscriber’s private key;

- restrictions on private key and certificate use; and

- notification upon private key compromise.

3.1.3 Relying party obligations

This section has to clearly state all representations made to relying parties in accordance with the CPS, including any CP that the CA supports, for example:

- understanding the purpose for which the certificate is used;

- responsibilities over the verification of digital signature;

- responsibilities over the checking of certification revocation and suspension; and

- acknowledgement of applicable liability limitations and warranties.

3.1.4 Repository obligations

This section has to clearly state the obligations the CA assumes in providing the repository service, encompassing specific requirements set out in the Ordinance, including any conditions for its recognition, and the Code of Practice. Examples of such obligations may include the timely publication of certificates and revocation (including certificate suspension) information.

3.2 Liability

The CA has to clearly specify any applicable provisions regarding apportionment of liability including handling of transactions supported by a certificate and occur between the time when the subscriber requests the revocation or suspension of the certificate and the time when the CA actually revokes or suspends the certificate.

The CA also has to clearly specify the implications of a stated reliance limit. In any event, nothing in this section should be taken to exclude, or indemnify the CA against liability that cannot be lawfully excluded.

3.2.1 Warranties and limitations on warranties

With respect to each type, class or description of certificates that it issues, the CA has to clearly specify any warranties and/or limitations it may want to impose.

3.2.2 Damages covered and disclaimers

With respect to each type, class or description of certificates that it issues, the CA has to clearly specify any damages that it covers, (e.g. indirect, special, consequential, incidental, punitive, liquidated damages, negligence and fraud), and any disclaimers and limitations on its obligations.

3.2.3 Loss limitations

With respect to each type, class or description of certificates that it issues, the CA has to clearly specify any limitations on losses per certificate or per transaction.

3.2.4 Other exclusions

With respect to each type, class or description of certificates that it issues, the CA has to clearly specify additional exclusions that may be applicable.

3.3 Financial responsibility

This section has to specify aspects relating to the financial responsibilities of the CA and any other parties identified in the CPS. Areas that may be addressed include:

- whether fiduciary relationships would exist between any of the parties identified in the CPS or are expected to be created as a result of the act of issuance of certificates;
- financial responsibility for administrative processes ;
- financial assurances provided by the CA to subscribers and relying parties in respect of its potential or actual liabilities and claims against reliance limits on its certificates; and
- any other financial aspects e.g. existence of performance bonds, insurance policies, or any other responsibilities that may arise from the recognition process (e.g. as a condition of recognition).

3.4 Interpretation and enforcement

3.4.1 Governing law

The CPS has to specify the governing jurisdiction for the CA and the related CPS, subscriber agreement and relying party agreements.

3.4.2 Severability of provisions, survival, merger, and notice

This section has to state the fact that if one or more of the sections in the CPS is found to be illegal, unenforceable, or void, then the other sections will still remain in effect. Any identified issues or problems have to be immediately addressed.

3.4.3 Dispute resolution procedures

This section has to state the procedures established by the CA to resolve disputes and claims regarding its operations and representations to their subscribers or relying parties. The procedures should state at a minimum the process of filing a dispute or claim with the CA and the steps a CA takes upon notification of a claim or dispute.

3.5 Fees

This section has to clearly state all costs and fees to subscribers and relying parties for each class, type or description of certificates issued by the CA.

3.6 Publication and repositories

This section has to specify the policy and mechanism that the CA has implemented to communicate with its subscribers and relying parties the information relating to its CPS, including the details of any certificate policies that the CA supports, and the current recognition status of the certificates that it issues. This should include, for example, the means of publication, the frequency of publication, the availability of the information, any controls over access, and details of the repository.

The full version of the CPS, or possibly a version that withholds details of the operation that could be exploited to adversely affect the integrity of the CA and its components, has to be displayed prominently on the CA's web page or other conveniently available location.

Since the actual procedures followed by the CA can be reasonably expected to evolve, updates to the CPS have to be posted as appropriate. All changes have to be prominently displayed at the same location where the CPS is displayed.

3.7 Compliance assessments

This section has to state the mechanism and frequency for any compliance assessments relevant to the CA, including any mandatory requirements under the Ordinance and the Code of Practice. Specific aspects that may be covered include, for example:

- the frequency of compliance review for the CA and any of its outsourced functions;
- the identity or qualifications of the independent party to carry out the review;
- the relationship of the party which carries out the review to the entity being reviewed;
- overview of the coverage of the compliance review; and
- policy concerning the communication of the compliance review results (i.e. who will receive copies of the report) and policy on follow up actions.

3.8 Confidentiality policy

This section has to specify the CA's policy on maintaining confidentially of information. Aspects that may be specifically addressed include, for example:

- types of information that must be kept confidential by the CA, including any outsourced functions;
- types of information that are not considered confidential;
- the persons that are entitled to be informed of reasons for revocation and suspension of certificates;
- policy on release of information, e.g. to law enforcement officials, requirement under disclosure procedure in legal proceedings, etc;
- conditions upon which CA, including any outsourced functions, may disclose upon owner's request/consent; and
- any other circumstances under which confidential information may be disclosed.

As a general rule, CAs have to comply with all applicable regulations regarding the privacy of personal information and the provisions of the CPS should not contradict current privacy regulations within Hong Kong and section 41 of the Ordinance.

3.9 Intellectual property rights

This section specifically addresses the intellectual property ownership rights of certificates, data structure of certificates, CPS, practice/policy specifications, names, and keys.

4 Identification and Authentication

This section sets out the procedures used by the CA, or its outsourced registration function where appropriate, to authenticate a subscriber prior to the issuance of certificates. Each class, type or description of certificates that a CA issues has to be described in this section.

This section also has to cover the authentication process in the event of rekey or rekey after revocation. This section also has to address the CA practices relating to naming, such as name ownership, name dispute and name resolution.

The CA has to specify in the CPS the acceptable forms of identification such as the Hong Kong Identity Card, passports, articles of incorporation, etc.

4.1 Initial Certification

This section address the identification, authentication and naming procedures to be followed during the issuance of new certificates. This section should cover the specific procedures that the CA follows in order to identify the certificate applicant, including the specific documents that an individual or organisation must produce prior to the CA issuing a certificate to the end entity.

4.1.1 Types of Names

This section has to specify the CA’s naming convention that is adopted, such as X.500 Distinguished Names (DN) or other forms of DNs in the case of web site certificates. Alternate name forms including for example an email address or a personal identification number may be included to ensure that the certificate of a person can be unambiguously obtained.

This section also has to specify the details of all name forms, including prefixes and conventions that may be implemented to avoid name collisions.

4.1.2 Need for names to be meaningful

This section has to specify whether names within a certificate must be meaningful and if so, the CA’s procedures for ensuring that the DNs assigned to its subscribers are meaningful and appropriately identify the subscriber.

4.1.3 Rules for interpreting various name forms

This section should include guidance on the interpretation of the name formats contained within the certificates issued under the CPS. The degree of depth in this area depends upon the name formats contained in the certificates. In general if the interpretation of names within a certificate may be misconstrued by relying parties, the CA should consider providing guidance to relying parties to reduce the risk of misinterpretation.

4.1.4 Uniqueness of names

The CA has to make specification if names within certificates are required to be unique. If so, the CA should disclose its requirements or any uniform rules that are applied for ensuring distinguished names to be unique.

4.1.5 Name claim dispute resolution procedure

If appropriate, this section has to specify the CA's resolution procedures, as appropriate, concerning any naming conflicts.

4.1.6 Method to prove possession of private key

In cases where the subscribers generate their own key pairs and remain in exclusive control of the private keys, the CPS must state how the CA verifies that the subscriber's private key corresponds to the public key submitted for certification.

4.1.7 Authentication of subscriber identity

This section has to specify the CA's procedures for ensuring that the name on a certificate corresponds to the person being issued the certificate. A primary purpose of this section is to enable subscribers to understand the requirements necessary to obtain a digital certificate under this CPS as well as to enable relying parties to understand and draw conclusions as to the reliability of the certificates issued under this CPS.

4.2 Routine Rekey and Certificate Renewal

This section has to describe the procedures the CA adopts for routine rekey and certificate renewal, especially if such procedures for identification of the subscriber differ from the initial registration and issuance. The CPS should state whether certificate renewal takes place without rekeying. This section has to specify the CA's policy as to whether it will adopt a procedure which is different from that for initial certificate issuance upon the expiration of the validity of the certificates.

4.3 Rekey after revocation

This section has to specify whether the CA will adopt a procedure different from that for initial certificate issuance after revocation of a certificate. If so, the details of such procedure have to be included in the CPS.

4.4 Revocation request

This section has to specify the CA procedures and mechanisms for authenticating and handling revocation requests, covering for example:

- who is authorised to request revocation of a certificate and under what circumstances;
- the effect of a revocation;
- how soon will the validity status of certificates be published after revocation;
- the responsibilities of the subscriber regarding the report of events requiring revocation; and
- protections afforded to the subscriber once revocation is requested, including the apportionment of liability between the CA and the subscriber.

4.5 Suspension request

This section has to specify whether the CA supports the suspension of certificates, and if so has to detail the conditions for, as well as the effect of a suspension. The CPS should be specific about the implementation of suspensions and, if appropriate, address the same elements identified for revocations in section 4.3.

5 Operational Requirements

5.1 Certificate application

In this section, the CA has to set out the details on the specific process for obtaining a new certificate. It has to include:

- the method of applying for a certificate and the documentation required to prove the identity of the subscribers;
- the information provided to the subscriber including, but not limited to, subscriber responsibilities, representations by the CA, and terms and conditions for the certificate, the recognition status of the CA and the certificate and what that means to the subscriber, especially if the certificate is not recognised by the Director; and
- interface requirements for the certificate requests.

5.2 Certificate issuance

In this section, the CA has to set out the details on the specific process to be followed by the CA in issuing certificates. The process for issuance of certificates includes:

- the generation of keys;
- the delivery of the keys to the appropriate parties (i.e., if the keys are generated by the subscriber, the public key must be delivered to the CA with the certificate request and

the CA must verify that the subscriber is in possession of the corresponding private key; if the keys are generated by the CA, the private key must be securely delivered to the subscriber and the CA must indicate appropriate measures to ensure the proper handling of the keys in its possession);

- the CA must not have possession of subscribers' private keys without the consent of the subscribers;
- the generation of the certificates;
- the delivery of certificates to the subscribers; and
- the posting of the certificates to a repository.

5.3 Certificate acceptance

Acceptance is the action by a subscriber that triggers the subscriber's duties and potential liability. In this section, the CA has to define the technical or procedural mechanism to:

- explain to subscribers their responsibilities as defined in Section 3.1.2;
- inform subscribers of the creation of a certificate and the contents of the certificate;
- require the subscribers to indicate acceptance of the responsibilities and the certificate; and
- enable the subscriber to obtain the digital certificate from the CA.

5.4 Certificate suspension and revocation

In this section, the CA has to explain the procedures employed to initiate a certificate suspension, if supported, and certificate revocation. This section should include the procedures that a subscriber or other authorised party would use to instruct a CA to suspend or revoke a certificate.

5.4.1 Suspension (if supported)

In this section, the CA has to provide the details of the suspension process, including:

- the conditions for suspension (including, but not limited to, who can trigger/recall a suspension);
- the means for requesting/triggering a suspension;
- the means for notification of a suspension (e.g. through postings, e-mail or inclusion in a certificate revocation list);
- the conditions, such as time limits, for recalling the suspension or moving from suspension to revocation;

- the time for the recognised CA to suspend a recognised certificate as well as the allocation of liability for transactions using the certificate in between the time when suspension is requested by the subscriber or a person who is authorised to act for the subscriber, and the time when the certificate is actually suspended;

- the associated CPS has to define the expected time period within which the CA checks with the subscriber or authorised person whether the recognised certificate that was suspended should be revoked or should be reinstated after suspension; and

- the action the CA takes in the event that it is not possible for the recognised CA to contact the subscriber or the authorised person to ascertain the ultimate disposition of the suspended certificate.

5.4.2 Revocation

In this section, the CA has to provide the details of the revocation process, including:

- the conditions for revocation (including, but not limited to, who can trigger/recall a revocation);

- the means for requesting/triggering a revocation;

- the means for notification of revocation (e.g. through postings, e-mail, inclusion in a certificate revocation list, or updates to a revocation/validity information server); and

- the time for the recognised CA to revoke a recognised certificate as well as the allocation of liability for transactions using the certificate in between the time when revocation is requested by the subscriber or a person who is authorised to act for the subscriber, and the time when the certificate is actually revoked.

Authorised parties may request revocation of the subscriber’s certificate using an interface that identifies the certificate to be revoked, explains the reason for revocation, and allows the request to be authenticated (e.g. digitally or manually signed). Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorised parties. The means for transmitting the information has to be readily available to subscribers such as electronic mail and web interfaces.

Typically, a certificate has to be revoked under the following circumstances:

- identifying information or attributes in the user certificate change before the certificate expires;

- the certificate subject is known to have violated the stipulations of the applicable CPS of the CA who issued the certificate;

- the subscriber suspects or confirms compromise of the private key; or

- the user no longer wants or requires the ability to sign electronic messages.

5.4.3 Certificate revocation lists

Certificate Revocation Lists (CRLs) identify unexpired certificates that are no longer valid and give the reason why each was revoked. The CPS should state the mechanisms used to distribute the CRLs and how relying parties may access such lists or other mechanisms to establish the status of a particular certificate.

The CA has to specify in this section the frequency for updating CRLs. The CA may decide to use or support additional mechanisms for verifying certificate validity. The CPS has to address the available mechanisms, the terms and conditions for their use and how to access the information.

5.4.4 CRL checking requirements

CAs have to notify subscribers and post prominently in a location generally accessible that there are risks in relying on a digital signature if a certificate containing the public key is no longer valid. Relying parties assume their own risks if they fail to check the validity of certificates.

The CPS has in addition to specify, clearly and prominently, its policy concerning the situation where a relying party is temporarily unable to obtain revocation information. The CA may wish to address specifically the apportionment of any liability that may arise in such circumstances.

5.5 Security review procedures

This section is used to describe event logging and review systems that are implemented by the CA for the purpose of maintaining a secure environment. Elements include the following:

5.5.1 Types of events recorded

This section has to describe the types of events that are recorded by the CA. At a minimum, the CA has to consider recording:

- suspicious network activity;
- repeated failed access attempts;
- events related to equipment and software installation, modification, and configuration within the entire CA operation;
- privileged accesses to all CA components; and
- regular certificate management operations, such as:
  - certificate revocation and suspension requests;
  - actual issuance, revocation, and suspension of certificates;

- certificate renewals;
- updates to repository(ies);
- CRL generation and posting;
- CA key rollover;
- backups; and
- emergency key recoveries.

To the extent practicable, the events recorded have to identify the entities or individuals that triggered the event and include any action taken in response and by whom. All entries have to be dated and time stamped.

It is good practice for the CA to first establish the thresholds for severity and significance of individual security-related events and trends based on currently accepted practices. All events and significant trends beyond those thresholds have to be recorded.

The CA has to implement separation of privilege and other mechanisms or procedures to ensure the integrity of all records. The mechanisms and procedures used to implement separation of privilege should be described in the CPS.

5.5.2 Frequency of processing event logs

This section specifies the frequency with which the event logs are processed, e.g. consolidated and reviewed.

5.5.3 Retention period for event logs

This section specifies the retention period for event logs, which has to conform to the requirements in the Code of Practice.

5.5.4 Protection of event logs

This section specifies the mechanism in place to protect the event logs from accidental damage or deliberate modifications.

5.5.5 Event log backup procedures

This section specifies the procedures for backing up the event logs, as well as the retention period. It is good practice to ensure that the storage facility can affords the backups adequate protection against theft, destruction, or media degradation. Further, it is important to ensure that the method of storage and retrieval of the data must remain current and functional for the life of the archive.

5.6 Records archival

This section is used to describe the CA's policy relating to general records retention. As a general rule, the CA has to ensure that archive records are detailed enough to establish the validity of a certificate and the proper operation of the CA at some point in time. Typical data that the CA may consider for archiving include:

- data relating to the initialisation of the CA equipment, such as:
    - CA system equipment configuration files;
    - results of CA assessments and/or reviews accreditation (if necessary);
    - certification practice statement; and
    - any contractual agreements to which the CA is bound; and
- data relating to CA operation:
    - modifications or updates to any of the above data items;
    - all certificates and CRLs (or other revocation information) as issued or published;
    - periodic event logs (in accordance with section 5.5); and
    - other data necessary for verifying archive contents.

5.6.1 Retention period for archive

This section specifies the retention period for archived records, which has to conform to the requirements in the Code of Practice.

5.6.2 Protection of archive

This section specifies the procedures in place to protect the archive records, covering for example:

- the custodian of such archives;
- the mechanism for accessing such records, such as for the purpose of reviews, for or the resolution of disputes; and
- the protection in place to protect the archive from accidental destruction or deliberate modification, theft, or media degradation.

5.6.3 Archive backup procedures

This section specifies the procedures for backing up the archived records, as well as the retention period. It is good practice to ensure that the storage facility affords the backups adequate protection against theft, destruction, or media degradation. Furthermore, it is important to ensure that the method of storage and retrieval of the data must remain current and functional for the life of the archive.

5.7 Key changeover

This section has to specify the details of the CA key changeover and the mechanism for informing the subscribers of the procedure.

5.8 Compromise and disaster recovery

This section describes the CA's requirements relating to notification and related recovery procedures in the event of key compromise or disaster. The CA must address specifically the following:

- the CA's procedures to recover from situations where its computing resources, software, and/or data are corrupted or compromised, or suspected to be corrupted or compromised; these procedures typically describe how a secure environment is re-established, which certificates are revoked, whether the CA's own key is revoked, how the new CA public key is provided to the subscribers, and how the subscribers are re-certified;

- the procedures to recover from a key compromise or suspected key compromise, including the notification of subscribers and relying parties as well as procedures to re-establish the trustworthiness of the CA; and

- the CA's procedures for securing its facility during the period of time following a natural or other disaster and before a secure environment is re-established, either at the original site or a backup site. For example, procedures to protect against theft of sensitive materials from a damaged site.

The Director must immediately be notified of any of the above events.

5.9 CA termination

This section specifies the arrangements relating to procedures for the CA's termination and for notifying its subscribers and relying parties of such termination, including the identity of the custodian of the CA's archival records. Such arrangements have to comply with the requirements set out in section 11 of the Code of Practice.

6 Physical, Procedural, and Personnel Security Controls

This section describes the non-technical operational controls established by the CA to provide assurance that its business is conducted in a trustworthy manner.

Example of such controls typically include physical, procedural, and personnel controls over key CA functions, such as key generation, authentication, certificate issuance, certificate revocation, audit, archival, etc. Similar controls may also be established in respect of repositories, as well as any outsourced functions, such as registration function.

6.1 Physical security controls

This section describes the physical controls on the facility housing the CA systems, covering for example:

- site location and construction;
- identification of secure areas and physical access considerations;
- environmental hazards arising from factors such as power, air conditioning, humidity, water, fire, etc; and
- media storage and disposal.

6.2 Procedural controls

A trusted role is one of which the incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. People in trusted roles include responsible officers with CA management oversight and operational personnel. The persons selected to assume these roles must be capable and competent. The functions performed in these roles form the basis of trust in the entire CA.

This section describes the CA's procedures for identifying trusted roles, such as the generation of the CA's keys, and defining the responsibilities for these roles. Typically such procedural requirements would specify the tasks to be performed, and the number and level of individuals required to perform each task, together with the controls to be implemented, such as dual control, identification and even authentication of the individuals concerned.

Typical trusted roles might include:

- CA Administrator who oversees the issuance of all certificates, the operation of the CA, and the collection and maintenance of records. Primarily, the CA Administrator should ensure the CA functions are conducted in accordance with the stipulations in the CA's CPS;
- key recovery agent - an individual in charge of the more specific functions related to the maintenance of key recovery material or systems; and
- other trusted roles - CAs may define additional roles under the supervision of the CA Administrator. Such roles have to perform specific functions in accordance with relevant provisions in this document. Whenever appropriate, separation of duties has to be implemented for all operations potentially affecting system integrity.

6.3 Personnel security controls

This section describes the controls over the recruitment, monitoring, assessment, training and termination of CA personnel. Specific aspects that could be addressed may include:

- recruitment process, including background checks and clearance procedures for personnel filling trusted roles and for those who are engaged in less sensitive positions;
- training requirements and training procedures, including any retraining period and retraining procedures;
- frequency and sequence for job rotation among various roles;
- performance assessment framework, and disciplinary and termination procedures against personnel for unauthorised actions, improper use of authority, and unauthorised use of CA systems;
- controls on contracting personnel, including contractual requirements such as indemnification for damages due to the actions of the contractor personnel, monitoring the performance of contractor personnel, etc; and
- documentation to be supplied to personnel, such as user manuals, operational procedures, etc, necessary to support these personnel in performing their duties.

7 Technical Security Controls

This section defines the technical security measures established by the CA to specifically protect its cryptographic keys and activation data (e.g., PINs, passwords, etc). The CA may also describe any requirements or constraints that it wishes to impose on repositories, subscribers, etc, to ensure the proper protection of their cryptographic keys and critical security parameters. Secure key management is critical to maintaining a trustworthy system, and ensures that all private keys and activation data are protected and used only by authorised personnel. This section also describes other technical security controls used by the CA to support the key and certificate management life cycle.

It is important to separate the controls performed by the CA from those performed by other parties, such as any outsourced functions (e.g. registration function, repositories, etc.) and subscribers, so that the responsibilities of the respective parties can be clearly identified.

Specific control areas that may be addressed would include, for example:

- key pair generation, installation, and other aspects of key pair management, including:
  - the responsibility for generating the public and private key pair;
  - secure delivery of the private key to subscribers;
  - secure delivery of the subscribers' public key to the certificate issuer;

  - secure delivery of the CA public key to subscribers;
  - key size adopted, taking into consideration the available technology;
  - controls over generation and quality checking of public key parameters;
  - where keys are generated, i.e. within hardware or software module; and
  - key usage and purpose (and mapping to key usage flags for X.509 version 3 certificates).

- private key protection, for example:
  - the standards, if any, required for the key generation module; for example, key generation modules are compliant with a specific level according to the ISO 15782-1/FIPS 140-1 standard;
  - the use of multi-person control over private key;
  - back up of private keys, including the form of back up and the related security controls of the backup system;
  - archive of private keys, including the form of the key archived and the related security controls on the archival system;
  - controls over the activation, usage and deactivation of the private key, including for example the number of persons required for key entry, the form of the private key, the activation mechanism, the active period of an activated key, etc;
  - controls over the destruction of the private key, such as token surrender, token destruction, or key overwrite;
  - public key archival; and
  - usage period for public and private keys.
- controls over activation data, which outline the controls over the life cycle of activation data, from generation, distribution, through to archival and destruction. Control considerations should be similar to those for key pair generation and private key protection described above;
- computer security controls, which outline the security features in place to prevent and detect unauthorised access, modification, or compromise of the CA systems. Reference may be made to an appropriate computer security rating framework, such as ISO 15408:1999 / The Common Criteria for Information Technology Security Evaluation (CC);

- system development life cycle control, which outline the controls implemented by the CA over the development life cycle of its systems, covering mechanisms and procedures for purchasing or developing the software and hardware for the initial configuration of the CA equipment to prevent tampering;
- network security controls, which outline the control to protect all connectivity to CA equipment, such as an appropriately configured and maintained firewall, or equivalent access control device, as well as the monitoring of unauthorised access attempts and prevention against malicious attacks; and
- cryptographic module engineering controls, which outline the specific control requirements for cryptographic modules. These may be referenced to an appropriate standard, such as ISO 15782-1/FIPS 140-1 Security Requirements for Cryptographic Modules.

8 Certificate and CRL Profiles

This section specifies the certificate format and, where applicable, the CRL format adopted by the CA, including information on profiles, versions, and extensions used. It is generally envisaged that the CA would issue and manage public key certificates defined in accordance with the X.509v3 certificate format and would generate and post CRL in accordance with the ITU X.509 v2 CRL Format.

8.1 Certificate Profile

This section provides information relating to the specific format of the certificate profile, and may cover the areas set out below.

- version number(s) supported;
- certificate extensions, specifically those populated and their criticality;
- cryptographic algorithm object identifiers;
- name forms used;
- name constraints;
- certificate policy object identifier(s);
- usage of the policy constraints extension;
- policy qualifiers syntax and semantics; and
- processing semantics for the critical certificate policy extension.

8.2 CRL profile

This section provides information relating to the CRL, possibly referencing to an appropriate standard, covering:

- Version numbers supported for CRLs; and

- CRL and details of the CRL entry extensions populated and their criticality; the certificate profile used should be as simple as possible and should be in conformance with RFC 2459 Internet X.509 PKI Certificate and CRL Profile.

9 Specification Administration

This section describes how a CPS will be maintained.

9.1 Specification change procedures

This section describes the procedures for effecting any changes to the CPS, including the mechanism for notifying the Director, subscribers and relying parties in accordance with the requirements set out in the Code of Practice for such changes. Changes to CPS must be reflected and highlighted on the CA's repository upon taking effect or sooner. The CA may in addition specify the types of changes that do not require prior notification.

9.2 Publication and notification procedures

This section describes the CA's procedures in publishing all relevant information on a repository that is known to all subscribers and relying parties, which could be a web site. The location of this repository, and any other alternative information sources must be identified.

10 Interoperability

To facilitate interoperability, the CA may choose to specify, where appropriate, the level of interoperability that it will support based on the technology that it has implemented. This may require the CA to specify the specific standards or protocols that it adopt for its systems, or components of its systems. Details that could be published may, for example, include the standards adopted for the repository (e.g. LDAP compatible), or the specific certificate profile (e.g. X.509), certificate extension, etc.

Compliance Assessment on Certification Authorities

Introduction

1 Subsection 19(3)(b) of the Ordinance specifies that a CA seeking recognition must furnish to the Director a report prepared by a person acceptable to the Director for giving the report. The report must provide an assessment as to whether the CA is capable of complying with the provisions of the Ordinance applicable to a recognised CA and the Code of Practice. Subsections 37(1) and (2) of the Ordinance specify that at least once in every 12 months, a recognised CA must furnish to the Director a report containing an assessment as to whether the recognised CA has complied with the provisions of the Ordinance applicable to a recognised CA and the Code of Practice during the period for which the report is prepared. The report must be prepared by a person approved by the Director as being qualified to make such a report. This Annex provides further clarification and elaboration on the concerned arrangements.

2 This Annex is aimed at:

- ■ the person referred to in subsections 19(3)(b)(ii) and 37(2) of the Ordinance who will be preparing the report referred to in subsections 19(3)(b)(i) and 37(1);
- ■ CAs that are preparing for a compliance assessment; and
- ■ CAs that are considering applying for recognition.

3 This Annex has two parts. Part 1 sets out the required minimum qualifications of persons qualified to conduct such compliance assessment review. Part 2 sets out the minimum areas that should be covered as part of the compliance assessment review.

Part 1: Qualification of the independent assessor

4 The purpose of Part 1 is to provide guidance on the qualifications that assessors are required to possess in order that they are to be considered acceptable by the Director to conduct such an assessment in accordance with subsections 19(3)(b)(ii) and 37(2) of the Ordinance.

The assessor has to:

- ■ be organisationally independent of the CA seeking recognition; and
- ■ be accredited by a recognised professional organisation or association. Membership in the particular organisation or association has to require members to adhere to certain requirements, such as:
  - – possession of certain skill sets;
  - – adherence to quality assurance measures, such as peer review;
  - – successfully complete competency testing set by the organisation or association;

  - – adhere to standards with respect to proper assignment of staff to engagements; and
  - – compliance with requirements for continuing professional education; and

- ■ possess demonstrated proficiency in:
  - – public key infrastructure and related technology, such as digital signatures and certificates, etc;
  - – applying information security tools and techniques;
  - – performing financial reviews;
  - – performing security reviews; and
  - – performing third-party reviews.

5 The assessor can be an individual possessing all of the above requirements, or a party or an organisation comprising individuals that collectively possess all of the above requirements. The individual signing the assessment report must:

- ■ be a registered member of a recognised 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 signatures and certificates, 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.

Part 2: Guidance on scope of compliance assessment

6 The purpose of Part 2 is to provide specific guidance on the required scope and coverage of the compliance assessment to be performed under subsections 19(3)(b)(ii) and 37(2) of the Ordinance.

Objective of compliance assessment

7 The objective of the compliance assessment is to determine:

- ■ whether, in all material respects, the CA under assessment is capable of, or have been complying with the requirements under relevant provisions of the Ordinance and the Code of Practice; and

- ■ whether, in all material respects, the CA has complied with the policies and business practices specified in its CPS.

Scope of the compliance assessment

8 The assessment has to cover the assertions made by the CA concerned, based on the recognition criteria set out in the Ordinance. The focus of the assessment is on the CA's capability to comply or actual compliance with the relevant provisions under the Ordinance and the Code of Practice.

9 The key areas to be covered in the assessment, which are further elaborated in the following sections, have to cover as a minimum the following:

- obtaining an understanding of the CA's policies and business practices, and assessing whether such information has been properly disclosed;
- assessment of the CA's adherence to its financial commitments, e.g. meeting its liabilities;
- assessment of the CA's adherence to the requirements concerning the use of a trustworthy system to support its operations; and
- where applicable, assessment of the CA's adherence to the requirements regarding the recognition of certificates.

Disclosure of CA policies and business practices

10 The assessor has to obtain an understanding of the policies and business practices defined by the CA. It is envisaged that such information, including details of the services provided or intended to be provided by the CA, will be incorporated into the CPS issued and maintained by the CA.

11 Where the CA supports one or more CPs, the assessor has also to seek to obtain an understanding of the requirements specified in each policy.

12 The assessor has to assess whether these policies and business practices are disclosed in accordance with the requirements set out in the Ordinance and the Code of Practice.

Assessment of financial commitments

13 The assessor has to assess whether the CA under assessment, is in all material respects capable of being, and remaining, a going concern, i.e. a financially viable business entity. Considerations have to be made to the following aspects:

(a) the arrangements established by the CA to determine its potential liability exposure and to ensure adequate cover against potential claims arising out of any error or omission on the part of the CA, its officers, employees or agents, for example through obtaining professional indemnity insurance for negligence;

(b) the arrangements established by the CA to ensure adequate cover of its potential liability arising from the reliance limits specified in the certificates issued, or planned to be issued by the CA, such as through appropriate insurance cover; and

(c) the CA's intention of being, and remaining, a going concern. Such intentions may be demonstrated by:

- maintaining adequate financing to support the CA operation;

- installing, or contracted to install, systems and equipment necessarily required to support the CA operation and having made the necessary financial arrangements; and

- ensuring the availability of appropriate level of personnel, both in terms of quality (skill set) and quantity (number of staff), to support the CA operation and having made the necessary financial arrangements.

Assessment of systems, procedures, security arrangements and standards

14 Section 31 of the Ordinance requires a recognised CA to use a trustworthy system in performing its services. The CA under assessment must demonstrate that its systems can adequately fulfil this requirement as well as those requirements set out in its CPS. Section 5 of the Code of Practice provides guidelines over the assessment of a trustworthy system.

15 The assessor has to design appropriate tests as considered necessary to provide adequate evidence of the implementation and use of a trustworthy system by the CA.

Assessment of certificate life cycle controls

16 A CA seeking recognition of its certificates must demonstrate that:

(a) the certificates are issued in accordance with the CA's CPS as well as in compliance with the requirements set out in the Code of Practice; and

(b) the CA's arrangements for ensuring liability cover are consistent with the context of its business.

17 The assessor has to obtain sufficient evidence to assess whether the above conditions are met by assessing the effectiveness of controls implemented by the CA over the certificate life cycle.

Reporting

18 The assessor is required to prepare a formal written report on the results and findings of the assessment.

19 The assessor is required to provide an assessment as to whether or not, in all material respects, the CA under assessment is capable of, or have been complying with relevant provisions in the Ordinance and the Code of Practice. Specifically the assessor has to consider the following aspects:

- whether or not the CA discloses its business practices in its CPS and maintains effective controls over its CPS, and provides its services in accordance with its disclosed business practices;
- whether or not the CA maintains effective controls to provide reasonable assurance that environmental controls over the CA's operation contribute to maintaining a trustworthy system; and
- whether or not the CA maintains effective controls to provide reasonable assurance that operations specific to a CA, including key management and certificate life cycle management are effective and conform to the CA's CPS.

Reliance on work performed by internal audit

20 Where appropriate, the assessor has to consider the extent to which the CA's internal audit activities may be relied upon to modify the nature, timing and extent of test work performed by the assessor. If reliance on the internal audit function is planned, the assessor should consider:

- the competence and objectivity of the internal audit function;
- the extent to which the internal audit activities cover the specific certification practices of interest; and
- the follow up of the issues identified and status of the resolution of these issues.

Conduct of the assessment

21 The assessor has to perform the assessment in accordance with appropriate standards and practices relating to the performance of such work (where applicable) established by the professional organisation or association to which he is a member.

22 The assessment has to consider the severity of any noted exceptions or deficiencies, based on the results of the work performed in each of the areas subject to the assessment. In addition to the assessment report, significant findings may be communicated to the CA in separate correspondence to facilitate improvements to its operations.

23 The assessor has to design and execute tests to validate that the appropriate requirements set out in CPS, and any CP that it supports, are adequately reflected in the operations, technology and/or documentation. The tests performed by the assessor is expected to include for example:

- inquiry of management and observation of the CA's operation;
- inspection of relevant documents and logs;
- verification of system settings; and
- other tests deemed appropriate by the assessor.

24 Not withstanding the above, the assessor has to apply due professional judgement in determining the nature, timing and extent of testing procedures to be performed during the assessment.

References and Authoritative Bodies

25 In performing the compliance assessment, the assessor has to consider generally accepted control principles that may apply to the CA's operation. The related body of knowledge that is currently available may include:

- Institute of Internal Auditors’ Systems Auditability and Control Report
- Information Systems Audit and Control Association and Foundation, Control Objectives for Information and Related Technology (CObIT)
- ANSI (American National Standards Institute) ASC draft X9.79 standard, PKI Policies and Practices Framework, which includes the Certification Authority Control Objectives in a normative annex
- AICPA/CICA CATrust Principles and Criteria
- Evaluation Criteria for Information Technology Security (Common Criteria)
- IETF PKIX Drafts and Requests for Comment