Code of Practice for Recognized Certification Authorities
Published by
the Government Chief Information Officer
under Section 33 of the
Electronic Transactions Ordinance (Cap. 553)

Published in July 2004

(Version 2.0)

Office of the Government Chief Information Officer
The Government of the Hong Kong Special Administrative Region

TABLE OF CONTENTS

1 INTRODUCTION

1.1 This Code of Practice for Recognized Certification Authorities (the Code of Practice) is published by the Government Chief Information Officer (GCIO) pursuant to section 33 of the Electronic Transactions Ordinance (Cap. 553) (the Ordinance).

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

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

1.4 The GCIO shall take into account whether a particular certificate or a type, class or description of certificates is issued or is to be issued by a recognized CA in accordance with this Code of Practice in granting recognition to that particular certificate or that type, class or description of certificates under section 22 of the Ordinance.

1.5 The GCIO may take into account the failure of a recognized CA to comply with this Code of Practice in suspending, revoking, or not renewing a recognition granted to that CA or a recognition granted to a particular certificate or a type, class or description of certificates issued or is to be issued by that recognized CA under sections 22, 23, 24 or 27 of the Ordinance, as the case may be.

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

1.7 The GCIO may from time to time amend this Code of Practice. The GCIO may consult the industry, including CAs recognized under sections 21 and 34 of the Ordinance, in respect of amendments to this Code of Practice. The primary channel of consultation with the industry will be through an Advisory Committee on Code of Practice for Recognized Certification Authorities chaired by the GCIO.

1.8 If any conflict arises in respect of any difference between the English version and the Chinese version of this Code of Practice, the English version shall prevail.

1.9 This version 2.0 of the Code of Practice supersedes version 1.0 of the Code of Practice published in January 2000 including the related Supplementary Note, Second Supplementary Note and Third Supplementary Note published on 28 March 2001, 13 August 2002 and 28 June 2004 respectively.

2 DEFINITION OF TERMS

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

certificate	means a record which (a) is issued by a CA for the purpose of supporting a digital signature which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair; (b) identifies the CA issuing it; (c) names or identifies the person to whom it is issued; (d) contains the public key of the person to whom it is issued; and (e) is signed by the CA issuing it;
certification authority or CA	means a person who issues a certificate to a person (who may be another CA);
certification authority certificate or CA certificate	means a certificate issued by or to a CA for the purpose of certifying certificates issued by that CA. This certificate may be issued by a CA for its own use or by one CA to another CA;
certification authority disclosure record	in relation to a recognized CA, means the record maintained under section 31 of the Ordinance for that recognized 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 or CPS	means a statement issued by a recognized CA to specify the practices and standards that the recognized 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 electronic record and the signer's public key can determine (a) whether the transformation was generated using the private key that corresponds to the signer's public key; and (b) whether the initial electronic record has been altered since the transformation was generated;
electronic record	means a record generated in digital form by an information system, which can be (a) transmitted within an information system or from one information system to another; and (b) stored in an information system or other medium;
fit and proper person	in determining whether a person is a fit and proper person, the GCIO shall, in addition to any other matter the GCIO considers relevant, have regard to the following: (a) the fact that the person has a conviction in the Hong Kong Special Administrative Region or elsewhere for an offence for which it was necessary to find that the person had acted fraudulently, corruptly or dishonestly; (b) the fact that the person has been convicted of an offence against the Ordinance; (c) if the person is an individual, the fact that the person is an undischarged bankrupt or has entered into a composition or a scheme of arrangement or a voluntary arrangement within the meaning of the Bankruptcy Ordinance (Cap. 6) within 5 preceding years; and

(d) if the person is a body corporate, the fact that the person is in liquidation, is the subject of a winding-up order or there is a receiver appointed in relation to it or it has entered into a composition or a scheme of arrangement or a voluntary arrangement within the meaning of the Bankruptcy Ordinance (Cap. 6) within 5 preceding years;

information	includes data, text, images, sound codes, computer programmes, software and databases;
information system	means a system which (a) processes information; (b) records information; (c) can be used to cause information to be recorded, stored or otherwise processed in other information systems (wherever situated); and (d) can be used to retrieve information, whether the information is recorded or stored in the system itself or in other information systems (wherever situated);
issue	in relation to a certificate, means to— (*a*) create the certificate, and then notify the person named or identified in the certificate as the person to whom the certificate is issued of the information on the person as contained in the certificate; or (*b*) notify the person to be named or identified in the certificate as the person to whom the certificate is issued of the information on the person that is to be contained in the certificate, and then create the certificate, and then make the certificate available for use by the person;
key pair	in an asymmetric cryptosystem, means a private key and its mathematically related public key, where the public key can verify a digital signature that the private key generates;
personal data	means personal data as defined in the Personal Data (Privacy) Ordinance (Cap. 486);

Postmaster General	means the Postmaster General within the meaning of the Post Office Ordinance (Cap.98);
properly authorised person	means a person who is authorised to act for the subscriber;
private key	means the key of a key pair used to generate a digital signature;
public key	means the key of a key pair used to verify a digital signature;
recognized certificate	means (a) a certificate recognized under section 22 of the Ordinance; (b) a certificate of a type, class or description of certificate recognized under section 22 of the Ordinance; or (c) a certificate designated as a recognized certificate and issued by the Postmaster General;
recognized certification authority or recognized CA	means a CA recognized under section 21 of the Ordinance or the Postmaster General;
record	means information that is inscribed on, stored in or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in a perceivable form;
reliance limit	means the monetary limit specified for reliance on a recognized certificate;
repository	means an information system for storing and retrieving certificates and other information relevant to certificates;
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;

sign and signature	include any symbol executed or adopted, or any methodology or procedure employed or adopted, by a person with the intention of authenticating or approving a record;
subscriber	means a person (who may be a CA) who (a) is named or identified in a certificate as the person to whom the certificate is issued; (b) has accepted that certificate; and (c) holds a private key which corresponds to a public key listed in that certificate;
trustworthy system	means computer hardware, software and procedures that (a) are reasonably secure from intrusion and misuse; (b) are at a reasonable level in respect of availability, reliability and ensuring a correct mode of operations for a reasonable period of time; (c) are reasonably suitable for performing their intended function; and (d) adhere to generally accepted security principles;
verify a digital signature	in relation to a given digital signature, electronic record and public key, means to determine that – (a) the digital signature was generated using the private key corresponding to the public key listed in a certificate; and (b) the electronic record has not been altered since its digital signature was generated and any reference to a digital signature being verifiable is to be construed accordingly.

3 GENERAL RESPONSIBILITIES OF A RECOGNIZED CERTIFICATION AUTHORITY

3.1 A recognized CA shall comply with the conditions attached by the GCIO to the recognition granted under section 21 or renewed under section 27 of the Ordinance.

3.2 A recognized CA may appoint agents or subcontractors to carry out some or all of its operations provided that:

- the agents or subcontractors are equally capable of complying with this Code of Practice relevant to their operations, and

- the recognized CA is and remains responsible for the activities of its agents or subcontractors in the performance or purported performance by them of the functions, powers, rights and duties of the recognized CA under the Ordinance.

3.3 A recognized CA shall take all reasonable care in issuing certificates to its subscribers and shall take all reasonable care to persons who may rely upon these certificates.

3.4 A recognized CA shall furnish the GCIO with a copy of its certification authority certificate (CA certificate) that it uses to sign its recognized certificates. The GCIO shall publish the CA certificate in the certification authority disclosure record maintained by the GCIO for that CA. The disclosure record serves as an additional means for making the CA certificate available to persons who need to verify the validity of the recognized certificates issued by that CA for at least 7 years after the concerned CA has terminated its service.

3.5 Where the Code of Practice requires a recognized CA to record, retain or archive information and records, the recognized CA shall do so for a period of at least 7 years or such longer or shorter period as may be specified by the GCIO and in a manner that ensures the security, integrity and accessibility of the information and records for retrieval and inspection.

3.6 A recognized CA shall comply with all applicable ordinances and regulations regarding the privacy of personal data. In particular, a recognized CA shall:

(a) set out its privacy policy in respect of the collection, holding and use of personal data of data subjects (e.g. applicants of its certificates and subscribers);

(b) give a written Personal Information Collection Statement to data subjects before or upon the collection of personal data from the data subjects;

(c) include a purpose statement (e.g. in its repository or certification practice statement as appropriate) defining the purpose(s) of keeping its repository and the permitted use of personal data contained therein; and

(d) as a minimum requirement to ensure compliance with all applicable ordinances and regulations regarding the privacy of personal data, conduct a self-assessment in accordance with the "Privacy Compliance Self-Assessment Kit" or any document of a similar nature published by the Office of the Privacy Commissioner for Personal Data. Such a self-assessment shall be conducted by the recognized CA regularly or whenever there is major changes in its operation affecting its handling of personal data of data subjects.

3.7 A recognized CA shall refrain from engaging in restrictive practices that impair economic efficiency or free trade.

3.8 If a recognized CA issues to the public both recognized certificates and certificates which are not recognized certificates, the recognized CA shall publicize in its certification practice statement(s) and repository the fact that it issues these two categories of certificates. The fact so publicized by the recognized CA shall clearly identify which particular certificate(s) or type(s), class(es) or description(s) of certificates issued by it are recognized under the Ordinance and which are not.

3.9 A recognized CA shall take care of the needs of persons with disabilities in the provision of its services in accordance with all applicable ordinances and regulations regarding the prevention of any discriminatory practice against any person with disabilities.

4 CERTIFICATION PRACTICE STATEMENT

4.1 A recognized CA shall publish for public knowledge and maintain up to date certification practice statement(s) (CPS) for the types, classes or descriptions of recognized certificates that it issues.

4.2 A recognized CA shall state in its CPS(s) the liabilities, limitations on liability, rights and obligations of the recognized CA, its subscribers and persons who rely on the certificates issued by the recognized CA, and the significance of its reliance limit on its certificates. A recognized CA shall draw the attention of its subscribers and persons who may rely on its certificates to such liabilities, limitations, rights and obligations and the significance of its reliance limits by:

- specifying separately as appropriate such information in any contract with its subscribers; and
- making such information available, both in printed form and in electronic form via an on-line and publicly accessible means.

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

4.4 A recognized CA shall draw the attention of its subscribers and persons who may rely upon those of its certificates which are not recognized certificates to the significance of using and relying upon those certificates.

4.5 A recognized CA shall draw the attention of applicants of its certificates to the extent that their personal data will become public information when such data are

incorporated in recognized certificates issued by the recognized CA to them and published in a repository of the recognized CA. Its CPS(s) shall state clearly the contents of the relevant recognized certificates.

4.6 A recognized CA shall submit a copy of its CPS(s) to the GCIO upon publication of the CPS(s), and notify the GCIO in writing of any subsequent changes to the CPS(s) as soon as practicable. A recognized CA must also record all changes made to the CPS(s) together with the effective date of each change as soon as practicable.

4.7 If a recognized CA issues a type, class, or description of recognized certificates that are specified in a certificate policy, then the certificate policy will be considered as part of the CPS.

4.8 A recognized CA shall retain a copy of each version of the CPS(s) it has issued, together with the date the CPS(s) come into effect and the date the CPS(s) cease to have effect if applicable.

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

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

4.11 The standards and procedures regarding the contents of a CPS are set out in Appendix 1.

4.12 Before a recognized CA effects any intended material change to its operation or CPS that corresponds to one or more types, classes or descriptions of recognized certificates that the recognized CA issues, the recognized CA shall inform details of the change in writing to the GCIO. The GCIO will consider whether the intended material change complies with relevant provisions of the Ordinance and this Code of Practice, and may require the recognized CA to furnish to the GCIO an assessment report and/or a statutory declaration in respect of the material change in accordance with paragraphs 12.1(c) and 13.1(c) of this Code of Practice. Examples of material change to the operation of the recognized CA or its CPS include without limitation:

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

(b) changes in the reliance limit of the recognized certificates; or

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

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

5 TRUSTWORTHY SYSTEM

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

General Interpretation

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

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

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

Guiding Principles

5.5 In accordance with the technology-neutral and minimalist regulatory approach adopted under the Ordinance, a recognized CA is free to determine the technical solutions to support its operations.

5.6 Where there is a high risk on specific aspects of a recognized CA's operation, for example, those in relation to security sensitive functions, the recognized CA is expected to adopt systems and procedures that meet such standards as are widely accepted or recognized world-wide. In addition, as a matter of good practice, a recognized CA shall perform structured assessments to ascertain the underlying risks of its operations, and implement appropriate counter-measures for managing, mitigating and monitoring such risks.

Specific Areas for Consideration

5.7 A recognized CA operating in a public key infrastructure (PKI) shall make use of any hardware, software and cryptographic components. These components shall be supported by appropriate security policies and procedures in order to ensure that the recognized CA operates in a secure environment.

5.8 The manner in which a recognized CA achieves its objective in maintaining a trustworthy system may vary, depending on the kind of services to be provided by the recognized CA, the state of technology and the business environment. A recognized CA shall adhere to the following generally accepted good practices.

Generally Accepted Industry Good Practices

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

Generally accepted security principles

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

(a) Asset classification and management

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

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

(b) Personnel security

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

- defining roles and responsibilities within formal job descriptions having regard to its security policies;
- performing verification checks on its personnel in accordance with its security policies and procedures; and
- incorporating confidentiality or similar clauses within formal terms and conditions of employment contracts.

(ii) A recognized CA shall provide appropriate and adequate training to its personnel, with the aim of maintaining their competency and ensuring effective implementation of and compliance with its security policies. Training may include without limitation:

- appropriate technical training;
- organisational policies and procedures; and
- procedures to deal with security incidents and notify senior level of management of major security incidents.

(iii) A recognized CA shall establish appropriate controls to monitor the performance of its personnel including, for example:

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

(c) Physical and environmental security

(i) A recognized CA shall maintain effective physical and environmental security controls including without limitation :

- identifying and defining secure areas, and implementing security controls as appropriate for securing such areas;
- establishing formal procedures for access to such areas by staff of the recognized CA as well as by visitors;

- establish appropriate security and access monitoring mechanisms, with specific attention to those areas where the recognized CA stores its security-sensitive equipment;

- establishing appropriate controls to safeguard its equipment against environmental threats and hazards, such as fire, flood, power failures, etc, as well as against opportunity for unauthorised access;

- establishing general security controls, such as clear desk policy and general controls over equipment, information and other assets belonging to the recognized CA; and

- ensuring that its environmental control mechanisms are maintained and reviewed on a regular basis.

(ii) Where a recognized CA relies on services provided by third parties for the protection of physical and environmental security, such services shall be stated in formal service agreements established with these third party suppliers.

(d) Management over systems access

A recognized CA shall develop, establish, maintain and update effective controls and procedures over access to its information systems, including application systems, that are appropriate to the sensitivity and criticality of the systems being protected, including without limitation:

- establishing proper business requirements for controlling access to systems;

- establishing formal user responsibilities;

- establishing formal procedures for the management of user identification profiles and monitoring of access to its systems, including for example:

  – allocating, amending and revoking user access rights; and

  – the monitoring of access attempts through logging or similar means;

- establishing proper controls over access to networks, operating systems, and application systems, such as firewalls, router filters, etc;

- establishing proper procedures and controls over the monitoring of system access and usage;

- establishing proper procedures and controls over mobile computing and teleworking;

- establishing proper procedures and controls against unauthorised or illegal usage of software; and

- establishing proper procedures to deal with security incidents concerning access to networks, operating systems, and application systems.

Operational management

5.9.2 A recognized CA shall maintain effective controls and procedures in respect of its day-to-day operations. Operational policies and standard operating procedures shall be formalised and documented, including without limitation the following aspects:

- clear definition of duties and responsibilities of its operational personnel;

- regular capacity monitoring procedures to monitor system performance and identify performance bottlenecks;

- proper procedures to protect its computing infrastructure against malicious programs, such as viruses, etc.;

- proper procedures over systems and network management, including housekeeping tasks such as backup and archiving;

- proper procedures over the handling, distribution, storage and disposal of electronic information and media; and

- proper procedures for handling and resolving operational problems.

Development and maintenance of computer systems

5.9.3 A recognized CA shall develop, establish, maintain and update effective controls and procedures over system development and maintenance activities, including for example:

- establishing proper internal standards to ensure uniformity of development work, whether conducted by the staff of the recognized CA or by outside parties in the case of outsourcing;

- procedures to ensure segregation of the production and development environments;

- procedures to ensure segregation of duties between operational and development personnel;
- controls over access to data and systems held in its production and development environments;
- controls over change control process, including emergency changes to systems and/or data; and
- procedures for the proper management in respect of the acquisition of equipment and services.

Continuity of business operations

5.9.4 A recognized CA shall develop, establish, maintain and update a business continuity plan that covers all critical aspects of its operations.

5.9.5 The continuity plan shall be tested vigorously on a regular basis, involving relevant key personnel detailed in the plan. Wherever possible, such tests shall be independently observed.

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

Maintenance of appropriate event journals

5.9.7 A recognized CA shall maintain adequate event journals, which includes the retention of documents related to the issuing and managing of recognized certificates by the recognized CA.

5.9.8 A recognized CA shall archive such event journals. It shall also regularly review the event journals and take action against any exceptions identified.

5.9.9 A recognized CA shall maintain journals relating to all major events including without limitation:

- access to materials and equipment used for key generation;
- in respect of keys and certificates, their generation, issuance, distribution, storage, backup, suspension, revocation, withdrawal, archival, destruction, and other related events;
- security incidents, including key compromise; and

- procurement, installation, implementation, decommission and retirement of cryptographic devices.

Compliance monitoring and assurance

5.9.10 A recognized CA shall develop, establish, maintain and update appropriate controls to ensure compliance with applicable legal, regulatory and technical requirements including without limitation:

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

- ensuring that its compliance monitoring function meets the current industrial standards and practices; and

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

Good Practices Specific to Functions of a Recognized CA

5.10 A recognized CA shall develop, establish, maintain and update formally documented and approved policies, procedures and practices over specific functions of a recognized CA, including without limitation the areas discussed in the following sub-paragraphs.

Management of certification practice statement

5.10.1 A recognized CA shall disclose its business practices in its CPS(s) and maintain effective controls over its CPS(s) including without limitation:

- forming a management committee with the authority and responsibility for determining and approving the contents of CPS(s), including any certificate policy or policies that are adopted by the recognized CA;

- establishing effective procedures for the on-going review and updating of the CPS(s); and

- making the CPS(s) available to its subscribers and persons who may rely on the recognized certificates issued by that recognized CA.

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

5.10.2 A recognized CA shall maintain effective procedures to monitor and ensure compliance with all legal and regulatory requirements, including relevant provisions in the Ordinance, the Regulations thereunder and this Code of Practice.

Key management

5.10.3 A recognized CA shall maintain effective procedures and controls over the generation, storage, backup, recovery, distribution, use, destruction, and archiving of the recognized CA's own keys including without limitation:

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

- operational controls over key generation including without limitation:

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

  – procedures to ensure the keys are generated by authorised personnel in a controlled manner;

- controls over key storage, backup and recovery including without limitation:

  – regular and vigorous testing of the recognized CA's recovery procedures;

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

  – procedures to ensure that the backup of recognized CA's private key is securely performed under dual control, and that backup copies of the recognized CA's private key shall be kept in a secure manner;

- controls over security for the key distribution process including without limitation:

  – procedures to ensure the integrity and authenticity of the public key of the recognized CA which the recognized CA provides to the GCIO for deposit in the CA disclosure record maintained by the GCIO for that recognized CA; and

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

- controls over the usage of the key, including the procedures for activating the key; for example:

  - more than one responsible officer is required to activate the private key of the recognized CA; and

  - the recognized CA's private key shall only be activated if proper authority for an intended purpose in a prescribed manner is obtained;

- controls to ensure the safe destruction of key pairs and any related devices including procedures that ensure destruction of all copies of private keys (so that they cannot be recovered or reconstructed after destruction) and revocation of the corresponding public keys; and

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

Management of key generating devices

5.10.4 A recognized CA shall maintain effective procedures and controls over the procurement, receipt, installation, acceptance tests, commissioning, usage, repair, maintenance, and retirement of key generating devices. Control examples include:

- procedures for ensuring the integrity of the cryptographic module;

- procedures for ensuring that the handling of key generating device is under proper supervision by authorised personnel to prevent the device from being tampered with; and control mechanism established to ensure that the cryptographic modules cannot be tampered with without being detected; and

- procedures for ensuring that the strength of keys generated using the cryptographic modules is of the appropriate strength for the purpose of the keys for both the recognized CA and its subscribers.

Key management services provided by the recognized CA (where appropriate)

5.10.5 A recognized CA shall maintain effective procedures and controls over key management services, if any, provided by the recognized CA to its subscribers, such as key generation, storage, backup, recovery, destruction and archival. Such procedures and controls shall be consistent with the principles set out in paragraphs 5.10.3 and 5.10.4 of this Code of Practice. Where subscriber key pairs are generated by the recognized CA, procedures shall be established to ensure that the private key is delivered to the applicant of the certificate in a secure manner

without being tampered with; the recognized CA shall not maintain a copy of the subscriber's private key without the written consent of the subscriber.

Lifecycle management of tokens (where appropriate)

5.10.6 A recognized CA shall maintain effective procedures and controls over the preparation, activation, usage, distribution, and termination of any tokens, such as smart cards, used by the recognized CA.

Certificate management

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

- before issuing or renewing a recognized certificate, a recognized CA shall verify the identity of the person who applies to the recognized CA for the issuance or renewal of a recognized certificate in accordance with procedures stated in the relevant CPS; the recognized CA shall also verify the uniqueness of the person's distinguished name;
- there shall be appropriate procedures to notify the subscribers the need to renew their certificates prior to the expiry of their certificates;
- a recognized CA shall adopt an open and common interface for the issuance of its recognized certificates; the format of the certificate shall be stated in the relevant CPS;
- there shall be proper policies and procedures to ensure that the performance of the repository of a recognized CA meets the service levels set out by the recognized CA in its CPS in respect of the repository; and
- a recognized CA shall set out in its CPS the procedures for handling complaints from subscribers.

Management of the publication of certificate revocation information

5.10.8 A recognized CA shall maintain effective procedures and controls over the management of its publication of certificate revocation information, such as through its certificate revocation list and any other means of publishing certificate revocation information. For example:

- a recognized CA shall update its certificate revocation list and any other means of publishing certificate revocation information in accordance with the policies, procedures and arrangements stated in its CPS; and

- there shall be procedures to ensure that only authorised personnel have access to the repository, the certificate revocation list and any other means of publishing certificate revocation information for their maintenance.

Key Generation Using a Trustworthy System and Keeping of Records

5.11 A recognized CA shall use a trustworthy system to generate key pairs of its own as well as for its subscribers. Where an applicant of any of its recognized certificates generates his key pair using his own system, the recognized CA shall request the applicant to use a trustworthy system for generation of the applicant's key pair. The recognized CA shall provide guidelines to the applicant and shall take reasonably practicable steps to ascertain the applicant's compliance with the guidelines in relation to the use of a trustworthy system by the applicant for the generation of his key pair. The recognized CA shall not accept the applicant's key pair if the applicant fails to comply with its guidelines or otherwise fails to use a trustworthy system for the generation of the key pair.

5.12 A recognized CA shall separately keep its own private key and the activation data (e.g. PINs, passwords, etc.) in a secure manner.

5.13 A recognized CA shall make and retain records in respect of:

- activities relating to the issuance, renewal, suspension and revocation of recognized certificates (including the identification documents of any person applying for a recognized certificate from the recognized CA);
- the publication of certificate revocation information, such as the certificate revocation list and any other means of publishing certificate revocation information;
- the documents relating to the generation of the recognized CA's own key pair;
- the documents relating to the generation of the subscribers' key pairs; and
- the administration of the recognized CA's computer facilities.

5.14 A recognized CA shall archive all recognized certificates issued by it and maintain mechanisms to access such certificates.

Digital Signatures

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

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

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

Matters Affecting a Trustworthy System

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

- inform the GCIO immediately in respect of the incident;
- use all reasonable endeavours to notify all persons who are or who will be affected by that incident; and
- act in accordance with the procedures, if any, specified in the CPS governing such an incident.

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

5.18 A recognized CA shall ensure that all its responsible officers and those officers with trusted roles such as security officers, CA administrators, privileged system operators, registration personnel, and any other personnel that have access to key material, cryptographic modules, or activity event logs shall be fit and proper persons.

Security and Risk Management

5.19 A recognized CA shall adopt a security policy in accordance with generally accepted security principles.

5.20 A recognized CA shall establish a comprehensive security incident reporting and handling procedure, and disaster recovery set-up and procedure for its operation.

5.21 A recognized CA shall adequately identify and establish procedures to deal with the risks associated with its operation. It shall implement a risk management plan that will provide for the management of, including without limitation, the following incidents:

- key compromise;
- security breach of the system or network of the recognized CA;
- unavailability of the infrastructure of the recognized CA; and

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

6 CERTIFICATES AND RECOGNIZED CERTIFICATES

6.1 A recognized CA may issue recognized certificates or certificates which are not recognized certificates. Where a recognized CA issues both recognized certificates and certificates which are not recognized certificates, it shall use separate private keys to sign the two streams of certificates respectively.

6.2 Recognized certificates shall contain the necessary information to facilitate subscribers and persons who rely on the certificates to locate the associated CPS during the conduct of electronic transactions.

Issuance of Certificates

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

(a) has received a request for issuance of the recognized certificate from the person applying for such a certificate; and

(b) has complied with all of the practices and procedures set out in the CPS including procedures regarding identity verification of the person in respect of that type, class or description of recognized certificates.

6.4 A recognized CA shall provide a reasonable opportunity to the applicant of any of its recognized certificates to verify the information on the applicant that is included or to be included in the certificate. Information on the applicant means information supplied by the applicant that the recognized CA includes or will include in the certificate. Furthermore, the recognized CA shall take all reasonably practicable steps to ensure accuracy of the information included or to be included in the certificate.

6.5 A recognized CA shall publish recognized certificates that it issues and that are accepted by its subscribers in the on-line and publicly accessible repositories maintained by it or maintained for it by one or more third parties. If a recognized CA issues to the public both recognized certificates and certificates that are not recognized certificates, the recognized CA shall use separate repositories to publish these two categories of certificates.

6.6 A recognized CA shall obtain the consent of applicants of its recognized certificates in respect of any personal data of the applicants which the CA intends to include in the certificates that are to be issued to the applicants and to be listed in an on-line and publicly accessible repository.

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

6.8 A recognized certificate shall state when its validity expires.

6.9 By issuing a recognized certificate, a recognized CA represents to any person who reasonably relies on the recognized certificate or a digital signature verifiable by a public key listed in the recognized certificate that the recognized CA has issued the recognized certificate in accordance with its applicable CPS.

6.10 All transactions related to the issuance of a recognized certificate including the date and time shall be recorded.

Suspension and Revocation of Recognized Certificates

6.11 A recognized CA shall be able to revoke and may also be able to suspend recognized certificates in accordance with the following paragraphs.

6.12 A recognized certificate shall contain or incorporate by reference necessary information to locate or identify the repository or repositories in which suspension or revocation notices of the recognized certificate will be published.

6.13 Unless a recognized CA and its subscriber otherwise agree, the recognized CA that issues a recognized certificate to the subscriber shall suspend or revoke the certificate within a reasonable time after receiving a request from:

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

(b) a properly authorised person.

6.14 Within a reasonable time following suspension or revocation of a recognized certificate by a recognized CA, the recognized CA shall publish a notice of the suspension or revocation (e.g. certificate revocation list signed by the recognized CA or any other means of publishing the suspension or revocation information) in a repository maintained by it or by an outside organisation for the recognized CA.

6.15 The exact time of the revocation or suspension by the recognized CA as well as the allocation of liability for transactions using the certificate in the period between the receipt of the request for revocation or suspension and the time when the certificate is revoked or suspended shall be agreed between the recognized CA and the subscriber.

6.16 A recognized CA may temporarily suspend a recognized certificate that it has issued if the recognized CA has reasonable grounds to believe that the recognized

certificate is unreliable, regardless of whether the subscriber consents to the suspension; but the recognized CA shall complete its investigation regarding the reliability of the recognized certificate and decide within a reasonable time period whether to reinstate the certificate or to revoke the certificate.

6.17 If the recognized CA considers that an immediate revocation of a recognized certificate issued by it is justified in the light of all the information available to it, the certificate shall be revoked, regardless of whether the subscriber has given consent to the revocation.

6.18 In the case of suspension requested by the subscriber or a properly authorised person, the recognized CA shall check with the subscriber or that properly authorised person whether the recognized certificate to be suspended shall be revoked or reinstated after suspension. The relevant CPS shall state the action to be taken in the event that it is not possible for the recognized CA to contact the subscriber or the properly authorised person for his instruction of whether the suspended certificate shall be revoked or reinstated after suspension.

6.19 Whenever a recognized CA suspends or revokes a recognized certificate which is issued by it, the recognized CA shall, within a reasonable time, notify the suspension or revocation of the recognized certificate and provide a record to the subscriber of the recognized certificate or the properly authorised person.

6.20 A recognized CA shall provide hotline or other facilities for subscribers to report to the recognized CA incidents affecting their certificates or private keys, for example, keys having been lost or compromised.

6.21 All transactions, including the date and time, in relation to suspension or revocation of certificates shall be recorded.

Renewal of Recognized Certificates

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

6.23 All transactions including the date and time in relation to the renewal of a recognized certificate shall be recorded.

7 VERIFICATION OF SUBSCRIBER'S IDENTITY

7.1 A recognized CA shall specify in the relevant CPS that corresponds to a particular type, class or description of recognized certificates the procedure to verify the identity of a person who applies for such a recognized certificate from the recognized CA.

7.2 A recognized CA shall retain copies of the documentary evidence that identifies its subscribers.

8 RELIANCE LIMIT AND LIABILITY COVER

8.1 In issuing a type, class or description of recognized certificates to subscribers, a recognized CA may specify in the relevant CPS that corresponds to that type, class or description of certificates a reliance limit on the certificates. A recognized CA shall specify in the relevant CPS the significance of the reliance limit on the use of the recognized certificates.

8.2 A recognized CA shall arrange suitable insurance or other forms of cover to ensure that it is capable of covering potential liabilities arising from or related to issuance and use of recognized certificates. Specifically, the recognized CA shall provide evidence that it has acquired insurance cover against claims arising from its error or omission, with a minimum limit of indemnity in relation to each and every single claim during the period of insurance of not less than –

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

(b) $200,000;

whichever is higher. Moreover, in each insurance policy acquired by the recognized CA for this purpose, the total insurance cover for aggregated claim amount in respect of those recognized certificates covered under the insurance policy in any one insurance period of 12 months shall be set at 10 times the amount of (a) or (b) whichever is higher. Such liability cover shall be in place at all times and shall cover all type, class or description of recognized certificates issued by the recognized CA. Should the recognized CA choose to put in place other forms of liability cover, the same minimum limit of indemnity shall be provided for. Any such other forms of liability cover shall be administered by an independent third party. The recognized CA shall seek approval from the GCIO before putting any such other forms of liability cover into effect.

8.3 An insurance policy acquired by a recognized CA shall be:

(a) issued by an insurer authorized to carry out the pertinent insurance business in the Hong Kong Special Administrative Region under the Insurance Companies Ordinance (Cap. 41), including Lloyd's; and

(b) governed by and construed in accordance with laws of the Hong Kong Special Administrative Region.

In addition, both the recognized CA and the insurer shall agree to submit to the non-exclusive jurisdiction of the courts of the Hong Kong Special Administrative Region as regards any claim or matter arising under the insurance policy.

8.4 In respect of claims arising from error or omission of a recognized CA, the recognized CA shall maintain procedures which prescribe the documentation requirements supporting the process of submitting the claims.

9 REPOSITORIES

9.1 A recognized CA shall make available at least one on-line and publicly accessible repository for the publication of recognized certificates and related information. It shall ensure that its repository or repositories are implemented through trustworthy systems. The recognized CA shall state in its CPS(s) the service levels in respect of the operation of its repository or repositories.

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

9.3 A repository of a recognized CA shall contain :

- recognized certificates issued by the recognized CA;
- suspension or revocation notices of its recognized certificates (including certificate revocation lists or any other means of publishing the suspension or revocation information as appropriate);
- the CA disclosure record for that recognized CA; and
- other information as specified by the GCIO.

9.4 A repository of a recognized CA shall not contain any information which the recognized CA knows to be inaccurate or unreliable.

9.5 A recognized CA shall keep in its repository an archive of recognized certificates that have been suspended or revoked, or that have expired within at least the previous seven years.

10 DISCLOSURE OF INFORMATION

10.1 A recognized CA shall publish in its repository or repositories:

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

(b) the suspension, revocation or non-renewal notice of its CA certificate or recognition granted by the GCIO; and

(c) any other fact that materially and adversely affects either the reliability of a recognized certificate that the recognized CA has issued or its ability to perform its services relevant under the Ordinance.

10.2 A recognized CA shall inform the GCIO 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 recognized CA shall submit progress reports to the GCIO at 6-month intervals containing information with regard to:

(a) the number of its subscribers classified by type, class or description of certificates;

(b) the number of certificates issued, suspended, revoked, expired and renewed by type, class or description of certificates;

(c) its performance compared with its stated service levels;

(d) new types, classes or descriptions of certificates issued;

(e) changes in its organisational structure or systems;

(f) actions taken by the recognized CA to address recommendation(s) made or exception(s) or deficiency(ies) identified in the assessment report which is prepared and submitted to the GCIO under section 20(3)(b), 27(5A)(b), 43(1)(a) or 43A(1)(c) of the Ordinance, and

(g) any changes related to the above items since the preceding progress report was submitted or since the application for recognition or renewal as a recognized CA.

10.4 A recognized CA shall report to the GCIO immediately any material changes in the above information. The GCIO may also call for such report as well as other information relevant under the Ordinance at any time by giving a reasonable notice.

10.5 A recognized CA shall report to the GCIO immediately when the recognized CA realises that there is an event which may or will lead to potential conflict of interest in respect of the operation of the recognized CA.

10.6 A recognized CA shall report any incident that materially and adversely affects its operation to the GCIO immediately.

10.7 On submission by a recognized CA of any report or information under the Ordinance or the Code of Practice, the recognized CA shall ensure that it has the necessary rights over such report or information so that it can grant or procure the grant of a licence to the GCIO for the GCIO to reproduce and publish the whole or any part of the report or information for the purposes of the Ordinance. Upon request by the GCIO, the recognized CA shall grant or procure the grant of the aforesaid licence to the GCIO. The recognized CA shall at its expense do such thing and execute such document (or procure the same to be done or executed) as may be required by the GCIO to give effect to the aforesaid licence.

10.8 A recognized CA agrees to the disclosure of any such report or information by the GCIO as the GCIO thinks fit for the purposes of the Ordinance.

10.9 A recognized CA shall not attempt in any way to prevent the GCIO from publishing any information for the purposes of the Ordinance.

11 TERMINATION OF SERVICE

11.1 A CA shall submit to the GCIO a termination plan when the CA applies for recognition as a recognized CA. A recognized CA shall submit to the GCIO an updated termination plan when it applies for renewal of its recognition or when requested by the GCIO by the time specified in a notice issued by the GCIO to the recognized CA.

11.2 The termination plan shall specify the arrangements for the termination of the recognized CA's service, especially the arrangement for its records, including the certificates which it has issued and its CA certificate, to be archived for not less than 7 years.

11.3 The termination plan shall cover both voluntary and involuntary termination of the recognized CA's service including the expiry or revocation of the recognition granted by the GCIO to the recognized CA. The termination plan shall also include measures to ensure that the interests of the subscribers are safeguarded upon termination of the recognized CA's service.

11.4 Any CPS published by a recognized CA must refer to the termination plan of the CA.

11.5 Before a recognized CA’s service is terminated , the recognized CA shall

(a) inform the GCIO of its intention to terminate service at least 90 days before the termination of its service;

(b) inform all its subscribers of its intention at least 60 days before the termination of its service;

(c) advertise such intention in one English language daily newspaper and one Chinese language daily newspaper in circulation in the Hong Kong Special Administrative Region for at least three consecutive days at least 60 days before the termination of its service;

(d) if considered necessary by the GCIO, make arrangements to revoke all certificates which remain not revoked or expired, regardless of whether the subscribers have requested for the revocation, when it terminates its service; and

(e) make appropriate arrangements to effect an orderly transfer of information contained in the recognized CA's repository, including details of certificates issued by the recognized CA and the recognized CA's public key(s). The transfer of information shall be made to a custodian who shall maintain the information for not less than 7 years from the date on which the recognized CA terminates its service or the transfer of information is effected whichever is later. Such information to be maintained by the custodian shall only be used for purposes that are consistent with the original services provided by the recognized CA. The public should be informed of the means and procedures to access the information.

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

12.1 A recognized CA shall submit to the GCIO a report

(a) at least once in every 12 months, containing an assessment as to whether the recognized CA has, for the period to which the report relates, complied with such provisions of the Ordinance and of this Code of Practice as are specified under paragraph 1 of Appendix 2;

(b) when the recognized CA applies for renewal of recognition, containing an assessment as to whether the recognized CA is and is capable of complying with such provisions of the Ordinance and of this Code of Practice as are specified under paragraph 1 of Appendix 2; and

(c) when required by the GCIO in relation to major changes of the recognized CA, containing an assessment as to–

– whether**,** having regard to the major changes that have occurred, the recognized CA is and is capable of complying; or

– whether, having regard to the major changes that will occur, the recognized CA is capable of complying

with such provisions of the Ordinance and of this Code of Practice as are specified under paragraph 3 of Appendix 2.

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

- independent of the recognized CA under assessment;
- accredited by a recognized professional organisation or association; and
- proficient in:
  - the assessment of public key infrastructure and related technologies, such as digital signature and certificate, etc;
  - applying information security tools and techniques;
  - performing financial reviews;
  - performing security reviews; and
  - performing third-party reviews.

12.3 The qualified person may be an individual possessing all of the above requirements, or a partnership or an organisation comprising individuals that collectively possess all of the above requirements. The individual signing the assessment report shall:

- be a registered member of the recognized professional organisation or association, e.g. holding a valid practising certificate or attaining a similar status;
- have overall responsibility for ensuring that the person(s) performing the assessment possess sufficient knowledge of the subject matter, such as digital signature and certificate, public key infrastructure, financial matters, etc.; and
- have overall responsibility for ensuring the quality of the assessment and adherence to any standards or practices adopted for the purpose of performing such assessments.

12.4 The following person who meets the requirements set out in paragraphs 12.2 and 12.3 above may apply to the GCIO for approval as the person qualified to conduct the assessment:

(a) a Certified Public Accountant, i.e. a professional accountant with a practising certificate issued under the Professional Accountants Ordinance (Cap. 50); or

(b) a Corporate Member in the Information Discipline of the Hong Kong Institution of Engineers who is also a Registered Professional Engineer under the Engineers Registration Ordinance (Cap. 409) in the same discipline.

The GCIO may also approve applications submitted by other persons as being qualified to conduct the assessment.

12.5 The professional organisation or association referred to in paragraph 12.2 must have an established system to properly admit and regulate its members. The key features of such a system shall include without limitation:

- rules and regulations that govern membership admission requirements, such as in respect of training, competency testing, fitness for membership;
- rules and regulations that govern professional and ethical standards and guidelines to members that govern the performance of their professional services, such as in respect of conflict of interest, undertaking and accepting instructions;
- mechanism for enforcing the professional and ethical standards and monitoring the conduct of members including without limitation formal disciplinary procedures, quality assurance measures such as peer reviews; and
- mandatory continuing professional education requirement.

12.6 With regard to an assessment report referred to in sub-paragraph 12.1(a), a copy of the report shall be submitted to the GCIO by the recognized CA within 4 weeks of the completion of the assessment. With regard to an assessment report referred to in sub-paragraph 12.1(b), the recognized CA shall submit to the GCIO a copy of the report of the assessment which is completed within 4 weeks prior to the date of the application for renewal by the recognized CA. With regard to an assessment report referred to in sub-paragraph 12.1(c), the GCIO may specify in the notice given in respect of the major changes to the recognized CA the period of time within which the recognized CA shall furnish the report to the GCIO.

12.7 When a recognized CA submits an assessment report to the GCIO, the recognized CA shall at the same time furnish the GCIO with its response to any exception(s), deficiency(ies) or recommendation(s) raised by the qualified person in the assessment report.

12.8 Failure to meet the requirements as stated in the Ordinance, the Regulations thereunder and the Code of Practice may be a ground for suspending or revoking the recognition granted by the GCIO to a recognized CA or for rejecting a recognized CA's application for renewal of its recognition by the GCIO.

13 DECLARATION OF COMPLIANCE WITH THE ORDINANCE AND THIS CODE OF PRACTICE

13.1 A recognized CA shall submit to the GCIO a statutory declaration–

(a) at least once in every 12 months, stating whether the recognized CA has, for the period to which the statutory declaration relates, complied with such provisions of the Ordinance and of this Code of Practice as are specified under paragraph 2 of Appendix 2;

(b) when the recognized CA applies for renewal of recognition, stating whether the recognized CA is and is capable of complying with such provisions of the Ordinance and of this Code of Practice as are specified under paragraph 2 of Appendix 2; and

(c) when required by the GCIO in relation to major changes of the recognized CA, stating–

- whether**,** having regard to the major changes that have occurred, the recognized CA is and is capable of complying; or

- whether, having regard to the major changes that will occur, the recognized CA is capable of complying

with such provisions of the Ordinance and of this Code of Practice as are specified under paragraph 3 of Appendix 2.

13.2 A recognized CA shall ensure that the statutory declaration is made, at the expense of the recognized CA, by a responsible officer of the recognized CA.

13.3 With regard to a statutory declaration referred to in sub-paragraph 13.1(a), the statutory declaration shall be submitted to the GCIO by the recognized CA within 4 weeks of making the statutory declaration. With regard to a statutory declaration referred to in sub-paragraph 13.1(b), the recognized CA shall submit to the GCIO the statutory declaration which is made within 4 weeks prior to the date of the application for renewal by the recognized CA. With regard to a

statutory declaration referred to in sub-paragraph 13.1(c), the GCIO may specify in the notice given in respect of the major changes to the recognized CA the period of time within which the recognized CA shall furnish the statutory declaration to the GCIO.

14 ADOPTION OF STANDARDS AND TECHNOLOGY

14.1 A recognized CA shall continuously review and, where appropriate, improve and update its standards and technology in order to uphold the confidence that its subscribers place in it and to protect the interests of the subscribers. The recognized CA shall

(a) establish defined policies, controls and procedures for the function of continuously reviewing and, where appropriate, updating its standards and technology;

(b) assign such function to specific organisational units within the recognized CA; and

(c) regularly re-assess the defined policies, controls and procedures and performance of the organisational units concerned.

15 INTER-OPERABILITY

15.1 To reduce barriers for digital signatures supported by recognized certificates to be widely accepted, a recognized CA shall, wherever applicable, adopt an open and common interface to facilitate the verification by others of digital signatures supported by its recognized certificates.

15.2 A recognized CA shall state in its CPS(s) the open and common interfaces that it supports and any inter-operability that it has established with other CAs.

16 CONSUMER PROTECTION

16.1 The advertisement of services by a recognized CA shall be decent, honest and truthful. Comparative advertising shall be fair and not misleading. All claims shall be capable of independent substantiation.

Appendix 1 – Standards and Procedures regarding the Contents of Certification Practice Statements

1 Introduction

The standards and procedures set out in this appendix are issued under section 33 of the Electronic Transactions Ordinance (Cap.553) (the Ordinance) by the Government Chief Information Officer (the GCIO). These standards and procedures are based on the IETF (Internet Engineering Task Force) RFC 2527 "Certificate Policy and Certification Practices Framework" commonly referred as "IETF PKIX Part 4". These standards and procedures set out the minimum standards which the GCIO expects recognized certification authorities (CAs) to adopt and to comply with when issuing their certification practice statements (CPSs[1]).

The following sections set out the minimum standards and procedures which a recognized CA is expected to meet.

2 Key Attributes and Introduction of a CPS

2.1 Key attributes

A recognized CA shall consider providing a summary of the key attributes relating to the type(s), class(es) or description(s) of certificates that it issues. The key attributes will enable subscribers of a recognized CA and parties which rely on the certificates to quickly gain an understanding of the relevant characteristics of the certificates issued under the CPS.

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

2.2 Introduction to a CPS

2.2.1 Overview

A recognized CA shall provide a high level summary of the purpose and scope of the CPS. This summary should set out, among others, the scope of the recognition granted under the Ordinance to it (including conditions attached to the recognition) and a general description of

[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 shall not be confused with Certificate Policies (CP) because they tend to differ in terms of authorship, purpose, level of specificity, and approach.

what such recognition means for both subscribers and relying parties. A recognized CA may also highlight the scope and the terms and conditions of its CA services.

2.2.2 Identification

A recognized CA shall provide the appropriate object identifier(s) of its CPS(s) if available. Where the recognized CA supports specific certificate policies (CPs) for recognized certificates issued under the CPS(s), the recognized CA shall identify those CPs and provide the appropriate object identifiers of the CPs if available in this section of the CPS. In addition, it shall ensure that the full text of the policies identified is posted in a location accessible on-line to subscribers and prospective subscribers.

2.2.3 Identification of parties involved in the operation and maintenance of certification services and scope of usage of certificates

A recognized CA shall identify all known groups or functions that form part of, or participate in, the operation and maintenance of its certification services. Examples may include the CA function, the registration function, repositories, and target end users (i.e. subscribers and relying parties). 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, a recognized CA shall also set out the limitations on the usage of each type, class or description of certificates issued by it, covering for example:

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

2.2.4 Contact details

A recognized CA shall provide at least one point of contact for handling enquiries from subscribers and relying parties on regulatory and other matters. Typically the recognized CA would state at least a telephone number, postal address and electronic mail address for subscribers and relying parties to contact the recognized CA. A recognized CA shall also provide information on reporting or hotline facilities for subscribers to report lost or compromised keys.

3 General Provisions

3.1 Obligations

3.1.1 Duties and obligations of a recognized CA

A recognized CA shall clearly state the duties and obligations it assumes as part of its service offerings, encompassing specific requirements set out in the Ordinance, including any conditions for its recognition, and this Code of Practice. Examples of such obligations 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 a recognized CA has outsourced any of its functions, the respective duties and obligations of these functions shall be separately described.

3.1.2 Duties and obligations of subscriber

A recognized CA shall describe the duties and obligations assigned to its subscribers including requirements set out in the CPs it 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 compromise or loss of private key.

3.1.3 Relying party's obligations

A recognized CA shall clearly state all representations made to relying parties in accordance with the CPS, including any CP it 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

A recognized CA shall clearly state the obligations it assumes in providing the repository service, encompassing specific requirements set out in the Ordinance, including any conditions for the CA's recognition, and this Code of Practice. Examples of such obligations include the timely publication of certificates and revocation (including certificate suspension as appropriate) information, and the terms of accessibility and availability of the repository.

3.2 Liability

A recognized CA shall clearly specify any applicable provisions regarding the allocation of liability including the handling of transactions that are supported by a certificate and that occur in between the time when the subscriber or his properly authorised person as defined in this Code of Practice requests the revocation or suspension of the certificate and the time when the recognized CA actually revokes or suspends the certificate.

A recognized CA shall also clearly specify the implications of each stated reliance limit. In any event, nothing in this section should be taken to exclude, or indemnify the recognized 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 a recognized CA issues, it shall 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 a recognized CA issues, it shall clearly specify the extent of liability that it covers (e.g. direct, indirect, special, consequential, incidental and liquidated damages) and any disclaimers and limitations on its obligations.

3.2.3 Loss limitations

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

3.3 Financial responsibility

A recognized CA shall specify aspects relating to its financial responsibilities and that of any other parties identified in the CPS. Areas that may be addressed include:

- whether any fiduciary relationships exist between any parties identified in the CPS or any other interested parties as a result of the act of issuance of certificates;
- financial responsibility for administrative processes ;
- financial assurances provided by the recognized 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

A recognized CA shall state the governing law and jurisdiction for it and the CPSs, subscriber agreements and relying party agreements.

3.4.2 Dispute resolution procedures

A recognized CA shall state the procedures established by it to resolve disputes and claims regarding its operations and representations to its subscribers or relying parties of the certificates it offers. The procedures shall state at a minimum the process of filing a dispute or claim with it and the steps it takes upon notification of a claim or dispute.

3.5 Fees

A recognized CA shall clearly state all costs and fees to subscribers and relying parties in respect of the issuance, revocation, suspension, retrieval, or the verification of status of certificates under each class, type or description of certificates it issued.

3.6 Publication and repositories

A recognized CA shall specify the policy and mechanism that it has implemented to provide its subscribers and relying parties with the information relating to its certificates, its CPS (including the details of any CPs that the recognized CA supports), and its current recognition status and the recognition status of the certificates it issues. A recognized CA should state, at a minimum, 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 a recognized CA and its components, shall be displayed prominently on the recognized CA's web page or other conveniently accessible locations.

Since the procedures followed by a recognized CA are expected to evolve, updates to the CPS shall be published as soon as practicable. All changes shall be prominently displayed at the same locations where the CPS is displayed and reported to the GCIO as soon as practicable.

3.7 Compliance assessments

A recognized CA shall state the mechanism and frequency for any compliance assessments relevant to it, including any mandatory requirements under the Ordinance and this Code of Practice. Specific aspects that may be covered include, for example:

- the frequency of compliance assessment for the recognized CA and any of its outsourced functions;
- the identity and qualifications of the independent assessor that carries out the assessment;
- the relationship between the assessor and the recognized CA;
- coverage of the compliance assessment; and
- policy concerning the communication of the compliance assessment results (i.e. who will receive copies of the report) and policy on follow up actions.

3.8 Confidentiality policy

A recognized CA shall specify its policy on maintaining confidentiality of information. Aspects that may be specifically addressed include, for example:

- types of information that must be kept confidential by the recognized CA, including any outsourced functions;
- types of information that are not considered confidential;
- the persons who 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;
- policy on release of records and information;
- conditions upon which the recognized CA, including any outsourced functions, may disclose records and information upon owner's request/consent; and
- any other circumstances under which confidential information may be disclosed.

As a general rule, recognized CAs shall comply with all applicable regulations regarding the privacy of personal data and the provisions of the CPS shall not contradict current privacy regulations within the Hong Kong Special Administrative Region and section 46 of the Ordinance.

3.9 Intellectual property rights

A recognized CA shall address the intellectual property rights of certificates, revocation/validity information of certificates, CPS, CPs, practice/policy specifications, names, and keys.

4 Identification and Authentication

A recognized CA shall set out the procedures used by it, or its outsourced registration function where appropriate, to authenticate applicants of its certificates prior to the issuance of certificates. Procedures for each class, type or description of certificates that a recognized CA issues shall be described.

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

A recognized CA shall specify the acceptable forms of identification such as the Hong Kong Identity Card, passports, articles of incorporation, business registration certificates, etc.

4.1 Initial Certification

A recognized CA shall set out the identification and authentication procedures and the naming conventions to be followed in the issuance of new certificates. A recognized CA shall cover the specific procedures that it follows in order to identify the certificate applicant, including the specific documents that an individual or organisation must produce prior to the recognized CA issuing a certificate to the applicant of the certificate.

4.1.1 Types of Names

A recognized CA shall specify the naming convention that its has adopted, such as X.500 Distinguished Names (DN) or other forms of names in the case of web site certificates. Alternate name forms including for example an electronic mail address or a personal identification number may be included to ensure that the certificate of a person can be unambiguously identified.

A recognized CA shall also 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

A recognized CA shall specify whether names within a certificate must be meaningful (i.e. using commonly understood semantics to describe the identity of the person or organisation) and if so, its 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

A recognized CA shall provide 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 recognized CA shall provide guidance to relying parties to reduce the risk of misinterpretation.

4.1.4 Uniqueness of names

A recognized CA shall make specification if names within certificates are required to be unique. If so, the recognized CA shall 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, a recognized CA shall specify its resolution procedures, as appropriate, concerning any naming conflicts.

4.1.6 Method to prove possession of private key

In cases where applicants of its certificates generate their own key pairs and remain in exclusive control of the private keys, a recognized CA must state how it verifies that the applicant's private key corresponds to the public key submitted for certification.

4.1.7 Authentication of subscriber identity

A recognized CA shall specify its procedures for ensuring that the name of the subscriber in a certificate is the name of the applicant of the certificate to whom the certificate will be issued. Where a recognized CA adopts specific procedures for verifying information on the applicant other than the name of the applicant that is placed or to be placed in the certificate, the recognized CA shall set out such specific procedures. The information will enable applicants to understand the requirements necessary for obtaining a digital certificate under the CPS and will enable relying parties to understand and draw conclusions as to the reliability of the certificates issued under the CPS.

4.2 Routine Rekey and Certificate Renewal

A recognized CA shall describe the procedures it adopts for routine rekey and certificate renewal, especially if such procedures for identification of the subscriber differ from those adopted for initial registration and issuance. A recognized CA shall state whether certificate renewal takes place without rekeying in its CPS.

4.3 Rekey after revocation

A recognized CA shall specify whether it will adopt a procedure different from that for initial certificate issuance when issuing a replacement for the certificate after its revocation.

4.4 Revocation request

A recognized CA shall specify the 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 allocation of liability between the recognized CA and the subscriber.

4.5 Suspension request

A recognized CA shall specify whether it supports the suspension of certificates, and if so shall detail the conditions for, as well as the effect of a suspension. It shall be specific about the implementation of suspensions and, if appropriate, address the same elements identified for revocations in section 4.4.

5 Operational Requirements

5.1 Certificate application

A recognized CA shall set out the details for applicants of certificates to apply for new certificates. The details shall include:

- the method of applying for a certificate and the documentation required to prove the identity of the applicants;

- information including, but not limited to, subscriber responsibilities, representations by the recognized CA, and terms and conditions for the certificates, the recognition status of the CA and of the certificates and what the recognition status means to the subscriber especially if the certificates are not recognized certificates; and

- the interface requirements for submitting the certificate requests.

5.2 Certificate issuance

A recognized CA shall set out the details on the specific process to be followed by it 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 applicant of the certificate, the public key must be delivered to the recognized CA with the certificate request and the recognized CA must verify that the applicant is in possession of the corresponding private key; if the keys are generated by the recognized CA, the private key must be securely delivered to the applicant and the recognized CA must indicate appropriate measures to ensure the proper handling of the keys in its possession);

- the recognized CA must not have possession of the subscribers' private keys without the written consent of the subscribers;

- the generation of the certificates;

- the delivery of certificates to the applicants; and

- the posting of the certificates to a repository.

5.3 Certificate acceptance

A recognized CA shall define the technical or procedural mechanism to:

- explain to applicants of certificates their responsibilities as subscribers as defined in section 3.1.2;

- inform the applicants that their certificates have been issued and the information on the applicants in the certificates;

- allow the applicants to accept or reject the certificates; and

- enable the applicants to obtain the certificates from it.

A recognized CA shall ensure that the applicants have the opportunity to verify the information on the applicants that is included or to be included in the certificates before accepting the certificates.

5.4 Certificate suspension and revocation

A recognized CA shall explain the procedures for suspending or revoking a certificate. A recognized CA shall set out the procedures for a subscriber or a properly authorised person to instruct it to suspend or revoke a certificate.

5.4.1 Suspension

A recognized CA shall 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, electronic mail or inclusion in a certificate revocation list or any other means of publishing the suspension information);
- the conditions, such as time limits, for recalling the suspension or moving from suspension to revocation;
- the time for the recognized CA to suspend a recognized 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 properly authorised person, and the time when the certificate is actually suspended;
- the expected time period within which the recognized CA checks with the subscriber or the properly authorised person whether the recognized certificate that was suspended should be revoked or should be reinstated after suspension; and
- the action the recognized CA takes in the event that it is not possible for it to contact the subscriber or the properly authorised person to ascertain the ultimate disposition of the suspended certificate.

5.4.2 Revocation

A recognized CA shall 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, electronic mail, inclusion in a certificate revocation list, updates to a revocation/validity information server, or any other means of publishing the revocation information); and

- the time for it to revoke a recognized 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 properly authorised person, and the time when the certificate is actually revoked.

The subscriber or a properly authorised person 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 requests of revocation of certificates by unauthorised parties. The means for transmitting the request shall be readily available to the subscriber and the properly authorised person such as electronic mail and web interfaces.

Typically, a certificate shall be revoked under the following circumstances:

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

- the subscriber is known to have violated the stipulations of the corresponding CPS;

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

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

5.4.3 Certificate revocation lists and other means of publishing revocation information

Certificate Revocation Lists (CRLs) specify the certificates that are issued by a recognized CA and that have been revoked and may give the reason why each certificate was revoked. A recognized CA shall state the mechanisms used to distribute the CRLs and how relying parties may access such lists. A recognized CA shall specify the frequency of updating CRLs.

A recognized CA may decide to use or support any other means of publishing certificate revocation information. It shall address the available mechanisms to access the information, the terms and conditions for their use, and the frequency of updating the information.

5.4.4 Checking requirements for CRL or other means of publishing revocation information

A recognized CA shall notify subscribers and post prominently in a location generally accessible that there are risks in relying on a digital signature if the certificate containing the public key used to verify the digital signature is no longer valid.

A recognized CA shall in addition specify, clearly and prominently, its policy concerning the situation where a relying party is temporarily unable to obtain information on revoked certificates (and also on suspended certificates if the recognized CA also publishes certificate suspension information through CRLs or its other means of publishing revocation information). It shall address specifically the allocation of liability that arises in such circumstances.

5.5 Security review procedures

A recognized CA shall describe event logging and review systems that are implemented by it for the purpose of maintaining a secure environment. Elements include the following:

5.5.1 Types of events recorded

A recognized CA shall describe the types of events to be recorded. At a minimum, it shall consider recording:

- administration of its computer facilities including without limitation:
  - 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 (including the identification documents of any person applying for a recognized certificate from the recognized CA), revocation, and suspension of certificates;
  - certificate renewals;
  - updates to repository(ies);
  - generation and posting of certificate revocation and suspension information;
  - CA key generation and rollover (and related documents);
  - generation of subscribers' key pairs (and related documents)
  - backups; and

- emergency key recoveries.

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

It is a good practice for the recognized 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 shall be recorded.

A recognized CA shall 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 shall be described by the recognized CA.

5.5.2 Frequency of processing event logs

A recognized CA shall specify the frequency with which the event logs are processed, e.g. consolidated and reviewed.

5.5.3 Retention period for event logs

A recognized CA shall specify the retention period for event logs, which shall conform to the requirements in this Code of Practice.

5.5.4 Protection of event logs

A recognized CA shall specify the mechanism in place to protect the event logs from accidental damage or deliberate modifications.

5.5.5 Event log backup procedures

A recognized CA shall specify the procedures for backing up the event logs, as well as the retention period for the backups. It is a good practice to ensure that the storage facility can afford 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

A recognized CA shall describe its policy relating to general records retention. As a general rule, the recognized CA shall ensure that archived records are detailed enough to establish the validity of a certificate and the proper operation of it in the past. Typical data that the recognized CA may consider for archiving include:

- data relating to the initialisation of the CA equipment, such as:
  - system equipment configuration files;

- results of assessments and/or reviews for accreditation of the equipment (if conducted);
- certification practice statement; and
- any contractual agreements to which the recognized CA is bound; and

- data relating to the operation of the recognized CA:
  - modifications or updates to any of the above data items;
  - all certificates and certificate revocation and suspension 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

A recognized CA shall specify the retention period for archived records, which shall conform to the requirements in this Code of Practice.

5.6.2 Protection of archive

A recognized CA shall specify the procedures in place to protect the archived records, covering for example:

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

5.6.3 Archive backup procedures

The recognized CA shall specify the procedures for backing up the archived records, as well as the retention period of the backups. It is a 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

A recognized CA shall specify the procedure for the changeover of the recognized CA's keys and the mechanism for informing the subscribers of the procedure.

5.8 Key compromise and disaster recovery

A recognized CA shall describe its procedures relating to notification and recovery in the event of key compromise or disaster. It shall address specifically the following:

- the 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 its 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 its trustworthiness; and

- the 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. An example would be the procedures to protect against theft of sensitive materials from a damaged site.

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

5.9 CA termination

A recognized CA shall specify the arrangements for the termination of its service and for notifying its subscribers and parties relying on the certificates issued by it of such termination, including the identity of the custodian of the recognized CA's archival records. Such arrangements shall comply with the requirements set out in section 11 of this Code of Practice.

6 Physical, Procedural, and Personnel Security Controls

A recognized CA shall describe the non-technical operational controls established by it to provide assurance that its business is conducted in a trustworthy manner.

Examples of such controls typically include physical, procedural, and personnel controls over key CA functions, such as key generation, authentication of the identity of the applicants of certificates, certificate issuance, revocation or suspension of certificates, 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

A recognized CA shall describe the physical controls on its facility housing 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 in respect of the operation of a recognized CA is one where 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 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.

A recognized CA shall describe its procedures for identifying trusted roles, such as the generation of its 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.

Examples of trusted roles include:

- CA Administrator who oversees the issuance of all certificates, the operation of the recognized CA, and the collection and maintenance of records. Primarily, the CA Administrator should ensure that the CA functions are conducted in accordance with the stipulations in the recognized 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 - a recognized CA may define additional roles under the supervision of the CA Administrator. Such roles shall perform specific functions in accordance with relevant provisions in the CPS. Whenever appropriate, separation of duties shall be implemented for all operations potentially affecting system integrity.

6.3 Personnel security controls

A recognized CA shall describe the controls over the recruitment, monitoring, assessment, training and termination of its 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 systems of the recognized CA;
- controls on contractor 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 the relevant personnel, such as user manuals, operational procedures, etc, necessary to support these personnel in performing their duties.

7 Technical Security Controls

A recognized CA shall define the technical security measures established by it to specifically protect its cryptographic keys and activation data (e.g., PINs, passwords, etc). It 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. The recognized CA shall also describe other technical security controls used by it to support the key and certificate management life cycle.

It is important to separate the controls performed by a recognized 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 applicants of its certificates (if the key pair is generated by the recognized CA for the applicants);
- secure delivery of the applicants' public key to the certificate issuer (if the key pair is generated by the applicants);
- secure delivery of the recognized CA's public key to subscribers;
- key size adopted, taking into consideration the available technology;
- controls over generation and quality checking of public key parameters;
- requirements for the type and quality of cryptographic modules used; and
- key usage and purpose (mapping to key usage flags under the X.509 PKI Certificate Profile version 3 and CRL Profile version 2 standards).

- private key protection, for example:
  - the standards, if any, required for the key generation module, such as compliance with a specific level according to the ISO 15782-1/FIPS 140-1 Security Requirements for Cryptographic Modules standard;
  - the use of multi-person control over private keys;
  - 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 of the archival system;
  - controls over the activation, usage and deactivation of the private keys, including for example the number of persons required for key entry, the form of the private keys, the activation mechanism, the active period of an activated key, etc;
  - controls over the destruction of the private keys, 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 systems of the recognized CA. Reference may be made to an appropriate computer security rating framework, such as ISO 15408:1999 Common Criteria for Information Technology Security Evaluation (CC);

- system development life cycle controls, which outline the controls implemented by the recognized 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 equipment of the recognized CA to prevent tampering;

- network security controls, which outline the control to protect all connectivity to equipment of the recognized CA, 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

A recognized CA shall specify the certificate format and, where applicable, the CRL format and the format of any other means of publishing certificate revocation information adopted by it, including information on profiles, versions, and extensions used. It is generally envisaged that a recognized CA would issue and manage public key certificates defined in accordance with the ITU X.509 v3 certificate format and would generate and post CRL in accordance with the ITU X.509 v2 CRL Format.

As far as possible, a recognized CA shall adopt widely accepted standards to foster interoperability of applications using certificates. As such, the use of certificate and CRL profiles that conform to the RFC 3280 Internet X.509 PKI Certificate and CRL Profile (or any updated version subsequently published by the Internet Engineering Task Force) as well as the avoidance of the use of critical extensions are strongly recommended.

8.1 Certificate Profile

A recognized CA shall provide 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

A recognized CA shall provide information relating to the CRL, possibly referencing to an appropriate standard, covering:

- version numbers supported for CRLs; and
- details of the CRL entry extensions populated and their criticality.

Where a recognized CA adopts other means of publishing certificate revocation information, the recognized CA shall provide information about such other means so as to enable other parties to access the certificate revocation information.

9 Specification Administration

A recognized CA shall describe how a CPS will be maintained.

9.1 Specification change procedures

A recognized CA shall describe the procedures for effecting any changes to the CPS, including the mechanism for notifying the GCIO, subscribers and relying parties in accordance with the requirements set out in this Code of Practice for such changes. Changes to CPS must be reflected and highlighted on the recognized CA's repository promptly. The recognized CA may in addition specify the types of changes that do not require prior notification.

9.2 Publication and notification procedures

A recognized CA shall describe the procedures for 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, a recognized CA shall implement widely accepted technical standards and management practices. It shall specify where appropriate the standards and practices that it has adopted, together with details of the options chosen and interface specifications for applications to use its certificates and services. It shall publish details including without limitation the standards adopted for the repository (e.g. LDAP compatible for directories; HTML for web pages, etc.), and the specific certificate profile (e.g. X.509) certificate extension, etc.

Appendix 2 – Specification of Provisions in the Electronic Transactions Ordinance and this Code of Practice in relation to Assessment of a CA

1 Specification of the provisions of the Electronic Transactions Ordinance (Cap. 553) (Ordinance) and of this Code of Practice for the purposes of sections 20(3)(b)(i), 27(5A)(b)(i) and 43(1)(a)(i) of the Ordinance

1.1 The following provisions of the Ordinance shall come within the scope of assessment to be performed by a qualified person approved by the GCIO.

(a) Part VII - Recognition of CAs and certificates by GCIO:

Sections 21(4)(a), (b), (c) and (f).

(b) Part X - General Provisions as to Recognized CAs:

Sections 36, 37, 39, 40, 42(1) and (2), 44 and 45(1).

(c) Part XI - Provisions as to secrecy, disclosure and offences:

Sections 46, 47 and 48.

1.2 The following provisions of this Code of Practice shall come within the scope of assessment to be performed by a qualified person approved by the GCIO.

(a) General Responsibilities of a Recognized CA:

Paragraphs 3.1 to 3.6 inclusive and 3.8.

(b) Certification Practice Statement:

Paragraphs 4.1 to 4.13 inclusive.

(c) Trustworthy System:

Paragraphs 5.1 to 5.3 inclusive, 5.6 to 5.17 inclusive and 5.19 to 5.21 inclusive.

(d) Certificates and recognized certificates:

Paragraphs 6.1 to 6.23 inclusive.

(e) Verification of subscriber's identity:

Paragraphs 7.1 and 7.2.

(f) Reliance limit and liability cover:

Paragraphs 8.1 to 8.4 inclusive.

(g) Repositories:

Paragraphs 9.1 to 9.5 inclusive.

(h) Disclosure of information:

Paragraphs 10.1 to 10.6 inclusive.

(i) Termination of service:

Paragraphs 11.1 to 11.5 inclusive.

(j) Assessment of compliance with the Ordinance and this Code of Practice:

Paragraph 12.1.

(k) Declaration of compliance with the Ordinance and this Code of Practice:

Paragraph 13.1.

(l) Adoption of standards and technology:

Paragraph 14.1.

(m) Inter-operability:

Paragraphs 15.1 and 15.2.

(n) Appendix 1:

All paragraphs in Appendix 1 of this Code of Practice.

2 Specification of the provisions of the Ordinance and of this Code of Practice for the purposes of sections 20(3)(c)(i), 27(5A)(c)(i) and 43(1)(b)(i) of the Ordinance

2.1 The following provision of the Ordinance shall be dealt with by means of a statutory declaration to be made by a responsible officer of a CA.

(a) Part VII - Recognition of CAs and certificates by GCIO:

Section 21(4)(e).

2.2 The following provisions of this Code of Practice shall be dealt with by means of a statutory declaration to be made by a responsible officer of a CA.

(a) General Responsibilities of a Recognized CA:

Paragraphs 3.7 and 3.9.

(b) Trustworthy System:

Paragraph 5.18.

(c) Disclosure of information:

Paragraphs 10.7 to 10.9 inclusive.

(d) Consumer protection:

Paragraph 16.1.

3 Specification of the provisions of the Ordinance and of this Code of Practice for the purposes of sections 43A(1)(c)(i) and (d)(i) of the Ordinance

3.1 Depending on the specific circumstances of the major changes that a recognized CA will make or has made to its systems, operation, controls and procedures, the relevant provisions of the Ordinance and this Code of Practice for the purposes of sections 43A(1)(c)(i) and (d)(i) of the Ordinance will be specified in the notice that the GCIO may give to the recognized CA under section 43A(1) of the Ordinance.