Certificate Policy for Mutual Recognition of Electronic Signature Certificates Issued by Hong Kong and Guangdong

Certificate Policy Version	:	1.0
Effective Date	:	10 Aug 2012

English translation of 粵港電子簽名證書互認證書策略 version 1.0. This translation is only for information purpose and it may be changed without any notice. No OID is assigned to this version. Applications of mutual recognition in Hong Kong must refer to current traditional Chinese version of 粵港電子簽名證書互認證書策略 published under OGCIO web site.

Certificate Policy for Mutual Recognition of Electronic Signature Certificates Issued by Hong Kong and Guangdong

Version 1.0

Table of contents

I. Certificates that are within the applicable scope

(1) This certificate policy (“CP”) is an important basis for determining whether the electronic signature certificates or the recognized digital certificates (hereinafter both electronic signature certificates and recognized digital certificates are referred to as “electronic signature certificates”), the former of which are issued by third party certification authorities which have obtained electronic certification permit and registered in Guangdong Province under the Electronic Signature Law of the People’s Republic of China whereas the latter by recognized certification authorities which are established under the Electronic Transactions Ordinance of the Hong Kong Special Administrative Region (hereinafter both third party certification authorities and recognized certification authorities are referred to as “certification authorities” (“CAs”)), are applicable to cross-boundary electronic transactions between Hong Kong and Guangdong.

(2) This CP is mainly applicable to the personal electronic signature certificates and the organizational electronic signature certificates for cross-boundary electronic transactions between Hong Kong and Guangdong (hereinafter referred to as “personal certificates” and “organizational certificates” respectively, or to be known as “certificates” collectively). This CP is also applicable to the certificates of CAs which issue the aforementioned certificates (hereinafter referred to as “CAs’ certificates”).

(3) On the basis of governing the conduct of CAs that issue the aforementioned certificates, this CP also sets out specific requirements on governing the conduct of the participating parties, such as certificate holders (hereinafter referred to as “subscribers”) and certificate relying parties (hereinafter referred to as “relying parties”).

II. Regulatory scope

This CP sets out the following regulatory requirements on certificate services and management provided by CAs:

- Publication of information;
- Identification and verification of identity;
- Certificate lifecycle operational requirements;
- CA facility, management and operational controls;
- Certification system technical security controls;
- Certificate and certificate revocation list ("CRL") profiles;
- Compliance;
- Reliance limit, indemnity arrangements and legal settlement;
- Confidentiality of information.

III. General obligations

(1) CAs (including their registration authorities ("RAs")) shall undertake obligations, including but not limited to the following:

- Formulating a certification practice statement ("CPS") that complies with the requirements of this CP, and providing certification services and related infrastructure in accordance with the requirements of this CP and the provisions of CPS;

* CAs shall establish and implement a security mechanism that is in compliance with the relevant requirements in order to ensure private keys are kept and protected in a secure manner;

* All activities relevant to certification practices shall be in compliance with the local laws and regulations as well as the requirements of the local competent authorities.

(2) CAs shall undertake obligations to certificate subscribers, including but not limited to the following:

* There are no misstatements in the certificates known to or originating from CAs;

* Errors made by CAs during certificate generation do not lead to inconsistency between the information contained in the certificates and those received by CAs;

* Certificates issued to subscribers shall be in compliance with the requirements of this CP and the relevant CPS;

* Certificates shall be revoked in accordance with the requirements of this CP and the relevant CPS on a timely basis;

* Subscribers shall be informed of any known incidents which may fundamentally affect the validity and reliability of the certificates.

(3) CAs shall undertake obligations to relying parties (persons who reasonably rely on signatures (such signatures can be verified by the public key in the certificates) in accordance with this CP and the relevant CPS), including but not limited to the following:

* Except the unverified information of subscribers, all

information contained or referred in the certificates is accurate;

- * Certificates shall be issued in full compliance with the requirements of this CP and the relevant CPS;

- * Through open publication of certificates, confirmation shall be given to the relying parties who reasonably rely on the information contained in the certificates that: the issuing CAs have issued certificates to the subscribers and the latter have accepted the certificates in accordance with the requirements of this CP and the relevant CPS.

IV. Publication of information

1. Repository

(1) CAs shall set up and maintain one or more online and publicly accessible repository/repositories to publish the following information:

- * Information on CP, CPS and relevant disclosed documents;

- * Information on certificates and certificate status enquiries (including but not limited to information on certificate directory, information on certificate status, CRL);

- * The latest version of subscriber agreements that can be made public and the latest version of relying party agreements that must be made public;

- * Other information that must be published as specified by the local competent authorities.

(2) CAs shall clearly specify the means of publishing information on certificate status in their CPS. In addition to CRL on their websites, CAs can publish certificate status information via

other effective supplementary means such as Lightweight Directory Access Protocol ("LDAP") directory server and Online Certificate Status Protocol ("OCSP") server.

(3) CAs shall determine the scope of contents of their CPS in accordance with Request for Comments ("RFC") 3647 standard (or relevant updated version). If there is any scope of contents inapplicable to them or inapplicable to a particular type, class or description of certificates, CAs shall clearly specify it in their CPS with reasons provided.

(4) CAs shall publish information in their repository/repositories to make the relying parties clearly understand that they are required to undertake major obligations for the use of certificates issued by CAs when relying on such certificates, including but not limited to the following:

* The relying parties are familiarized with the provisions of this CP and the relevant CPS, and understand the objectives of using the certificates as well as the assurance provided by these certificates. Before relying on the certificates, the relying parties shall accept the provisions of relying party agreement. They shall decide whether the certificates are trustworthy by taking into account the circumstances and conditions for using the certificates;

* If the relying parties need CAs to provide additional protection, i.e. the additional protection provided by relevant provisions in CPS, they shall confirm if such protection can be obtained and decide whether the corresponding certificates can be relied upon at their own discretion;

* The relying parties shall reasonably check and verify the certificates, including checking the latest CRL published by CAs to confirm that the certificates are not suspended or revoked; checking the reliability of those certificates that

have appeared in the trust path of the certificates; checking the validity of the certificates; checking other information which can affect the validity of the certificates;

- * Other reasonable obligations of the relying parties stated in CPS;

- * The relying parties shall bear the legal consequences arising from their failure to perform the aforesaid obligations.

(5) CAs shall clearly state the location of their repository/repositories and the means of enquiry in their CPS and other related documents to facilitate the relevant parties to access to the repository/repositories for obtaining the required information, and particularly to handle enquiries from subscribers and relying parties on CPS, certificates and certificate status.

(6) CAs shall adopt effective security measures to protect their repository/repositories from unauthorized addition, deletion or modification. In operating and maintaining their repository/repositories, they shall not carry out any activities that may create unreasonable risk to persons relying on the repository/repositories (including the certificates and other information).

(7) CAs shall declare in their CPS associated with this CP that, on the basis of compliance with the local legal regulatory requirements and this CP, CAs, subscribers and relying parties shall not take actions against the governments of Hong Kong and Guangdong as well as the competent authorities of certification services of the two places for any liabilities and claims for compensation arising from the deficiencies of CAs or relevant certificates or the negligence of CAs.

2. Publication of information by CAs

(8) CAs shall publish the following certificate information in their repository/repositories, including but not limited to:

- * CAs' certificates that contain the public key corresponding to the private key used by CAs for the issuance of certificates;

- * The notice of suspension, revocation or non-renewal of CAs' certificates by CAs or the competent authorities;

- * Any other incidents that materially and adversely affect the reliability of certificates issued by CAs or the ability of CAs to perform their services.

3. Time or frequency of publication

(9) CAs shall publish and update the information of disclosed documents and their amendments in their repository/repositories on a timely basis, including but not limited to:

- * CP;

- * CPS;

- * Relevant documents that are required for the use of CAs' certificate services;

- * CAs' disclosure records of the aforesaid previously published documents and their amendments.

(10) CAs shall timely publish the relevant information on the issued certificates upon the effective date of these certificates for download, reference and use.

(11) CAs shall publish information about the suspension or revocation of certificates (including CAs' certificates), including CRL and other information on certificate suspension or revocation.

* When certificates are suspended or revoked, CAs shall publish relevant information on a timely basis;

* When certificates are suspended or revoked, CAs shall publish the relevant CRL on a timely basis;

* CAs shall publish CRL in relation to certificates at least once every 24 hours;

* When CAs' certificates are suspended or revoked, CAs shall publish relevant information on a timely basis;

* When CAs' certificates are suspended or revoked, CAs shall publish the relevant CRL on a timely basis;

* CAs shall issue CRL in relation to CAs' certificates at least once every year;

* CAs shall publish CRL within a reasonable period of time, and clearly specify the publication time of CRL in their CPS.

(12) The repository/repositories of CAs shall not contain any information which is confirmed to be incorrect or unreliable.

V. Identification and verification of identity

1. Naming of identity in certificates

CAs shall provide assurance in the certificates issued by them:

(1) Certificates shall contain an X.501 Distinguished Name ("DN")

in the subject name field and adopt X.500 as the naming convention.

(2) The name adopted by subscribers must be meaningful with commonly understood semantics used to clearly describe the identity of the person or organization appeared in the subject name field of the certificates and to link the name to the only identifiable entity (i.e. a person or an organization). In case of name collisions, CAs shall determine which applicant will be given the priority of using the name through a clearly defined system. Subscribers are not allowed to use anonymity or pseudonymity in the certificates. The subject name field of personal certificates shall contain a name which can identify the personal subscribers, while the subject name field of organizational certificates shall contain a name which can identify the organizational subscribers.

(3) CAs shall request certificate applicants to ensure they will not use any name that infringes intellectual property right. CAs shall request certificate applicants to submit relevant trade mark registration documents, such as legal proofs issued by government organizations, if the contents of the certificates for which they have applied contain trade mark information.

2. Verification of identity for new certificate applications

(4) Verification of identity of organizations:

When organizations (government organizations, enterprise units or other social organizations, etc.) apply for certificates, CAs shall strictly verify their identity in the first place, including but not limit to:

* Proving the physical existence of the organizations with the materials provided by an independent and authoritative third party, such as legal proofs issued by government organizations, or supporting materials provided by other

recognized authoritative organizations;

* Using effective means to confirm the authenticity of application information submitted by the organizations, and ensuring that due authorization has been obtained from the organizations for the application and that other required information can be provided for verification;

* Regarding applications for organizational certificates using the name of an individual, CAs shall request the organizations to confirm the identity of such individual and submit relevant materials for verification;

* Regarding applications for organizational certificates submitted by authorized representatives, CAs shall request the representatives to submit written authorization documents from the organizations (such as authorization letter) to confirm that express authorization has been obtained from the organizations;

* Verifying and confirming the genuine identity of the authorized representatives face-to-face by checking their statutory identity documents (including but not limited to identity card, passport or any other identity information);

* Other additional verification means and information as considered necessary under reasonable circumstances.

(5) Verification of identity of individuals:

When individuals apply for certificates, CAs shall strictly verify their identity in the first place:

* Verifying and confirming the genuine identity of the individuals face-to-face by checking their statutory identity documents (including but not limited to identity card, passport or any other identity information). The identity of

the individuals shall correspond to the subject name shown in the certificates for which they have applied;

- * Other additional verification means and information as considered necessary under reasonable circumstances.

(6) CAs shall clearly specify the means (including whether face-to-face verification is adopted) to verify the identity of organizations or individuals in their CPS that corresponds to a particular type, class or description of certificates.

(7) If certificates contain any subscriber information that has not been verified in a certain and reliable manner, CAs shall clearly specify these unverified information or the type of these unverified information in their CPS as well as in the certificates.

3. Verification of identity for certificate revocation requests

(8) CAs shall perform reasonable verification procedures for certificate revocation requests, including but not limited to following procedures:

- * When subscribers request certificate revocation, CAs shall ask these subscribers to provide the same identity information as that for certificate application or submit their legal and valid electronic signature through the existing certificates for identity verification. If face-to-face verification is not viable due to conditional constraints, CAs or their RAs shall verify the subscribers' identity by other reasonable means, such as by phone, mail or other proofs from third party. When certificate revocation requests are put forth by judicial agencies according to the laws, CAs or their RAs may directly use the written revocation requests issued by judicial agencies as the basis for verification and no further verification by other means is required.

* In general, it takes some time to verify the identity of the subscribers and the certificates in question cannot be revoked instantly. Nevertheless, CAs shall be allowed to suspend the certificates under reasonable circumstances. Still, CAs shall perform verification procedures on the subscribers' identity or handle written revocation requests issued by judicial agencies on a timely basis.

VI. Certificate lifecycle operational requirements

1. Certificate application

(1) CAs (including their RAs) can accept certificate applications from the following parties:

* Any organizations (government organizations, enterprise units or other social organizations, etc.);

* Authorized representatives of any organizations (government organizations, enterprise units or other social organizations, etc.);

* Individual applicants.

The identity of organizations, authorized representatives or individuals shall comply with the identity verification requirements set out in this CP.

(2) CAs shall ensure that all certificate applicants, during application,

* Clearly understand and accept the contents of the subscriber agreements, especially those relating to liabilities and assurance;

- Provide genuine, reliable and complete identity information according to the type of certificates for which they have applied ;

- Bear any legal liability for providing false and forged information.

2. Certificate application processing

(3) Acceptance or rejection of certificate applications:

CAs shall not approve certificate applications in the following cases:

- The application fails to fully comply with the requirements set out in this CP regarding the identification and verification of the subscriber information;

- The applicant fails to provide the necessary proof of identity or other supporting documents as required;

- The applicant does not accept the contents and requirements of the subscriber agreements, especially those relating to obligations and assurance.

(4) CAs shall keep the document records that can be used to identify applicants.

(5) Timeframe for processing certificate applications

CAs shall clearly specify the processing time in their CPS, and shall complete the processing of certificate applications within the pledged time.

3. Certificate issuance

(6) Upon acceptance of certificate applications from applicants, CAs

shall issue certificates based on the verification result of the application documents and applicants' identity.

(7) CAs shall ensure that the private keys are untampered when certificates (including the key pair) are generated by system for the subscribers under a secure environment and when certificates are delivered to the subscribers in a secure way. CAs shall not accept any private keys provided by the subscribers, nor shall they accept any key renewal requests from the subscribers.

(8) Once CAs have issued certificates, they have assured the persons who reasonably rely on the certificates or the electronic signatures verifiable by the public keys in the certificates that:

They have issued the certificates in accordance with the relevant rules and laws, this CP and the relevant CPS.

(9) CAs shall publish the issued certificates and other relevant information in the publicly accessible repository/repositories.

(10) CAs and their RAs shall record all transactions in relation to certificate issuance, including the date and time.

(11) After issuing the certificates, CAs shall timely inform the subscribers and provide them with the ways to collect the certificates, ensuring that the subscribers can collect the certificates by reasonable means.

4. Certificate acceptance

(12) CAs shall clearly specify in the subscriber agreements and their CPS the actions that constitute the subscribers' acceptance of certificates (for instance, subscribers' acceptance of a medium containing a certificate), and shall ensure their subscribers clearly understand that such actions constitute the acceptance of certificates.

5. Certificate renewal

(13) Each certificate issued by CAs shall specify its validity period. When a certificate expires, the subscriber shall obtain a renewed certificate if he/she wants to continue to use the certificate.

(14) When processing certificate renewal requests, CAs shall ensure that the person who makes the renewal request is the subscriber identified in the certificate that requires renewal.

(15) CAs and their RAs shall record all transactions in relation to certificate renewal, including the date and time.

6. Certificate modification

(16) When there are changes in information (except the public key) in the certificates, subscribers are required to submit a re-application for the certificates. CAs shall not accept applications for changing contents in the issued certificates.

7. Certificate revocation and suspension

(17) CAs shall suspend the certificates issued by them if they have reasonable grounds to believe that these certificates are no longer reliable, regardless of whether the subscribers consent to the suspension. CAs shall complete the investigation on the reliability of the certificates and decide within a reasonable time period whether to reinstate or revoke the certificates. If CAs consider that an immediate revocation of certificates issued by them is justified in the light of all the information available, the certificates shall be revoked, regardless of whether the subscribers consent to the revocation. CAs shall state in their CPS the actions to be taken in the event that the subscribers cannot be reached.

(18) CAs shall provide hotlines or other means of communication for subscribers to report to CAs incidents affecting their certificates

or private keys, for example, keys having been lost or compromised, etc..

(19) After receiving revocation requests, CAs shall check and confirm the identity and authority of the requesters as well as the justifications for revocation before revoking the certificates. CAs shall clearly specify in their CPS the period from the time when revocation requests are received to the time when the certificates are revoked. The processing of certificate suspension shall be within a reasonable period of time, and CAs shall clearly specify the processing time (preferably not longer than one working day) in the relevant CPS. Revocation requests made by persons other than the subscribers shall be subject to strict internal procedures and approval of the specified management personnel. Within a reasonable time following the suspension or revocation of certificates, CAs shall inform the subscribers of the suspension or revocation.

(20) CAs shall maintain strict control over errors during certificate generation (e.g. errors in downloading certificates, mismatched key pair) that will lead to certificate revocation.

(21) Upon certificate revocation, CAs shall publish the revocation information within 24 hours through CRL and other publicly accessible certificate status enquiry channels (if applicable). CAs shall specify in their CPS the time for updating the revocation information.

(22) When the security of keys of CAs (including keys of CAs or sub-CAs) are compromised or suspected to be compromised, CAs shall timely and properly inform the subscribers and the relying parties within a reasonable period of time.

(23) CAs shall properly record the certificate revocation process.

(24) For CAs' certificate revocation requests, CAs shall not put forth such requests prior to the confirmation of the relevant regulatory

authorities.

8. Key pair and certificate usage

(25) CAs shall require that all subscribers can use the private keys corresponding to the certificates only after they have signed the subscriber agreements and have confirmed their acceptance of the certificates. CAs shall also require that once the subscribers have accepted the certificates issued by CAs, these subscribers shall undertake the following obligations:

* The usage of subscribers' private keys shall comply with the requirements on "Key Usage" stated in the certificates;

* The usage of subscribers' private keys and certificates shall comply with the requirements stated in the subscriber agreements;

* When the subscribers generate their electronic signatures by using the private keys corresponding to the public keys in the certificates, it means these electronic signatures are generated in the name of the subscribers. Before electronic signatures are generated, the subscribers shall ensure that the certificates are valid and unrevoked (the subscribers shall stop using the private keys if the certificates have expired or have already been revoked);

* Subscribers shall maintain control over their private keys, and shall take reasonable measures to protect their private keys from being lost, compromised, tampered and used without authorization;

* Subscribers shall not use the certificates for illegal activities;

* Subscribers shall undertake other obligations stated in the subscriber agreements.

9. Certificate status services

(26) CAs shall provide as far as practicable uninterrupted certificate status services, preferably 24 hours a day and seven days a week. In case of service interruption, the interruption period shall be kept to a minimum. CAs shall specify in their CPS the period in which uninterrupted certificate status services are available as well as the scheduled period of service interruption. If CAs have to interrupt the certificate status services (according to schedule or under unexpected or uncontrollable circumstances), they shall keep the interruption period to a minimum. CAs shall ensure that the interruption period shall not be more than two hours per week for scheduled service interruption. CAs shall inform all parties concerned of the interruption in accordance with their local regulatory requirements.

10. Termination of certificate services/subscription

(27) CAs shall explain to the subscribers and the relying parties (including specifying in CPS) under what conditions the certificate services for the subscribers or the subscription would be terminated, including but not limited to the following:

- Certificates are revoked by CAs during their validity period;

- Requests for termination of services are received prior to the expiry of the certificates, and are accepted by CAs;

- Certificates or keys have not been renewed upon the expiry of the certificates.

(28) CAs shall clearly set out the requirements for certificate subscription termination, draw up specific workflow for that and properly retain the records.

11. Key escrow and recovery

(29) CAs shall specify in their CPS the specific workflow for key escrow and recovery.

(30) Neither the keys of CAs nor the subscribers’ keys for signature can be escrowed.

VII. CA facility, management and operational controls

1. Physical security and environmental controls

(1) CAs shall adopt effective physical security control measures:

* Identifying and defining secure areas (e.g. effectively distinguishing between public area, service area, administrative area, core area, shielded area, etc.), and employing effective physical security control measures in accordance with the requirements of different areas to ensure the physical security of such areas;

* Establishing formal procedures and putting in place appropriate security control measures for access to the secure areas by CAs’ employees and visitors, including access monitoring mechanism;

* Providing extra protection for the locations where sensitive physical security equipments are stored;

* Ensuring access to each physical security layer is auditable and controllable so that only authorized personnel can access each physical security layer;

* Implementing a computer room monitoring system to provide real-time monitoring for infrastructure equipments, computer room and security protection system 24 hours a day and seven days a week. The monitoring records shall be retained for the purposes of fault diagnosis and post-event auditing. CAs shall specify the retention period of these

monitoring records in their CPS, and such records shall be kept for at least 3 months;

- * Implementing an access control system with the functions of check-in/check-out record and time-out alert. CAs shall archive the records on regular basis. CAs shall specify the retention period of the check-in/check-out records in their CPS, and such records shall be kept for at least 3 months;

- * Ensuring that only authorized personnel can operate the physical equipments of CAs. CAs shall adopt different levels of access control measures for physical equipments of different security levels, including but not limited to:

  a) Authorized personnel shall enter log-in password for using physical equipments;

  b) Authorized personnel shall perform two-factor or multiple-factor authentication (one of which shall be biometric authentication) when entering sensitive areas;

  c) Ensuring the access logs of equipments are untampered and checked on regular basis;

  d) At least two authorized personnel are required to operate cryptographic modules or computer systems;

  e) Performing 24-hour automatic or manual monitoring for physical equipments of high security level.

(2) The physical security equipments of CAs and their RAs shall be provided with main and backup power supply systems to ensure continuous and uninterrupted power supply. Air-conditioning system shall also be provided to control temperature and humidity.

(3) CAs and their RAs shall take preventive measures, use

corresponding configuration and establish handling procedures to protect the security of physical equipments, particularly to protect the systems from damages or other adverse consequences arising from flooding or water leakage. Fire protective measures shall comply with the requirements specified by the local fire services department. The computer room shall be installed with automatic fire alarm system and fire extinguishing system. CAs shall specify in their CPS whether two types of fire detectors are installed for detecting temperature and smoke. The fire alarm system and the fire extinguishing system shall be linked together.

(4) CAs and their RAs shall strictly protect the storage media containing backup system data and any other sensitive information from damages arising from flooding, fire, electromagnetic interference and other environmental factors. Strict protection measures shall be taken to prevent unauthorized access to, use or disclosure of these media.

(5) CAs and their RAs shall establish strict waste disposal procedures, especially for paper documents, electronic media and any other wastes containing privacy or sensitive information. They shall ensure thorough physical destruction of such wastes or complete deletion of data stored in such wastes to prevent unauthorized access to, use or disclosure of privacy or sensitive information stored in such wastes.

(6) CAs and their RAs shall establish backup systems for critical systems and data (including any sensitive data and audit data). Off-site backup measures shall be implemented for critical systems and data to ensure these systems and data are stored in secure facilities.

(7) If CAs rely on a third party to provide physical security protection and environmental control services, such services shall be clearly specified in the formal service agreement between CAs and the third party service providers.

(8) Facilities of CAs shall be safeguarded and protected against natural disasters.

(9) CAs shall comply with other applicable requirements stipulated by the local laws, regulations and relevant technical standards (such as national standards for building computer rooms, fire services ordinance, etc.).

2. Procedural controls

(10) CAs shall only allow trusted personnel to work in trusted positions. Personnel holding trusted positions are those who can access or control certificates or operate keys, and who may have important influence in the following aspects, including but not limited to:

* Information verification and validation for certificate application;

* Approval, rejection or making other arrangements for certificate application or revocation;

* Certificate issuance and revocation;

* Access to strictly controlled repository/repositories;

* Handling of subscriber information and requests.

(11) CAs and their RAs shall establish, maintain and implement strict control procedures, take measures for segregation of duties in accordance with the working requirements and arrangements, and establish security mechanism of mutual checking and monitoring while ensuring sensitive operations are jointly completed by several trusted personnel. Roles that are subject to segregation of duties include but not limited to:

* Personnel who engage in verifying information for

certificate application;

* Personnel responsible for approving, rejecting or making other arrangements for certificate application, revocation, renewal as well as information registration;

* Personnel responsible for issuing and revoking certificates or who can access restricted areas and sensitive information;

* Personnel who handle subscriber information;

* Personnel who generate, issue and revoke CAs' certificates;

* Personnel responsible for putting systems online or offline;

* Personnel who keep important passwords;

* Personnel who manage and operate keys and cryptographic devices;

Critical physical and logical controls shall be implemented separately. At least two trusted personnel shall be required to participate in such sensitive operations as the logical and physical access to system devices, while at least three trusted personnel be required to participate in the access to CAs' hardware cryptographic devices throughout their lifecycle (from the commissioning of these devices to their logical/physical destruction). Besides, once the cryptographic module of a system device is activated, segregation of duties shall be implemented for further logical and physical access. Personnel vested with the rights to physical access of system devices shall no longer hold secret shares of the system devices, and vice versa.

3. Personnel security

(12) CAs shall formulate provisions for effective control over personnel security, and shall update such provisions if necessary.

(13) For those personnel who are going to work in trusted positions, CAs shall perform strict identification and assessment to ensure that they can fulfill the requirements of their duties and responsibilities:

* Identifying different roles, setting out the rights for these roles, specifying the qualifications and background requirements for different roles according to actual needs, and ensuring the fulfillment of these requirements by the relevant personnel;

* Conducting security check on the personnel (including but not limited to conducting face-to-face identification and requiring the personnel to present their valid proof of identity);

* Based on the nature of operations as well as the rights for these positions, granting the personnel working in trusted positions the rights to access systems and physical environments, and adopting appropriate access control techniques (including but not limited to such security tokens as system operation cards, door access cards, login passwords, operational certificates and operating account numbers for authentication purpose) to maintain a complete record of all sensitive operations performed by such personnel;

* Incorporating relevant security provisions in staff contract.

(14) CAs shall ensure all their staff (including those assuming the trusted roles) possess the required technical qualifications and expertise so that they can effectively carry out their duties and responsibilities. At the same time, they shall provide appropriate and sufficient training for their staff (at least once a year for those holding core positions) to ensure their capabilities in carrying out their duties as well as effective implementation and

compliance with the security policies. The content of training may include but not limited to:

* Appropriate technical training;

* Rules, mechanisms and procedures;

* Procedures for handling security incidents and notifying senior management of major security incidents.

(15) CAs shall formulate appropriate control measures to assess the performance of their staff. For examples:

* Performance assessment on regular basis;

* Formal disciplinary procedures (including procedures for handling unauthorized activities);

* Formal procedures of service termination.

4. Event logging procedures/audit process

(16) CAs shall keep sufficient event records (including documentations related to certificate issuance and certificate management), and perform regular (not less than once a month) checking on such records. Appropriate actions shall be taken in case of any irregularities.

(17) CAs shall keep records of all major events, including but not limited to:

* Access to the information and devices for key generation;

* Key and certificate generation, issuance, distribution, storage, backup, suspension, revocation, withdrawal, archival, disposal and other relevant matters;

- * Security incidents, including but not limited to leakage of key information, network intrusion, etc.;

- * Procurement, installation, commissioning, decommissioning and disposal of cryptographic devices;

- * Records of development and operation/maintenance of computer facilities.

(18) CAs shall keep the original audit logs for at least two months and regularly check these audit logs in order to detect any major security events and management issues. Corresponding actions shall be taken in case of such events or issues, and records of investigation or auditing actions shall also be kept. CAs shall strictly implement physical and logical access control measures for all audit logs and records to prevent unauthorized browsing, modification, reading, deletion, etc.. CAs shall establish and implement reliable backup system to perform regular backup for the audit logs (at least once every two months). The backup cycle shall be clearly specified in the CPS.

(19) CAs shall archive all audit log records in accordance with the requirements set out by this CP. The original records so archived shall be kept for at least five years or a period that is in compliance with the requirements stipulated by the local laws and regulations, whichever is the longer.

5. Record archival

(20) Apart from keeping event records as required, CAs shall also archive all other important records, including but not limited to:

- * Documentations of the establishment and upgrading of certificate system;

- * Certificates and CRL;

- * Documentations supporting certificate application, information on the approval and rejection of certificate services, and certificate subscriber agreements;

- * Audit records;

- * CP and CPS documentations;

- * Particulars of staff, including but not limited to information on their background, employment and training;

- * Documentations of external or internal assessments.

(21) The retention period of different archival records may vary. CAs shall define the retention period for different archival records according to legal and regulatory requirements, business needs and actual operational status. Nevertheless, archival records of all kinds shall be kept for at least five years from the date when the certificates expire or are revoked.

(22) CAs shall retain accurate time and date information of archival records, including record generation date and time.

(23) CAs shall take appropriate physical and logical access control measures to ensure only authorized and trusted personnel can access all archival records. CAs shall store the archival records in a reliable system or location in order to protect these records from unauthorized browsing, modification, deletion, etc.. CAs shall ensure that these archival records can be accessed effectively by the authorized and trusted personnel during the retention period. CAs shall verify the consistency of archival records during the archival process. During the archival period, CAs shall verify the consistency of all accessed records (through appropriate techniques or methods).

(24) CAs shall conduct backup for the electronic archival records generated by system regularly. Backup documentations shall be

stored in off-site locations. If no backup is conducted for archival records in paper form, CAs shall take strict measures to ensure their security.

6. Handling of incidents, emergency response, disaster recovery and business continuity

(25) CAs shall establish procedures and contingency measures for handling major incidents that may occur in their major operational areas, including procedures and contingency measures for emergency, disaster recovery and business continuity, to ensure the expected service level is maintained (including meeting the requirements for certificate status enquiry service [please refer to bullet 9 “Certificate status services” of Chapter VI “Certificate lifecycle operational requirements”], and specifying the interruption period for other core services like certificate suspension and revocation services). These procedures and contingency measures shall be maintained and updated in a timely manner. The possible major incidents include but not limited to:

* Computing resources, software, data are damaged or major failure incidents (including incidents affecting the external access to the repository/repositories) occur;

* RAs terminate their services due to incidents;

* Private keys of CAs or their subsidiaries are damaged, lost, leaked, cracked, tampered or suspected to be stolen by a third party.

(26) CAs shall conduct regular drilling exercises on their contingency measures for disaster recovery and business continuity, and shall record the drilling procedures and results. All personnel involved in the contingency measures shall participate in the drilling exercises.

VIII. Certification system technical security controls

1. Key pair generation and installation

(1) CAs shall formulate and adopt operational control measures for key pair generation, including but not limited to:

* Procedures to ensure the devices used for key pair generation are complete and correct;

* Procedures to ensure key pairs are generated under strict supervision by authorized personnel.

(2) After generating a key pair for subscribers, CAs shall deliver the private key to the subscribers in a secure way without being tampered with. The medium technology for storing the certificate (including private keys) shall comply with the standards specified in the "Table of technical standards for mutual recognition of electronic signature certificates issued by Hong Kong and Guangdong and measures for adopting these standards" (Annex 1.2). CAs shall specify in CPS the medium technology used to store the private keys of subscribers' certificates. The subscribers' private keys and the activation data for the private keys shall be delivered to the subscribers by different means. CAs shall record the details of each delivery of private keys.

(3) CAs shall generate key pairs for issuing certificates and certificate status information by using hardware devices that are in compliance with the local security and regulatory requirements and this CP.

2. Key changeover of CAs

(4) CAs shall timely renew their certificates and key pairs to ensure smooth transition of certificate chain and key pairs, with a view to minimizing the adverse effects on their subscribers and relying

parties.

(5) CAs shall ensure smooth transition of the entire certificate chain upon changeover of their key pairs.

3. Private key protection and cryptographic module engineering controls

(6) CAs shall ensure the security standards of cryptographic modules for generating private keys are in compliance with the "Table of technical standards for mutual recognition of electronic signature certificates issued by Hong Kong and Guangdong and measures for adopting these standards" (Annex 1.2).

(7) CAs shall specify in the relevant CPS that corresponds to a particular type, class or description of certificates all cryptographic algorithm technical standards adopted.

(8) CAs shall implement effective procedures and controls over the procurement, receipt, installation, acceptance test, commissioning, usage, repair, maintenance and retirement of key generating device, including but not limited to:

* Implementing effective procedures to ensure the integrity of the cryptographic modules;

* Implementing effective procedures to ensure the handling of key generating device is under proper supervision by authorized personnel to protect the device from being tampered with; establishing control mechanisms to ensure that the cryptographic modules cannot be tampered with without being detected;

* Implementing effective procedures to ensure the strength of keys generated using cryptographic modules is of the appropriate strength for the purpose of using the keys by both CAs and their subscribers, and complies with the

relevant cryptographic algorithm for electronic signature specified in the “Table of technical standards for mutual recognition of electronic signature certificates issued by Hong Kong and Guangdong and measures for adopting these standards” (Annex 1.2);

* Implementing effective procedures and controls to protect the private keys from being lost, stolen, disclosed, tampered or used without authorization when transferring keys among different cryptographic modules;

* CAs’ private keys shall be stored on the cryptographic modules in encrypted form.

(9) CAs shall implement effective procedures and controls over the preparation, activation, usage, distribution and termination of any key storage media (e.g. smart cards).

(10) Multiple-person control (M out of N (M>N>1)) strategy shall be adopted for operation of CAs’ private keys, and “secret sharing” technique shall be used to split the activation data needed for using and operating CAs’ private keys into several parts which are held by trusted personnel authorized by the management. The procedures for generation and separation shall be completed at the same time when operating the private keys. CAs shall separately keep their private keys and activation data in a secure manner.

(11) CAs shall perform the backup of their private keys in a secure manner, and keep the backup of these private keys in safe devices in a secure manner according to disaster recovery operational needs.

(12) When the lifecycle of CAs’ private keys has ended, CAs shall securely retain these private keys in accordance with the relevant archival requirements specified in this CP. After the end of archival period, CAs shall destroy these private keys in

compliance with the relevant requirements on private key destruction specified in this CP.

(13) CAs shall put in place controls to ensure secure destruction of key pairs and any related devices, including implementing procedures that are effective enough to ensure destruction of all backup copies of private keys (i.e. the destroyed private keys cannot be recovered or reconstructed) as well as procedures for revocation of the corresponding certificates.

4. Other aspects of key pair management

(14) CAs shall archive all their public keys.

(15) CAs shall comply with the following requirements for certificate operational period and key pair usage period, including but not limited to:

* The operational period of certificates ends upon their expiration or revocation;

* The usage period of subscribers' key pairs shall be the same as the operational period of the associated certificates. In spite of this, the public key of key pairs can still be used for signature verification even after the operational period of the certificates has ended;

* The operational period of certificates issued by CAs shall not exceed the usage period of the associated key pairs;

* The key pairs of certificates can be used for identity authentication only when the certificates are still valid. In spite of this, the public key of key pairs can still be used for signature verification even after the operational period of the certificates has ended;

* Subscribers' certificates shall specify that their maximum

validity period shall not be more than 5 years, whereas CAs' certificates shall specify that their maximum validity period shall not be over 50 years.

(16) CAs shall ensure that all procedures for generation and installation of activation data are secure and reliable, in order to protect private keys from being leaked, stolen, used without authorization, tampered or disclosed without authorization.

5. Computer and network security controls

(17) CAs shall develop comprehensive and well-established security management strategy and system, and implement stringent security controls to ensure the security and reliability of the system for storing CAs' software and data/documents, and to protect the system from unauthorized internal or external access.

(18) CAs shall implement stringent management mechanism to control and monitor the operating systems, in order to prevent unauthorized modification.

(19) CAs shall implement security measures such as multi-level firewall, intrusion detection system, security audit, anti-virus system to protect CAs' network environment. Timely version update, regular risk assessment and audit for network environment shall be conducted in order to detect intrusion risks and minimize risks from the network.

(20) When CAs dispose of waste devices, they shall delete the information stored within which might affect the security of certificate business, and shall confirm that this is properly done.

(21) CAs shall regularly employ an independent third party to conduct an overall assessment on areas such as computer and network security in accordance with the "Arrangement for Mutual Recognition of Electronic Signature Certificates Issued by Hong Kong and Guangdong".

6. System development controls

(22) CAs shall formulate procedures for system development, upgrade and maintenance, adopt effective controls, and modify or update these procedures and controls in a timely manner. These procedures and controls shall include but not limited to:

* Adoption of a set of uniform and effective internal standards for system development, whether it is conducted by the staff of CAs or by other parties under exceptional circumstances;

* Effective procedures for segregation of the production and development environments;

* Effective procedures for segregation of duties between operational, maintenance and development personnel;

* Effective access controls over access to data and systems held in the production and development environments;

* Effective controls (including but not limited to version control, stringent testing and verification, etc.) over change control process (including but not limited to normal and emergency changes to systems and data);

* Procedures for conducting security checking and assessment on systems before going online to see whether there are security vulnerabilities or intrusion risks, etc.;

* Effective procedures for the proper management of the acquisition of equipment and services.

7. Timestamping

(23) CAs shall ensure that all system entries and operational entries are time stamped accurately.

IX. Certificate and certificate revocation list profiles

(1) CAs shall ensure the technology and format adopted for certificates shall comply with the requirements specified in the "Arrangement for Mutual Recognition of Electronic Signature Certificates Issued by Hong Kong and Guangdong" and the "Table of technical standards for mutual recognition of electronic signature certificates issued by Hong Kong and Guangdong and measures for adopting these standards" (Annex 1.2). In adopting specific technical solution, CAs shall take into account the need for interoperability of certificates for cross-border use.

(2) CAs shall issue and manage public key certificates in accordance with the certificate format specified in the ITU X.509 v3, and generate and publish CRL in accordance with the CRL format specified in the ITU X.509 v2.

(3) CAs shall clearly specify in the relevant CPS that corresponds to a particular type, class or description of certificates the certificate format (including certificate extensions) and technical standards (such as type of numeric character) adopted.

(4) If CAs adopt OCSP technology as a means supplementary to CRL to facilitate timely checking on the certificate status by their subscribers and relying parties, CAs shall specify in their CPS the mode of operation, the information provided and the technical standards adopted.

X. Compliance

(1) CAs shall establish and implement effective internal auditing procedures to ensure their compliance with all applicable laws and regulations, this CP, the corresponding CPS as well as the relevant internal rules and mechanisms.

(2) CAs shall annually employ an independent third party to conduct

an assessment on their compliance with this CP according to the "Arrangement for Mutual Recognition of Electronic Signature Certificates Issued by Hong Kong and Guangdong".

(3) CAs shall timely submit a comprehensive proposal on improvements and preventive measures in response to the exceptions, inadequacies or suggestions mentioned in the assessment report.

XI. Reliance limit, indemnity arrangements and legal settlement

(1) In issuing a type, class or description of certificates to subscribers, CAs shall specify in the relevant CPS that corresponds to that type, class or description of certificates a reliance limit on the certificates as well as the significance of the reliance limit on the use of the certificates.

(2) CAs shall arrange suitable insurance or provide other forms of indemnity arrangements that are in compliance with the requirements of the regulatory authorities (e.g. indemnity assurance deposit) to ensure they are capable of covering potential liabilities arising from or related to the issuance or use of certificates. CAs who have acquired insurance shall publish the policy number or other proofs of existence of such insurance in their repository/repositories. Upon request by the local competent authorities or independent third party during assessment, CAs shall immediately provide them with the policy number or the proofs of existence of such insurance.

(3) CAs shall specify the indemnity commitment for subscribers and relying parties in the subscriber agreements and the CPS respectively.

(4) Regardless of where the subscribers or relying parties live and where they use the certificates, the local laws of the place of issuing the certificates are applicable to the implementation, interpretation and procedural effectiveness of this CP. CAs shall

clearly specify the courts responsible for resolving any disputes in relation to this CP or the CPS.

XII. Confidentiality of information

CAs shall bear the corresponding responsibility of protecting confidential information (including but not limited to confidential business information and personal privacy information), clearly define the scope of protection and protect such information through effective management mechanism and technical measures.

XIII. Supplementary provisions

(1) This CP is applicable to CAs that have participated in the mutual recognition of electronic signature certificates issued by Hong Kong and Guangdong in accordance with the “Arrangement for Mutual Recognition of Electronic Signature Certificates Issued by Hong Kong and Guangdong”.

(2) This CP may be modified by the Guangdong-Hong Kong Working Group on Pilot Applications of Mutual Recognition of Electronic Signature Certificates in accordance with the “Arrangement for Mutual Recognition of Electronic Signature Certificates Issued by Hong Kong and Guangdong”.

(3) This CP will come into force and effect upon the date of publication of the “Arrangement for Mutual Recognition of Electronic Signature Certificates Issued by Hong Kong and Guangdong”.

Annex 1.1: Chinese expression of terminologies for certificate policy between Hong Kong and Mainland

Terminologies	Terminologies commonly used in Mainland	Terminologies commonly used in Hong Kong	Definition*
Electronic signature certificate	电子签名证书	数码证书 (digital certificate)	A certificate that is issued in electronic form. The information contained in the certificate can be used for identity verification of certificate holder, and such information usually includes the public key, name and email address of the user.
Electronic signature	电子签名	数码签署 (digital signature)	It refers to the data in electronic form contained in and attached to a data message to be used for identifying the identity of the signatory and for showing that the signatory recognizes what is in the message.
Certificate policy	证书策略	证书政策	A named set of rules that indicates the applicability of a certificate to a

Terminologies	Terminologies commonly used in Mainland	Terminologies commonly used in Hong Kong	Definition*
			particular community and/or class of application with common security requirements.
Certification authority	电子认证服务机构	核证机关	An institution that issues certificates to individuals or organizations.
Certification practice statement	电子认证业务规则	核证作业准则	A statement issued by a certification authority to specify its business practices for the issuance, management, revocation or renewal of certificates.
Registration authority	注册机构	登记机关	An entity that performs certain duties on behalf of a certification authority (excluding the issuance of certificates).
Private key	私钥	私人密码匙	The cryptographic key of a key pair used to generate an electronic signature.
Public key	公钥	公开密码匙	The cryptographic

Terminologies	Terminologies commonly used in Mainland	Terminologies commonly used in Hong Kong	Definition*
			key of a key pair used to verify an electronic signature.
Subject Name	主体名称	主体名称	It refers to the information of the name of certificate holder.
Distinguished name	甄别名	甄别名	It refers to the only information in the certificate for identifying the certificate user.
Subscriber	订户	登记人	It generally refers to the subject issued with a certificate.
Relying party	依赖方	依赖方	The recipient of a certificate who relies on the certificate and/or the electronic signature verified by the certificate.
Certificate revocation	吊销证书	撤销证书	It refers to the termination of certificate's validity by a certification authority.
Certificate suspension	挂起证书	暂时吊销证书	It refers to the temporary suspension of certificate's validity

Terminologies	Terminologies commonly used in Mainland	Terminologies commonly used in Hong Kong	Definition*
			by a certification authority.
Certificate revocation list	证书吊销列表	证书撤销清单	A list published by a certification authority containing information of the revoked or suspended certificates issued by it.
Reliance limit	赔偿限额	倚据限额	The monetary limit specified for reliance on a certificate.
Certificate password	证书口令	证书密码	It refers to the character string required to be entered by the subscriber when using the certificate.
Performance assessment	工作绩效考核	工作表现评核	The systematic process to assess the performance of CAs staff in carrying out their duties.

- The above definitions are for reference only. All such terminologies should be defined in accordance with the respective laws and regulations of the two places, the respective definitions commonly adopted in the two places or the definitions adopted in the agreed contents of relevant certificates of the two places.

Annex 1.2: Table of technical standards for mutual recognition of electronic signature certificates issued by Hong Kong and Guangdong and measures for adopting these standards

Relevant technical areas	Adoption of basic standards for mutual recognition of certificates between the two places
Certificate format	ITU X.509 v3 Or formats that comply with “GB/T 20518-2006 Information security technology - Public key infrastructure - Digital certificate format”
Certificate Revocation List	ITU X.509 v2
Repository	HTML, LDAP, HTTP
Cryptographic algorithm for electronic signatures	Group 1: • RSA, SHA-1 (to be transited to SHA-2) • Certificates and CAs’ certificates: RSA 2048 bits Or Group 2: • SM2, SM3
Security standards for cryptographic module	Standards approved by local regulatory authorities
Medium technology for digital certificates	PKCS#11 compatible devices Or devices that comply with the “Smart Card and Smart Token Cryptography Application Interface Specification” issued by the Office of State Commercial Cryptography Administration

Contents that should be contained in electronic signature certificates (In accordance with the “Arrangement for Mutual Recognition of Electronic Signature Certificates Issued by Hong Kong and Guangdong”)
1. Name of issuing certification authority; 2. Name of certificate holder; 3. Certificate serial number; 4. Expiry date of certificate; 5. Data for validating certificate holder’s signature; 6. Signature of issuing certification authority; 7. Certificate policy object identifier;

Relevant technical areas	Adoption of basic standards for mutual recognition of certificates between the two places
8. Other required contents.	

Promoting (requiring) the adoption of facilitation measures for cross-boundary certificates	
Certification practice statement	Promoting the adoption of XML and PDF formats as well as the provision of bilingual version (Chinese and English); **Requiring the provision of PDF format (Chinese), which should be taken as a norm.**
“Trust list” of certificates that comply with the requirements of mutual recognition (regulatory scope)	Promoting the adoption of HTML/PDF format (human-readable) and XML format (machine-readable). Trust list should be placed on secure websites or other suitable channels; **Requiring the provision of trust list in HTML/PDF format (human-readable) on secure websites or other suitable channels, which should be taken as a norm.**