THE CERTIFICATION PRACTICE STATEMENT

OF

THE POSTMASTER GENERAL

As

A Recognized Certification Authority under the Electronic Transactions Ordinance

for

Hongkong Post Bank-Cert (Personal)
Hongkong Post Bank-Cert (Corporate)
Hongkong Post Bank-Cert (Bank)

Date : 1 December 2022
OID : 1.3.6.1.4.1.16030.1.2.17

Table of Contents

PREAMBLE

The Electronic Transactions Ordinance (Cap. 553) ("Ordinance") sets out the legal framework for the Public Key infrastructure (PKI) initiative. The PKI facilitates the use of electronic transactions for commercial and other purposes. The PKI is composed of many elements, including legal obligations, policies, hardware, software, databases, networks, and security procedures.

Public Key Cryptography involves the use of a Private Key and a Public Key. A Public Key and its corresponding Private Key are mathematically related. The main principle behind Public Key Cryptography used in electronic transactions is that a message that is encrypted with a Public Key can only be decrypted with its corresponding Private Key, and a message that is encrypted with a Private Key can only be decrypted by its corresponding Public Key.

The PKI is designed to support the use of such a method for commercial and other transactions in Hong Kong Special Administrative Region ("Hong Kong SAR").

Under the Ordinance, the Postmaster General (or "HKPost") is a Recognized Certification Authority ("CA") for the purposes of the Ordinance and the PKI. Under the Ordinance the Postmaster General may perform the functions and provide the services of a CA by the officers of the Hong Kong Post Office.

Under the Ordinance HKPost may do anything that is expedient for the performance of the functions, and the provision of the services, of a CA and under the Code of Practice for Recognized Certification Authorities issued by the Government Chief Information Officer, HKPost may appoint agents or subcontractors to carry out some or all of its operations under HKPost's overall management and control.

Since 1 April 2007, HKPost has provided the CA services in exercise of the powers conferred on it under the Ordinance, and the CA services have been outsourced to a contractor under the over the overall management and supervision of HKPost.

HKPost remains a recognized CA under Section 34 of the Ordinance and any Contractor (including the sub-contractor of such Contractor) from time to time appointed by HKPost to perform any of the CA functions for its behalf is an agent of HKPost appointed pursuant to Section 3.2 of the Code of Practice for Recognized Certification Authorities issued by the Government Chief Information Officer under Section 33 of the Ordinance.

HKPost, as a recognized CA, is responsible under the Ordinance for the use of a Trustworthy System for the issuance, revocation or suspension, and publication in a publicly available Repository of recognized and accepted digital certificates for secure on-line identification.**The Bank-Cert certificates issued under this CPS are Recognized Certificates under the Ordinance and are referred to as "Certificates" or "Bank-Certs" or "Bank-Cert certificates" in this CPS (upper or lower case).**

This CPS sets out practices and standards for Bank-Cert certificates, and the structure of this CPS is as follows:

Section 1 provides an overview and contact details
Section 2 sets out the functions and obligations of the parties
Section 3 sets out identity and authentication requirements
Section 4 describes the operational requirements
Section 5 describes the security controls
Section 6 sets out how the Public/Private Key pairs will be generated and controlled
Section 7 describes the certificate and certificate revocation list profiles
Section 8 documents how this CPS will be administered

Section 9 sets out other business and legal matters

Appendix A contains a glossary
Appendix B contains a Hongkong Post Bank-Cert format
Appendix C contains a Hongkong Post Certificate Revocation List (CRL) format
Appendix D contains a summary of Hongkong Post Bank-Cert features
Appendix E contains a list of Hongkong Post Bank-Cert Registration Banks (RBs), if any
Appendix F describes lifespan of CA root certificates

1. INTRODUCTION

1.1 Overview

This Certification Practice Statement ("CPS") is published for public knowledge by HKPost and specifies the practices and standards that HKPost employs in issuing, revoking or suspending and publishing Bank-Cert certificates.

The Internet Assigned Numbers Authority ("IANA") has assigned the Private Enterprise Number 16030 to HKPost. For identification purpose, this CPS bears an Object Identifier ("**OID**") "**1.3.6.1.4.1.16030.1.2.17**" (see description of the field "Certificate Policies" in **Appendix B**).

This CPS sets out the roles, functions, obligations, and potential liabilities of the participants in the system used by HKPost. It specifies the procedures used to confirm the identity of all Applicants for certificates issued under this CPS and describes the operational, procedural, and security requirements of HKPost.

Bank-Cert certificates issued by HKPost in accordance with this CPS will be relied upon by Relying Parties and used to verify Digital Signatures. Each Relying Party making use of a HKPost issued certificate must make an independent determination that PKI based Digital Signatures are appropriate and sufficiently trusted to be used to authenticate the identity of the participants in the Designated Transaction. Subscriber must not make use of, and a Relying Party must not accept, the signature through a Bank-Cert certificate in any applications other than the type of Designated Transaction specified opposite to the name of the Registration Bank in **Appendix E for such type of Bank-Cert certificate.**

Under the Ordinance, HKPost is a recognized CA. **HKPost has designated the Bank-Certs issued under this CPS as Recognized Certificates.** As the Bank-Cert enjoys the status as a Recognized Certificate under the Ordinance, the Designated Transaction in which a Bank-Cert is used shall be given certain recognition and protection as stated in the Ordinance.

One of the characteristics of Bank-Cert certificate is the support of a newer Public Key infrastructure model, wherein a Subscriber remotely accesses the private key on a hardware security module ("HSM") hosted in a trusted Registration Bank. The Subscriber's key pair for Bank-Cert is generated and stored in the HSM.

A summary of the Bank-Cert features is in **Appendix D**.

1.2 Community and Applicability

1.2.1 Certification Authority

Under this CPS, HKPost performs the functions of a CA. HKPost is the only CA authorised to issue certificates under this CPS (see Section 2.1.1).

1.2.1.1 Effect

HKPost publishes Bank-Cert certificates in a Repository.

1.2.1.2 HKPost's Right to contract

HKPost may appoint a Contractor to perform some or all of the functions stated in this CPS and the Subscriber Agreement. Regardless of any such appointment, HKPost shall remain as, and perform the role of, the CA and the issuer of the Bank-Certs.

1.2.2 Registration Bank

HKPost mostly deals with the Applicant or Subscriber of Bank-Cert (Personal) or Bank-Cert (Corporate) via the Registration Bank. In this regard, it is the agent acting for the Applicant for, and Subscriber of, Bank-Cert (Personal) or (Corporate). The Registration Bank is also required to apply for and maintain its

own Bank-Cert (Bank) for the creation of digital signature on the e-cheque to be drawn on such Registration Bank as the drawee bank. A Bank-Cert (Bank) may also be used in other permissible types of Designated Transactions entered into by the Registration Bank as principal specified opposite its name in Appendix E (if any). In the case of Bank-Cert (Corporate) or (Personal), for some limited functions, itis also at the same time a sub-contractor of the Contractor (and therefore also acting for HKPost) in performing such functions. These functions are verification of the identity of the Applicant and in case of Bank-Cert (Corporate), also the identity and due authorisation of the Authorised Representative(s) and Authorised User(s) of the Applicant, at the time of application of a Bank-Cert by the Applicant (first time or renewal). Similarly, verification of the identity of the Subscriber (and of its Authorised Representative or Authorised User) in the case of any revocation request from such Subscriber. All other functions and obligations, including the functions to be performed by the Registration Bank arising from the usage from time to time of the Bank-Certs, regardless of the nature of the Designated Transactions, are functions and obligations undertaken by the Registration Bank whether as principal or as agent for its Subscriber but not as sub-contractor or agent for the Contractor and for HKPost.

1.2.3 End Entities

Under this CPS there are two types of end entities, Subscribers and Relying Parties. For Bank-Cert (Personal) and Bank-Cert (Corporate), a Subscriber is defined in **Appendix A**. For Bank-Cert (Bank), a Subscriber is a Registration Bank listed in **Appendix E**. Relying Parties are entities that have relied on any class or category of Bank-Cert for use in Designated Transaction referred to in **Appendix E**. Relying Parties should exercise their own judgment to decide whether to rely on a Bank-Cert. Subscribers who rely on a Bank-Cert of another Subscriber for use in a Designated Transaction of the Registration Bank referred to in **Appendix E** will be Relying Parties in respect of such a certificate. **The Bank-Certs will not be issued to minors.**

1.2.3.1 Location of the Private Key

A Bank-Cert will be stored in a hardware security module (HSM) to be hosted in a Registration Bank. HKPost will publish the certificate (with public key) in the Repository, for the public to download and for the purpose of verification of digital signature.

1.2.3.2 Subscriber's Right to delegate obligations to a Registration Bank

Applicant/Subscribers of Bank-Cert (Personal)/(Corporate) must delegate a Registration Bank (see **Appendix E**) to act on behalf of the Applicant/Subscriber, such as submission of all documents relating to the initial application, renewal application, use and revocation of the certificate issued under this CPS. Subscriber must authorise the Registration Bank to receive, keep and manage the key and certificate issued by HKPost to the Subscriber under this CPS. The Subscriber of Bank-Cert (Personal)/(Corporate) acknowledges that its Registration Bank may also at the same time act as the sub-agent/sub-contractor of the Contractor (and therefore acting for HKPost) for performing certain specified functions of the Registration Bank stated in this CPS. The Subscriber acknowledges that there is no conflict arising from such dual role, and it is beneficial to all parties that the Registration Bank should take on such dual role.

1.2.4 Classes of Subscribers

HKPost issues certificates under this CPS only to Applicants whose application for a certificate has been approved and who have confirmed their acceptance of a Subscriber Agreement in the appropriate form. Three classes of Bank-Certs may be issued under this CPS.

1.2.4.1 Bank-Cert (Personal) certificates

A Bank-Cert (Personal) certificate is issued to an individual who has a bank account with the Registration Bank and who is 18 years of age or over.

Bank-Cert (Personal) certificates issued via a particular Registration Bank can only be used by the Subscriber in Designated Transactions specified opposite the name of that Registration Bank in **Appendix E** for such type of Bank-Cert.

1.2.4.2 Bank-Cert (Corporate) certificates

A Bank-Cert (Corporate) certificate is issued to any organisation (including a corporation) that holds a bank account with the Registration Bank identified in the certificate. The organisation shall in its

application for the Bank-Cert identify one or more individuals (whether acting singly or jointly), who has been duly authorised by the organisation to use the Bank-Cert (Corporate) issued to that organisation.

Bank-Cert (Corporate) certificates issued via a particular Registration Bank can only be used by Subscriber in respect of the Designated Transactions specified opposite the name of that Registration Bank in **Appendix E** for such type of Bank-Cert.

1.2.4.3 Bank-Cert (Bank) certificates
A Bank-Cert (Bank) certificate is issued to a bank with a valid banking licence issued under Section 16 of the Banking Ordinance (a "Bank"). Each time a bank has successfully been issued with a Bank-Cert (Bank), its name and the scope of the Designated Transactions permissible for the Bank-Cert (Bank) shall be specified in **Appendix E**. The Applicant Bank may specifically identify a unit within the Bank which has the authority to configure, operate and maintain the Private Key of that the specified Bank-Cert (viz., "Authorised Unit"). Where there is no Authorised Unit being identified, the Registration Bank still warrants that the Registration Bank adopts sufficient control and security measure internally to ensure that any configuration, operation and maintenance of the Bank-Cert (Bank) (including its Private Key and associated IT system) will be duly authorised and monitored throughout the validity of the Bank-Cert (Bank).

Bank-Cert (Bank) certificates can only be used by the Registration Bank for use in the Designated Transactions specified opposite to the name of that Registration Bank in **Appendix E** for this type of certificate.

EACH REGISTRATION BANK UNDERTAKES TO HKPOST TO USE BANK-CERT (BANK) ONLY FOR THE DESIGNATED TRANSACTIONS SPECIFIED OPPOSITE ITS NAME IN APPENDIX E IN RESPECT OF SUCH CERTIFCATE BUT NOT FOR ANY OTHER PURPOSE.

1.2.5 Certificate Lifespan
The validity period of a certificate commences on the date the certificate is generated by the HKPost system.

The range of the validity period of Bank-Cert (Personal) and Bank-Cert (Corporate) Certificates issued under this CPS is specified in **Appendix E** depending upon the Registration Bank viz., whom the Certificate is issued. The Applicant when applying for a Bank-Cert shall decide on the validity period within such range and notify the same to the Registration Bank. As for Bank-Cert (Bank), the Registration Bank will also select the length of validity in its application for first time issue or renewal within the range specified in **Appendix E.**

1.2.6 Application
All first applications and applications of renewal of a Bank-Cert will require the Applicants (represented by Authorised Representative in the case of Bank or organisation) to submit their applications as described in Sections 3 and 4 of this CPS.

1.2.7 Applicability

1.2.7.1 General Purpose
A type of Certificates issued via a Registration Bank (whether it be Bank-Cert (Personal) certificates or Bank-Cert (Corporate) certificates) is to be used exclusively for the Designated Transactions specified opposite the name of the Registration Bank via which the Certificate is issued as specified in **Appendix E**.

A Bank-Cert (Bank) issued to a Registration Bank is to be used exclusively in Designated Transactions specified opposite the name of that Registration Bank.

1.2.7.2 Restriction on use
These certificates may only be used for the purposes and in the manner described within this CPS.

1.2.7.3 Prohibitions on use

These certificates are not to be used for transactions other than the Designated Transactions defined in **Appendix E**.

1.3 Contact Details

Subscribers may send their enquiries, suggestions or complaints by:

Mail to : Hongkong Post Certification Authority, Kowloon East Post Office Box 68777
Tel: 2921 6633
Fax: 2775 9130
Email: enquiry@eCert.gov.hk

1.4 Complaints Handling Procedures

HKPost will handle all written and verbal complaints expeditiously. Upon receipt of the complaint, a full reply will be given to the complainant within 10 working days. In the cases where full replies cannot be issued within 10 working days, interim replies will be issued. As soon as practicable, designated staff of HKPost will contact the complainants by phone, email or letter mail to acknowledge and reply to the complaints.

2. GENERAL PROVISIONS

2.1 Functions and Obligations in relation to Bank-Cert (Personal) and Bank-Cert (Corporate)

HKPost's functions are defined and limited by this CPS and by the terms of the contracts with Subscribers in the form of a Subscriber Agreement.

2.1.1 CA Functions in relation to Bank-Cert (Personal) and Bank-Cert (Corporate)
In accordance with this CPS, HKPost performs the following functions in relation to the applications for Bank-Cert (Personal) and Bank-Cert (Corporate) (all or any of the functions may be performed by the Contractor under the management and control of HKPost):

a) Receive application for a Bank-Cert via a Registration Bank
b) Process application for a Bank-Cert via a Registration Bank
c) Notify Applicants, via a Registration Bank, approval or rejection of their applications
d) Issue and publish certificates in the Repository based on the CSR submitted;
e) Suspend or revoke certificates and publish revised Certificate Revocation Lists in a timely manner; and
f) Notify Subscribers, whether via Registration Bank or directly, the suspension or revocation.

2.1.2 Registration Bank Obligations in relation to Bank-Cert (Personal) and Bank-Cert (Corporate)

In relation to Bank-Cert (Personal) and Bank-Cert (Corporate), a Registration Bank performs the following functions on behalf of its customer being the Applicant or Subscriber and also for the function specified in the second bullet point only at the same time as sub-contractor of the Contractor (and therefore also acting for HKPost) :-

- Receiving and processing certificate applications from the Applicant who is its customer (i.e. a holder of a bank account opened with such Registration Bank) including obtaining evidence of identity and certificate applications information;
- Verifying the identity of the Applicant and in the case of Bank-Cert (Corporate), also the identity and due authorisation of the Authorised Representative(s) and Authorised User(s) of the Applicant, both in first time application and renewal of Bank-Cert (as more particularly specified in Sections 3.1.1, 3.15 and 3.2.1); verifying the identity of the Subscriber and in the case of Bank-Cert (Corporate), also the identity of the Authorised Representative(s) or Authorised User(s), in any request for revocation of Bank-Cert;
- Submitting certificate requests on behalf of the Applicant to HKPost containing information in relation to the Applicant and its Authorised Representative(s) and Authorised User(s)that matches with the information known to the Registration Bank(viz., information established in KYC procedures) at time of submission, together with a Subscriber's Terms and Conditions confirmed by the Applicant;
- Receive notification of approval or rejection of the Applicant's application on behalf of the Applicant, and convey such notification to the Applicant;
- When applications are approved by HKPost and are Issued, on behalf of the Applicant, Accepting the issued Bank-Cert from HKPost in a secure manner;
- Informing Subscribers of their obligations, including their duty to safeguard their security token that is required for accessing the private keys stored in the Registration Bank, and promptly report any compromise or suspected compromise;
- Quoting the Applicant/Subscriber's information through the use of a unique customer identity number ("CIN") assigned, that must uniquely reference to the Subscriber's evidence of identity, for submission of Bank-Cert application;
- Ensuring that the generation of the Subscriber's Key Pair and its storage only in a hardware security module (HSM) of the Registration Bank;
- Ensuring the Safe custody of the Subscriber's Key Pair;
- Ensuring that for each type of Bank-Cert, it is used for the corresponding Designated Transactions specified opposite its name in **Appendix E** only;

- Ensuring that the use by a Subscriber of a Bank-Cert certificate for purposes other than the Designated Transaction referred to in **Appendix E** specified opposite its name will not be permitted;
- Ensuring that only the Subscribers (or in the Bank-Cert (Corporate), only the Authorised User specified in the Bank-Cert) can make use of their Private Key to generate digital signature for the relevant Designated Transaction;
- Verifying the identity of the Subscriber, and in the case of Bank-Cert (Corporate), also the identity of the Authorised User(s) of the Subscriber, before the Subscriber is permitted using its Bank-Cert in Designated Transaction;
- Each Time a Bank-Cert(Personal) or (Corporate) issued via it is used in a Designated Transaction, ensuring the name of the drawer of the e-cheque matches the name of the Subscriber as stated in that Bank-Cert;
- Each time a Bank-Cert (Corporate) issued via it is used in a Designated Transaction, ensuring the name of the Authorised User as stated in the e-cheque matches the name of the Authorised User as stated in the Bank-Cert;
- Each time a Bank-Cert (Personal) or (Corporate) issued via is used in a Designated Transaction, ensuring that the Bank-Cert has not expired or revoked or suspended based on the information as shown in the Repository and the CRL. Where such Bank-Cert is expired or revoked or suspended, ensuring that the Designated Transaction will not be processed or completed using such Bank-Cert;
- Keeping all records and information of the Subscriber in accordance with the terms of this CPS and the Subscriber Agreement throughout the validity of the relevant certificate;
- Complying with all notices, instructions and manuals issued by HKPost from time to time; and
- Complying with this CPS.

2.1.3 Contractor Obligations in relation to Bank-Cert (Personal) and Bank-Cert (Corporate)

The Contractor is responsible only to HKPost under the terms of the Contract between HKPost and the Contractor under which the Contractor has been appointed by HKPost as its agent to operate and maintain the system for the issuance of certificates. In addition, HKPost may appoint the Contractor or any other agents or contractors from time to time to carry out all or any of its functions stated in this CPS under HKPost's overall management and control.

2.1.4 Obligations of Applicant and Subscriber of Bank-Cert (Personal) and Bank-Cert (Corporate)

2.1.4.1 Applicant Obligations

Without prejudice to its other obligations as stated in the CPS and the Subscriber Agreement, an Applicant of a Bank-Cert (Personal) or Bank-Cert (Corporate) is responsible for all of the following:

a) Completing the application procedures properly and confirming acceptance of a Subscriber Agreement (by the Authorised Representative acting for and on behalf of the Subscriber in the case of applying Bank-Cert (Corporate)) in the appropriate form and performing the obligations placed upon them by that Agreement, and ensuring accuracy of representations and warranties made in the certificate application;
b) Authorising the Registration Bank to perform the tasks mentioned in Section 2.1.2 above; and
c) Acknowledging that by submitting a Bank-Cert application, they authorise the publication of the Bank-Cert to any other person or in the HKPost's Repository.

2.1.4.2 Subscriber Obligations

Without prejudice to its other obligations as stated in the CPS and the Subscriber Agreement, a Subscriber of a Bank-Cert (Personal) or Bank-Cert (Corporate) is responsible for all of the following:

a) Agreeing that the key pair is generated by the Registration Bank in a hardware security module ("HSM") and an environment within the Registration Bank's premises on behalf of the Subscriber.
b) Following the requirements specified in this CPS concerning the application for first time issue and renewal of Certificates.
c) Notifying the Registration Bank identified in the relevant certificate immediately from time to time of any change in the information in the certificate provided by the Subscriber or of any change in

the Authorised Representative or Authorised User.

d) Notifying the Registration Bank identified in the relevant certificate immediately of any occurrence or event which may entitle HKPost, upon the grounds set out in Section 4.3 below, to revoke the certificate.
e) Agreeing that by having been issued or accepting a certificate they warrant and represent to HKPost and to all Relying Parties that during the validity period of the certificate, the warranties and representations stated in Section 9.6.3 are and will remain true accurate and complete.
f) Not using a certificate in a transaction on becoming aware of any ground upon which HKPost, could suspend or revoke it under the terms of the CPS, or after the Subscriber has made a revocation request or has received from HKPost, a Revocation Notice under Section 4.3.
g) Upon becoming so aware of any ground upon which HKPost could suspend or revoke the certificate, or upon it itself has made a revocation request or upon having received from HKPost a Revocation Notice under Section 4.3, immediately notifying Relying Parties in any transaction that remains to be completed at the time, that the certificate used in that transaction is liable to be suspended or revoked (either by HKPost or at its own request) and stating in clear terms that, as this is the case, the Relying Parties should not rely upon the certificate in respect of the transaction.

2.1.5 Relying Party Obligations

Without prejudice to its other obligations as stated in the CPS and the Subscriber Agreement, a Relying Party relying upon a Bank-Cert is responsible for all of the following:

a) Relying on such certificates only when the reliance is reasonable and in good faith in light of all the circumstances known to the Relying Party at the time of the reliance.
b) Before relying upon a Bank-Cert certificate determining that the use of the Bank-Cert certificate is appropriate for its purposes in the corresponding Designated Transaction under this CPS.
c) Acknowledging that HKPost does not undertake any responsibility or duty of care to Relying Parties if the Bank-Cert certificate is used or relied upon for any purposes other than the corresponding Designated Transaction specified opposite the name of the Registration Bank referred to in **Appendix E** of this CPS for such Certificate issued via or in favour of, such Registration Bank.
d) Perform all acts as specified in Section 9.6.4.

2.2 Functions and Obligations in relation to Bank-Cert (Bank)

HKPost's functions are defined and limited by this CPS and by the terms of the contracts with Subscribers in the form of a Subscriber Agreement in relation to a Bank-Cert (Bank).

2.2.1 CA Functions in relation to Bank-Cert (Bank)

In accordance with this CPS, HKPost performs the following functions in relation to the applications for Bank-Cert (Bank) Certificates (all or any of the functions may be performed by the Contractor under the management and control of HKPost):

a) Receive application for a Bank-Cert (Bank) from a bank which has a valid banking licence issued under Section 16 of the Banking Ordinance (Cap 155 of the Laws of Hong Kong)
b) Process application for a Bank-Cert (Bank);
c) Notify approval or rejection of its application;
d) Issue and publish certificates in the Repository;
e) Suspend or revoke certificates and publish revised Certificate Revocation Lists based on such suspension or revocation; and
f) Notify the Registration Bank the suspension or revocation of its Bank-Cert (Bank).

2.2.2 Contractor Obligations in relation to Bank-Cert (Bank)

The Contractor is responsible only to HKPost under the terms of the Contract between HKPost and the Contractor under which the Contractor has been appointed by HKPost as its agent to operate and maintain the system for the issuance of certificates. In addition, HKPost may appoint the Contractor or any other agents or contractors from time to time to carry out all or any of its functions stated in this CPS under HKPost's overall management and control.

2.2.3 Obligations of Applicant and Subscriber of Bank-Cert (Bank)

2.2.3.1 Applicant Obligations

Without prejudice to its other obligations as stated in the CPS and the Subscriber Agreement, an Applicant of a Bank-Cert (Bank) is responsible for all of the following:

a) Completing the application procedures properly and confirming acceptance of a Subscriber Agreement (by the Authorised Representative acting for and on behalf of the Bank), and ensuring accuracy of representations in the application; and
b) Acknowledging that by submitting a Bank-Cert application, it authorises the publication of the information stored in the Bank-Cert to any other person or in the HKPost's Repository.

2.2.3.2 Subscriber Obligations

Without prejudice to its other obligations as stated in the CPS and the Subscriber Agreement, a Subscriber of a Bank-Cert (Bank) is responsible for all of the following:

a) Agreeing that the key pair is generated by the Registration Bank in a hardware security module ("HSM") and an environment within the Registration Bank's premises on behalf of the Subscriber.
b) Following the procedures specified in this CPS concerning first time issue and renewal of Certificates.
c) Notifying HKPost immediately of any change from time to time in the certificate provided by the Subscriber or of any change in the Authorised Representative or any change of the Authorised Unit.
d) Notifying HKPost immediately of any occurrence or event which may entitle HKPost, upon the grounds set out in Section 4.3 below, to revoke the certificate.
e) Agreeing that by having been issued or accepting a certificate it warrants to HKPost and represents to all Relying Parties that during the validity period of the certificate, the warranties and representations stated in Section 9.6.3 are and will remain true, accurate and complete.
f) Not using a certificate in a transaction on becoming aware of any ground upon which HKPost could suspend or revoke it under the terms of the CPS, or after it itself has made a revocation request or has received a Revocation Notice from HKPost under Section 4.3.
g) Upon becoming so aware of any ground upon which HKPost could suspend or revoke the certificate, or upon it itself making a revocation request or upon having received a Revocation Notice from HKPost, immediately notifying Relying Parties in any transaction that remains to be completed at the time, that the certificate used in that transaction is liable to be or is to be suspended or revoked (either by HKPost or at the Subscriber's request) and stating in clear terms that, as this is the case, the Relying Parties should not rely upon the certificate in respect of the transaction.

2.3 Subscription Fees

The subscription fee and administration fee shall be paid by Subscribers or the Registration Bank. For details of the arrangement of fees charged in respect of Bank-Certs, please see **Appendix E** under the heading of the relevant Registration Bank. HKPost reserves its absolute right to review and determine the subscription fee and administration fee from time to time.

2.4 Publication and Repository

Under the Ordinance, HKPost maintains a Repository that contains a list of accepted certificates issued under this CPS, the current certificate revocation list ("CRL"), the HKPost Public Key, a copy of this CPS, and other information related to Bank-Cert certificates. The Repository is available on a substantially 24 hours per day, 7 days per week basis, subject to scheduled maintenance of an average of 2 hours per week and any emergency maintenance. HKPost promptly publishes each certificate accepted by and issued to the Subscriber under this CPS in the Repository. The HKPost Repository can be accessed at URLs as follows:-

http://www.eCert.gov.hk
ldap://ldap1.eCert.gov.hk

or alternatively

http://www.hongkongpost.gov.hk
ldap://ldap1.hongkongpost.gov.hk

2.4.1 Certificate Repository Controls

The Repository is maintained in a location that is viewable on-line and is protected from unauthorised access.

2.4.2 Certificate Repository Access Requirements

Only persons authorised by HKPost have access to the Repository to update and modify the contents.

2.4.3 Certificate Repository Update Cycle

The Repository is updated at 0915, 1415 and 1900 HKT as stated in paragraph 2 of Appendix C.

2.4.4 Permitted Use of information Contained in the Repository

The information, including any personal data, contained in the Repository is published under the Ordinance and for the purpose of facilitating the conduct of lawful electronic transactions or communications.

2.5 Compliance Assessment

Compliance assessments conducted on the HKPost's system of issuing, revoking or suspending and publishing Bank-Certs, including the functions performed by the Registration Bank, to determine if this CPS is being properly followed are performed at least once in every 12 months in accordance with the requirements set out in the Ordinance and the Code of Practice for Recognized Certification Authorities.

3. IDENTIFICATION AND AUTHENTICATION REQUIREMENTS

3.1 First Time Application

3.1.1 Initial Application by applicant of Bank-Cert (Personal) or (Corporate)

In respect of Bank-Cert (Personal) or (Corporate) applications lodged by an Applicant, the Applicant must already be a customer of the Registration Bank. The Registration Bank is required to comply with the due diligence requirements concerning verification of the identity of customer in accordance with the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (AMLO), Cap 615 of the Laws of Hong Kong and the Guideline on Anti-Money Laundering and Counter-Terrorist Financing issued under Section 7 of the AMLO. The Registration Bank will verify the identity of the Applicant (and in the case of an Applicant being an organisation, the identity of the Authorised Representative(s) and Authorised User(s)) in accordance with the requirements of the AMLO and the aforesaid Guideline and this review and verification are referred as "Know-Your-Customer" procedures or "KYC" procedures throughout this CPS.

3.1.2 Subscriber's Name appearing on the Bank-Cert (Personal) or (Corporate)

The Subscriber for a Bank-Cert (Personal) or (Corporate) certificate is identified in the certificate with a Subject Name consisting of the Subscriber's name as verified by the Registration Bank in accordance with KYC procedures as mentioned above.

3.1.3 Initial application by a Registration Bank

3.1.3.1 In respect of Bank-Cert (Bank) applications, the application must be submitted at a designated HKPost premises duly signed by the Authorised Representative, or premises of other organisations designated by HKPost, and present proof of identity of the Authorised Representative.

3.1.3.2 Applications for Bank-Cert (Bank) certificates should be made at a designated HKPost premises, or premises of other organisations designated by HKPost by the personal attendance of the Applicant's Authorised Representative who is required to present his/her own HKID Card or passport. At the sole discretion of HKPost, it may be permitted for submission of the application accompanied by a copy of the Authorised Representative's own HKID Card or passport with the Authorised Representative's signature, in lieu of the Authorised Representative's personal attendance, provided that (a) the Authorised Representative's identity has been authenticated in another application for Bank-Cert(Bank), and the Authorised Representative has personally appeared at a designated HKPost premises for identity verification in that application; and (b) sufficient material or avenue is available for re-affirming the identity of the Authorised Representative, such as confirmation with the Authorised Representative through telephone call or checking the Authorised Representative's signature against that on past application records. In case of doubt, HKPost may decline the application.

3.1.3.3 Each application for Bank-Cert (Bank) must be accompanied by the following documentation:-

a) a copy of the power of attorney duly executed by the Applicant and duly certified as true and complete of the original on each page of the power of attorney by a Hong Kong solicitor (with practising certificate) delegating the power to the Authorised Representative to apply for the Bank-Cert (Bank) on the terms set out in the Subscriber Agreement, and this CPS and where applicable, the Authorised Unit authorised to configure, operate and maintain the Bank-Cert, for the Designated Transactions specified therein on behalf of the Applicant; OR

b) a copy of the board resolution by the board of directors of the Applicant or extract thereof and duly certified as true and complete by a director or company secretary of the Applicant authorising the Authorised Representative to apply for the Bank-Cert (Bank) on the terms set out in the Subscriber Agreement and this CPS, and where applicable, the Authorised Unit authorised to configure, operate and maintain the Bank-Cert, for the Designated Transactions specified therein; AND
c) a copy of the Hong Kong Identity Card or passport of the Authorised Representative; AND
d) evidence that the Applicant is a licensed bank under the Banking Ordinance (Cap 155 of the Laws of Hong Kong) as appearing on the register kept by the Monetary Authority and published on its website; AND

e) a copy of the signed sub-contract between the Applicant and the Contractor in form and substance to the satisfaction of HKPost under which, inter alia, the Applicant undertakes to perform the Registration Bank functions and obligations as stated in this CPS.

3.1.4 Bank-Cert (Bank) certificates

The Subscriber of a Bank-Cert (Bank) certificate is identified in the certificate with a Subject Name (referred to in **Appendix B**) consisting of:

a) The Bank's name as shown on the valid banking licence issued to the bank under Section 16 of the Banking Ordinance (Cap 155 of the Laws of Hong Kong).

3.1.5 The Authorised Representative and the Authorised Users

Authorised Representative is the person who has the authority to apply for the Bank-Cert (Corporate) for the organisation and whose name will not be identified in the Certificate. The Registration Bank should verify the authority by requesting from the organisation a board resolution or other documentary evidence to the satisfaction of the Registration Bank authorising the Authorised Representative to submit application for Bank-Cert (Corporate) to be issued in the names of the persons stated therein (viz., Authorised Users) on the terms set out in the Subscriber Agreement and this CPS, and where applicable with the specified maximum amount for each Designated Transaction which may be transacted by the Bank-Cert (Corporate) issued to each such person. An Authorised User to be issued with Bank-Cert (Corporate) to use the same on behalf of the relevant organisation will be named as the Authorised User in that Certificate. This would mean that after successful application for the Bank-Cert (Corporate), this person, after having his identity authenticated in the 2-factor authentication process in the on-line banking platform operated by the Registration Bank, would have the authority to use the Bank-Cert (Corporate) in the Designated Transactions specified opposite the name of the relevant Registration Bank for this type of Bank-Cert in **Appendix E**. Any monetary limit on the value of the Designated Transaction which may be transacted by an Authorised User on behalf of an organisation should be separately stipulated by the organisation through the available mechanism provided by the Registration Bank. The Bank-Cert (Corporate) does not on its own impose any monetary limit. Different Bank-Cert (Corporate) marked for different Authorised Users named therein may be issued.

For Bank-Cert (Bank), other than the Authorised Representative who is responsible for applying for the Bank-Cert (Bank) for the Registration Bank, there may be an Authorised Unit within the Registration Bank which is authorised to configure, operate and maintain the Bank-Cert (Bank) in Designated Transactions for such Bank-Cert (Bank).

3.1.6 Names in Chinese Language

All Bank-Certs are issued in English language but will contain the Subscriber's Chinese name (to be stated in Chinese characters), where the Subscriber does have a name in Chinese and that such Chinese name is provided by the Registration Bank to the HKPost at the time of application. The existence and accuracy of the Chinese name shall be verified by the Registration Bank in accordance with the KYC procedures before providing the same to the HKPost.

3.1.7 Infringement and Violation of Trademarks

Applicants and Subscribers warrant to HKPost that the information supplied by them in the Bank-Cert application process does not infringe or violate in any way the trademarks, service marks, trade name, company name, or any other intellectual property rights of any person.

3.1.8 Method to Prove Authority to use the Private Key

3.1.8.1 The Registration Bank carries out the Digital Signature generation through the use of the Private Key kept by it on behalf of the Subscriber (in the case of usage of Bank-Cert (Personal) or (Corporate). Subscribers' Private Keys are kept securely by the Registration Bank. In respect of Bank-Cert (Personal), the Subscriber is required to pass through strong authentication procedure (viz., 2-factor authentication procedure) for the authentication of his identity as stipulated by the Registration Bank before he may invoke the use of the Private Key kept by the Registration Bank on his behalf for the generation of digital signature. In the case of Bank-Cert (Corporate), the Authorised User of the Subscriber is required to pass through strong authentication procedure (viz 2-factor authentication procedure) for the authentication of his identity as stipulated by the Registration Bank before he may invoke the use of the Private Key kept by the Registration Bank on behalf of the Subscriber for the

generation of digital signature.

3.1.8.2 The Authorised Unit of the Registration Bank or other authorised personnel (where applicable) through its IT system is required to pass through strong authentication method designed by the Registration Bank before it may configure, operate and maintain the system storing the Private Key kept by the Registration Bank for the generation of its digital signature.

3.1.9 Subsequent Authentication of Identity of Bank-Cert (Corporate) or (Bank) Subscriber

3.1.9.1 For Subscriber to whom a Bank-Cert (Corporate) certificate with a validity period of 2 years or above is issued, the Registration Bank may verify again the existence of the Subscriber one or more times during the validity period based on the KYC procedures. The Registration Bank shall inform HKPost to suspend or revoke the certificates issued to that Subscriber in accordance with the provisions set out in this CPS if the Subscriber's existence can no longer be ascertained. However no verification of the continued authorisation of the Authorised Representative or Authorised User will be done. It is incumbent on the Subscriber to inform the Registration Bank that any person who was previously acting as the Authorised Representative or Authorised User no longer has the authority to do so. It is also incumbent on the Subscriber to ensure that any ex-Authorised Representative and ex-Authorised User will return all security tokens or other devices used for accessing the on-line platform through the 2-factor authentication system and to change the password immediately. Neither HKPost nor the Registration Bank will be responsible in the event that the Subscriber has failed to do so.

3.1.9.2 For Subscriber with a Bank-Cert (Bank) certificate with a validity period of 2 years or above, HKPost will verify again the due and lawful existence of the Registration Bank and its status as a licensed bank with a valid banking licence issued under the Banking Ordinance (Cap 155 of the Laws of Hong Kong), approximately at the end of each anniversary date of the Bank-Cert certificate during the validity period. The authorisation of the Authorised Representative, and the Authorised Unit (if any) will also be verified and confirmed with the Registration Bank. HKPost may suspend or revoke the certificates issued to the Registration Bank in accordance with the provisions set out in Section 4.3.1 (Certificate Suspension and Revocation) of this CPS if the Registration Bank's existence cannot be attested.

3.1.9.3 For avoidance of doubt, the Subscriber (whether it be Bank-Cert (Corporate) or (Bank) shall be solely responsible for the due authorisation of Authorised Representative(s) and Authorised User(s) nominated by it (and the Authorised Unit in the case of Bank-Cert (Bank)) and ensuring that the information of such Authorised Representative, Authorised User, and where applicable the Authorised Unit provided to HKPost and the Registration Bank is true and correct. The Subscriber shall in any event be bound by any transactions duly authenticated by a certificate issued pursuant hereto irrespective of the identity of the person who makes use of the Bank-Cert with or without the authority of such Subscriber. HKPost disclaims all liabilities arising from the unauthorised application or use of the Bank-Cert by any person.

3.2 Certificate Renewal

3.2.1 Renewal of Bank-Cert (Personal), Bank-Cert (Corporate) Certificates

The Registration Bank identified in the Bank-Cert (Personal)/(Corporate)will notify the Subscribers to renew their certificates at least one month prior to the expiry of the certificates' validity period. The certificates can be renewed before expiry of their validity at the request of the Subscriber and the discretion of HKPost. HKPost may not perform renewal of expired, suspended or revoked certificates. The Subscriber (or the Authorised Representative of the Subscriber (in the case of organisation)) shall authorise the Registration Bank to submit renewal application of Bank-Cert (Personal) or Bank-Cert (Corporate) on behalf of the Subscriber prior to the expiry of the certificates' validity period. In the case of the Subscriber being an organisation, the Registration Bank should verify the authority of the Authorised Representative by requesting from the organisation a board resolution or other documentary evidence to the satisfaction of the Registration Bank authorising the Authorised Representative to submit application for renewal Bank-Cert (Corporate) to be issued in the names of the persons stated therein (viz., Authorised Users) on the terms set out in the Subscriber Agreement and this CPS, and

where applicable with the specified maximum amount for each Designated Transaction which may be transacted by the Bank-Cert (Corporate) issued to each such person. The Registration Bank will also continue to conduct periodic KYC review depending on the customer risk ranking which periodic review may or may not coincide the time upon renewal. Such periodic review will be performed as agent on behalf of the Contractor and therefore as sub-agent on behalf of the HKPost as agent for the HKPost.

3.2.2 Renewal of Bank-Cert (Bank) Certificate

HKPost will notify Subscribers to renew the Bank-Cert (Bank) certificates prior to the expiry of the certificates' validity period. The certificates can be renewed before expiry of their validity at the request of the Subscribers and the discretion of HKPost. HKPost may not perform renewal of expired, suspended or revoked certificates.

Upon renewal, the terms and conditions of the original Subscriber Agreement will apply to the renewed certificate, except insofar as such terms are incompatible with the terms of the Subscriber Agreement current at the date of renewal or the CPS current at the date of renewal. In the case of such incompatibility the terms of the current Subscriber Agreement and the current CPS will prevail. Applicants for renewal should read the terms of the Subscriber Agreement and the CPS current at the date of renewal before submitting the renewal requests.

3.2.3 Expired Bank-Cert

HKPost will still publish information of all expired, revoked and suspended certificates in the Repository with an annotation about their expired or revoked or suspension status and certificates which have been revoked or suspended are also published in CRL.

The time for updating the CRL for noting a Bank-Cert with revocation or suspension status is specified in Section 4.4.3(a) below. As for the time for updating the Repository for noting a Bank-Cert with expired status, HKPost will exercise reasonable endeavours to ensure that within 2 full working days after expiry, it will update the expired status on the Repository.

But just like the CRL, the latest Repository will only be published at the hours specified in Section 2.4.3 above and the latest status as updated by the HKPost will not be shown until such time it is published.

Registration Banks shall verify the validity period of a Subscriber's Bank-Cert issued via it from the Repository and CRL and check whether the Bank-Cert is expired or revoked or suspended, before allowing the Subscriber to use the Bank-Cert for Designated Transaction. It is incumbent on the Registration Bank acting for the Subscriber to do the aforesaid verification to ensure that where a Bank-Cert issued via it has expired but not renewed or revoked or suspended, such Bank-Cert can no longer be used by its Subscriber or any other person.

4. OPERATIONAL REQUIREMENTS

4.1 Bank-Cert (Personal) and Bank-Cert (Corporate) Certificates

Unless otherwise specified, all provisions in this Section 4.1 apply to the application and issuance of Bank-Cert (Personal) and Bank-Cert (Corporate).

4.1.1 Certificate Application

4.1.1.1 Applicants for Bank-Cert (Personal) or Bank-Cert (Corporate) (acting through its Authorised Representative) under this CPS (first time application or renewal) must submit a request for certificate either electronically (viz., via online backing and passing through the two-factor authentication) or in paper form, and accept a Subscriber terms and conditions for Bank-Cert (Personal) or Bank-Cert (Corporate) as the case may be. The authorisation evidence as required in Section 3.1.5 above or 3.2.1 above (where applicable) should be submitted by the Applicant in the case of organisation. The Registration Bank on behalf of the Applicant will complete and submit an application on behalf of the Applicant to the HKPost.

4.1.1.2 By submitting a Bank-Cert application to the Registration Bank, the Applicant authorises the Registration Bank to provide its personal data (in the case of the Applicant being an individual) and its other information kept by the Registration Bank and submit its application on its behalf to the HKPost, and to receive notification from the HKPost concerning the result of the application, and to signify Acceptance of the Bank-Cert (if the application is successful) by way of the Registration Bank receiving the Bank-Cert from HKPost. Subject to Section 4.1.1.3 below, the Applicant also authorises the Bank to submit to HKPost all such information as HKPost may require in order to process the application. Upon the application is successful, the Subscriber authorises HKPost to publish the issued Bank-Cert in the HKPost Repository.

4.1.1.3 The authentication of the identity of the Applicant relies on the authentication of identity of Applicant as stipulated in Sections 3.1of this CPS. For authentication of identity of the Applicant for Bank-Certs (Personal) and (Corporate), due to confidentiality duty owing by the Registration Bank to its customers, the Registration Bank will not provide any document to the HKPost or its Contractor to enable HKPost or its Contractor to separately verify the identity of the Applicant of the relevant Bank-Cert or the identity or due authorisation of the Authorised Representative (in the case of Bank-Cert (Corporate)) (in the case of first time application and renewal). Similarly for verification of identity of the Subscriber (and of its Authorised Representative or Authorised User) in the case of revocation request under Section 4.3.2.3. The accuracy and completeness of information to be provided by the Registration Bank to HKPost including the name of the Applicant and the Authorised User will be verified and/or reviewed by the Registration Bank as sub-contractor on behalf of the Contractor and therefore also acting for the HKPost. In the event of a change of Contractor, the Registration Bank and the new Contractor should enter into a new sub-contracting arrangement under which the Registration Bank will continue to undertake the aforesaid Registration Bank functions as sub-contractor. HKPost reserves the right to revoke the Registration Bank's Bank-Cert (Bank) in the event that no such sub-contracting arrangement can be put in place. Without prejudice to the warranties set out in Section 40 of the Ordinance, it is confirmed by HKPost that no further verification will be conducted by HKPost concerning such information and HKPost will receive the information on an as is basis.

4.1.1.4 The Registration Bank must have two separate units COMPRISING DIFFERENT STAFF processing an application for Bank-Cert. One unit ("Front Office") shall input the Applicant's information from its customer database including

(a) in the case of the Applicant being an individual: name, Hong Kong Identity Card or Passport number, date of birth, CIN and SRN (if renewal); and

(b) in the case of the Applicant being an organisation: the name, address of principal place of business in Hong Kong, the certificate of incorporation or certificate of change of name number, business registration certificate number, and the name, date of birth, CIN and SRN (if renewal) of the Authorised User;

4.1.1.5 Another unit within the Registration Bank ("Back Office") shall be responsible for verifying the accuracy of the data input in the application form based on the information available in the Registration Bank's customer database.

4.1.1.6 All application information transmitted electronically between the Registration Bank and HKPost must use a protocol prescribed by HKPost from time to time.

4.1.2 Certificate Issuance

4.1.2.1 Following the identity verification process by the Back Office, the Front Office of the Registration Bank on behalf of the Applicant will generate the Private Key and Public Key of the respective Applicant in a HSM and a secure environment within the Registration Bank's premises. The Registration Bank is responsible for ensuring that the Private Key will not be tampered with.

4.1.2.2 The Front Office of the Registration Bank on behalf of the Applicant will generate the Certificate Signing Request (CSR) containing the Public Key in a Trustworthy System and environment within the Registration Bank's premises, and transmits the CSR to the Back Office of the Registration Bank for further processing.

4.1.2.3 The Back Office shall prepare an XML Interface file, containing the Applicant's data, the record of the Applicant's acceptance of the Subscriber Agreement and the CSR generated by the Front Office. The XML Interface file shall be submitted to HKPost.

4.1.2.4 Upon receipt of the CSR from the Back Office of the Registration Bank, HKPost will verify that the Registration Bank is in custody of the corresponding Private Key by checking the digital signature on the CSR structure with the contained Public Key. HKPost will not have possession of the Applicants' Private Keys.

4.1.2.5 Upon verifying the Registration Bank's custody of the corresponding Private Key, HKPost will generate the certificate in which the Applicant's Public Key will be included. The issued Bank-Cert will then be transmitted to the Registration Bank identified in the issued Bank-Cert in a secure manner. The Back Office of the Registration Bank will then transmit the issued Bank-Cert to the Front Office of the Registration Bank.

4.1.2.6 The Front Office will activate the Bank-Cert with corresponding Private Key by loading into the HSM, link Bank-Cert to the Customer Account, and notify the Applicant via internet banking showing the SRN and the Certificate Data.

4.1.2.7 Acceptance is signified by the Registration Bank's receipt on behalf of the Applicant. Upon such Acceptance, in accordance with Section 36 of the Ordinance, the Issued and Accepted Bank-Cert will then be published in HKPost CA Repository.

4.1.2.8 The Registration Bank shall be fully accountable for the safe custody of the Private Key upon receipt of the Bank-Cert.

4.1.3 Publication of Bank-Cert

Under the Ordinance, HKPost's system will publish the Accepted and Issued Bank-Cert in the Repositoryat 0915, 1415 and 1900 HKT as stated in paragraph 2 of Appendix C. Applicants can either verify the information on the certificate by browsing the certificate file or through HKPost CA Repository. Applicants should notify HKPost immediately of any incorrect information of the certificate.

4.2 Bank-Cert (Bank) Certificates

4.2.1 Certificate Application

4.2.1.1 Applicants for Bank-Cert (Bank) under this CPS must complete and submit an application at a designated HKPost premises, or premises of other organisations designated by HKPost, and signs the

application form and accept a Subscriber Agreement for Bank-Cert (Bank).

4.2.1.2 By submitting a Bank-Cert (Bank) application, the Applicant authorises the publication of the Bank-Cert (Bank) to any other person or in the HKPost Repository and Accepts the Bank-Cert (Bank) to be Issued to the Applicant.

4.2.1.3 The documentation required for proving the identity of the Applicant and Authorised Representative(s) and that the Authorised Representative has been duly authorised by the Applicant to submit application for Bank-Cert (Bank) on the terms set out in the Subscriber Agreement and this CPS, and where applicable the Authorised Unit to configure, operate and maintain the Bank-Cert (Bank), in Designated Transactions is stipulated in Section 3.1.3 of this CPS.

4.2.1.4 Multiple Bank-Certs (Bank) may be applied for by the Registration Bank for different scope of Designated Transactions and different validity periods within the range specified in **Appendix E**.

4.2.2 Certificate Issuance

4.2.2.1 Following the identity verification process by HKPost, HKPost will Issue the Applicant with an approval of an application. The Applicant will then generate the Private Key and Public Key in a HSM and a secure environment within the Applicant's premises. The Applicant is responsible for ensuring that the Private Key will not be tampered with.

4.2.2.2 The Applicant will generate the Certificate Signing Request (CSR) containing the Public Key in a Trustworthy System and environment within the Applicant's premises, and transmits the CSR to HKPost in a secure manner.

4.2.2.3 Upon receipt of the CSR, HKPost will verify that the Applicant is in possession of the corresponding Private Key by checking the digital signature on the CSR structure containing the Public Key material. HKPost will not have possession of the Applicants' Private Keys.

4.2.2.4 Upon verifying the Applicant's possession of its Private Key, HKPost will generate the certificate in which the Applicant's Public Key will be included. The Issued Bank-Cert (Bank) will then be transmitted to the Applicant in a secure manner.

4.2.2.5 Acceptance is signified by the Applicant's receipt of the issued Bank-Cert (Bank) and its subsequent use of its key and Bank-Cert (Bank). The Issued and Accepted Bank-Cert (Bank) will then be published in HKPost CA Repository under the Ordinance.

4.2.3 Publication of Bank-Cert

Under the Ordinance, HKPost's system will promptly publish the Accepted and Issued Bank-Cert in the Repository (see Section 2.4). Applicants can either verify the information on the certificate by browsing the certificate file or through HKPost CA Repository. Applicants should notify HKPost immediately of any incorrect information of the certificate.

4.3 Certificate Suspension and Revocation

4.3.1 Circumstances for Suspension and Revocation

4.3.1.1 The compromise of a HKPost Private Key will result in prompt revocation of the certificates issued under that Private Key. Procedures stipulated in the HKPost key compromise plan will be exercised to facilitate rapid revocation of all Subscriber certificates in the event of compromise of the HKPost Private Keys (see Section 4.7.2).

4.3.1.2 Each Subscriber may make a request to revoke the certificate issued in its name at any time by following the revocation procedure set out in this CPS.

4.3.1.3 Each Subscriber of Bank-Cert (Personal)/(Corporate) **MUST immediately** apply to the Registration Bank for the revocation of the certificate in accordance with the revocation procedures in

this CPS **where: the Subscriber's Private Key, or the system of the Registration Bank containing the Private Key corresponding to the Public Key contained in a Bank-Cert has been, or is suspected of having been, compromised or the Authorised User named in the Bank-Cert (Corporate) is no longer acting as such or there is any other event as specified in Section 4.3.1.5 applicable to it or its Bank-Cert (see also Section 2.1.4.2(g)).**

4.3.1.4 The Registration Bank **MUST immediately notify and** apply to HKPost for the revocation of a Bank-Cert **whether issued in its name as Subscriber or via it as a Registration Bank where: a Private Key, or the media containing the Private Key corresponding to the Public Key contained in that Bank-Cert has been, or is suspected of having been, compromised or the Authorised User named in the Bank-Cert (in the case of Bank-Cert (Corporate)) is no longer acting as such or there is any other event as specified in Section 4.3.1.5 applicable to such Bank-Cert, or the Subscriber of such Bank-Cert . It must also immediately notify all Subscribers of Bank-Certs (Personal) and (Corporate) Issued via it as the Registration Bank where the aforesaid notification and application for revocation relates to its own Bank-Cert (Bank). It must notify the relevant Subscriber(s) of the relevant Bank-Cert(s) (Personal) or (Corporate) where the aforesaid notification and application for revocation relates to the Bank-Cert issued to such Subscriber(s). Where the Revocation Notice is issued by HKPost under Section 4.3.1.5, it must make the same notification to the aforesaid Subscribers (depending on in relation to which type of Bank-Cert the revocation relates). It must immediately suspend the use of the Bank-Cert and refrain from allowing the relevant Private Key(s) of the Bank-Cert(s) to be used (whether in the light of the application for revocation made by it under this Section for such Bank-Cert(s) or in the light of the Revocation Notice issued by HKPost under Section 4.3.1.5). All of the aforesaid application and notification shall be done immediately notwithstanding any contrary remark in Appendix E or otherwise.**

4.3.1.5 HKPost will suspend or revoke a Bank-Cert immediately upon the occurrence of any of the events below in relation to such Bank-Cert or there is any suspicion of such occurrence by serving a notice to this effect to the Subscriber via the Registration Bank (in the case of Bank-Cert (Personal) or Bank-Cert (Corporate) or directly to the relevant Registration Bank (in the case of Bank-Cert (Bank) ("Revocation Notice").

a) the application for the Bank-Cert has not been duly authorised by the Subscriber; or that there has been any unauthorised use;
b) the Bank-Cert's Private Key has been compromised;
c) any information in the Bank-Cert is not true or has become untrue or that the certificate is otherwise unreliable;
d) the Bank-Cert was not properly issued in accordance with this CPS;
e) the Subscriber to whom the relevant Bank-Cert was issued had failed to meet any of the obligations set out in this CPS or the Subscriber Agreement;
f) there is any regulation or law applicable to the certificate which requires such suspension or revocation;
g) the subscription fee in relation to the certificate has not been paid;
h) the Subscriber to whom the Bank-Cert (Personal) certificate was issued:

    (i) Is dead or has lost the capacity to enter into contracts;
    (ii) Is or has become an undischarged bankrupt or has entered into a composition or scheme of arrangement or a voluntary arrangement within the meaning of the Bankruptcy Ordinance (Cap. 6) within 5 years preceding the date of revocation; or
    (iii) Has been convicted in Hong Kong or elsewhere of an offence for which it was necessary to find that the person acted fraudulently, corruptly or dishonestly or committed an offence under the Electronic Transactions Ordinance; or
    (iv) an enforcement order has been granted by the court in respect of, any part of the Subscriber's assets within 12 months preceding the date of suspension or revocation and the enforcement order remaining undischarged as at the date of the proposed suspension or revocation

i) the Authorised User identified in a Bank-Cert (Corporate) certificate has ceased to be an Authorised User of the Subscriber organisation;
j) the Subscriber of the Bank-Cert (Corporate) or Bank-Cert (Bank) as the case may be:-

(i) is in liquidation, or a winding up order relating to the Subscriber has been made by any Court of competent jurisdiction;
(ii) 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 years preceding the date of intended revocation;
(iii) a director, officer or employee of the Subscriber has been convicted of an offence for which it was necessary to find that that person had acted fraudulently, corruptly or dishonestly or committed an offence under the Electronic Transactions Ordinance;
(iv) a receiver or administrator has been appointed over or an enforcement order has been granted by the court in respect of, any part of the Subscriber's assets within 12 months preceding the date of suspension or revocation and whose appointment or enforcement order remaining undischarged as at the date of the proposed suspension or revocation; or
(v) the Subscriber's existence can no longer be verified by the Registration Bank based on the KYC procedures (in the case of Bank-Cert (Personal) or (Corporate); or can no longer be verified by HKPost (in the case of Bank-Cert (Bank));

k) the Bank-Cert was issued via a Registration Bank whose Bank-Cert (Bank) is to be revoked or suspended or expired but not renewed under whatever circumstances; OR
l) under Section 4.1.1.3.

4.3.2 Revocation Request Procedure

4.3.2.1 A Subscriber of Bank-Cert (Personal), and the Authorised Representative or Authorised User of a Subscriber of Bank-Cert (Corporate), may submit a revocation request and subsequent final confirmation to the Registration Bank by fax, letter mail, email or in-person, depending upon which of these methods the Registration Bank to be contacted can accept (see **Appendix E**), and the Registration Bank will forward such revocation requests to HKPost. The Subscriber should not submit a request directly to HKPost as it will take time for HKPost to verify its identity and the two working days' performance pledge specified in Section 4.3.3 (a) will not be met.

4.3.2.2 For revocation of Bank-Cert (Bank), the Authorised Representative of a Registration Bank of Bank-Cert (Bank) may submit a certificate revocation request by giving no less than one month's notice and subsequent final confirmation to HKPost by fax, letter mail, email or in-person as specified in Section 1.3.

4.3.2.3 The Registration Bank shall perform identity verification of the Subscriber and in case of Bank-Cert (Corporate), also the identity of the Authorised Representative or Authorised User of the Subscriber, according to the KYC procedures of the Registration Bank, where there is a revocation request from such Subscriber or Authorised Representative or Authorised User, as the case may be. The Authorised Representative or Authorised User shall be deemed to have the authorisation to issue the revocation request on behalf of the Subscriber organisation. The Registration Bank shall perform such function as agent for the Subscriber and also as sub-contractor for the Contractor.

4.3.2.4 Based on the revocation request, HKPost will suspend the validity of the certificate. The certificate will be revoked, upon receipt of the final confirmation of revocation. Such final confirmation of revocation can be an original letter signed by the Subscriber addressed to HKPost (and via the Registration Bank (in the case of Bank-Cert (Personal) or (Corporate)) or a Request for Certificate Revocation Form signed by the Subscriber despatched to HKPost (and via the Registration Bank (in the case of Bank-Cert (Personal) or (Corporate)). If no final confirmation of revocation is received from the Subscriber, the status of such certificate will remain to be shown as suspended and such status will continue to be specified in the Certificate Revocation List (CRL) until the certificate expires. The Request for Certificate Revocation Form can be obtained from the web site at http://www.eCert.gov.hk or from the Registration Bank (see **Appendix E**). HKPost may consider Subscriber's request for resuming the validity of certificates that are suspended. However, resuming the validity of a certificate that is suspended is only at the discretion of HKPost.

4.3.2.5 The information of all Certificates that have been suspended or revoked, including the reason code identifying the reason for the certificate suspension and revocation, will be included in the Certificate Revocation List (see Section 7.2). A certificate that is resumed from a "suspended" status will not be included in the succeeding Certificate Revocation Lists.

4.3.2.6 Where a suspension request or revocation request or final confirmation of revocation from a Subscriber of Bank-Cert (Personal) or (Corporate) has been submitted to the Registration Bank otherwise than pursuant to the circumstances as specified in Section 4.3.1.3, that Registration Bank must, within one working day after the date of receipt or within such other period as specified in the "Remark" column in Appendix E opposite the name of that Registration Bank, notify HKPost of the receipt of the same via channels from time to time prescribed by HKPost to enable HKPost to post the suspension or revocation to the Certificate Revocation List.

4.3.2.7 Requests for revocation and confirmation of revocation can only be received by HKPost within its usual business hours.

The HKPost CA business hours for receiving certificate revocation requests from the Registration Bank via prescribed channels are as follows:

Monday - Friday	09:00 am - 5:00 pm
Saturday	09:00 am - 12:00 noon
Sunday & Public Holiday	No service

In case a tropical cyclone warning signal no. 8 (or above) or a black rainstorm warning signal is hoisted, receipt of revocation requests will be suspended immediately and will recommence at its usual business hours if the signal is lowered at or before 6 am on that day. If the signal is lowered between 6 am and 10 am or at 10 am, receipt of revocation requests will recommence at 2:00 pm for any weekday other than a Saturday, Sunday or public holiday. If the signal is lowered after 10 am, receipt of revocation requests will recommence at usual business hours on the next weekday other than a Sunday or public holiday.

4.3.3 Service Pledge & Certificate Revocation List Update

a) HKPost will exercise reasonable endeavours to ensure that within 2 full working days after actual receipt of a suspension or revocation request from the Registration Bank on behalf of the Subscriber of Bank-Cert (Personal) or (Corporate) or within 2 full working days plus expiry of not less than one month's notice as required under Section 4.3.2.2 after actual receipt of a suspension or revocation request from the Registration Bank (in relation to the Bank-Cert (Bank)), it will post the suspension status on the Certification Revocation List. HKPost will equally exercise reasonable endeavours to ensure that within 2 full working days after (1) actual receipt of a final confirmation of revocation from the Registration Bank on behalf of the Subscriber or (2) where applicable, the Revocation Notice issued by HKPost under Section 4.3.1.5, it will post the revocation status on the Certificate Revocation List. However, a Certificate Revocation List is not immediately published in the directory for access by the public following each certificate suspension or revocation. Only when the next Certificate Revocation List is updated and published will it reflect the suspended or revoked status of the certificate. Certificate Revocation Lists are published daily at 0915, 1415 and 1900 HKT as stated in paragraph 2 of Appendix C and are archived for at least 7 years.

   For the avoidance of doubt, all Saturdays, Sundays, public holidays and for all weekdays on which a tropical cyclone signal no 8 or above and black rainstorm warning signal is hoisted and remaining hoisted for any further duration after 7:00 am on that day, are not full working days for the purpose of this Section 4.3.3(a).

   HKPost will exercise reasonable endeavours to notify relevant Subscribers by email via the Registration Bank (in the case of Bank-Cert (Personal) or (Corporate)), within two working days after completion of the update of the CRL.

b) A Subscriber must not use a certificate registered in its name after the occurrence of any of the

following relevant events:

(i) on becoming aware of any ground upon which HKPost could revoke it under the terms of the CPS (including those specified in Section 4.3.1.5);

(ii) the Subscriber has made a revocation request to HKPost whether via the Registration Bank or otherwise in relation to such certificate; or

(iii) a Revocation Notice has been issued from HKPost under Section 4.3.1.5 in relation to such certificate or in relation to the Bank-Cert (Bank) in the name of its Registration Bank via which its own certificate was also issued; or

(iv) its Registration Bank has issued a revocation application to HKPost under Section 4.3.1.4 in relation to such certificate or in relation to the Registration Bank's Bank-Cert (Bank) and that such application has been notified to the Subscriber.

HKPost shall be under no liability to the Subscriber or Registration Bank via which the Bank-Cert was issued, or Relying Parties in respect of any such transactions if, Subscribers do use the certificate in a transaction any time after any of the relevant events specified in (i) to (iv) above.

c) Further, upon occurrence of any of the relevant events as specified in b)(i) to (iv) above, Subscribers must immediately notify Relying Parties accordingly and that the Relying Parties should not rely upon the certificate in respect of the transaction. HKPost shall be under no liability to the Subscribers, the Registration Bank, and Relying Parties regardless of whether or not the Subscriber has done so.

HKPost shall be under no liability to the Subscriber, Registration Bank, and Relying Parties in respect of the transactions in the period between HKPost's decision to suspend or revoke a certificate (either in response to a request or acting on its own accord or otherwise) and the appearance of the suspension or revocation status on the Certificate Revocation List, and any transactions effected by any suspended or revoked Bank-Cert any time thereafter.

d) The Certificate Revocation List (CRL) and Authority Revocation List ("ARL") of HKPost is updated and published in accordance with the schedule and format specified in **Appendix C**.

4.3.4 Effective time of Suspension and Revocation

Without prejudice to Sections 4.3.3b) to d) above, suspension or revocation suspends or terminates a certificate as at the actual time of the appearance of the suspension or revocation status on the Certificate Revocation List. Regardless, HKPost will not be responsible for any usage of the certificate in breach of Section 4.3.3b) or other applicable provision notwithstanding the aforementioned effective time or any time thereafter. Relying Parties are reminded to check both the Repository and the Certificate Revocation List before relying on a Designated Transaction effected through the use of a Bank-Cert. However, where the Registration Bank has duly performed its duty as specified in Section 3.2.3, it should not be possible for a Bank-Cert to be used in an unauthorised manner after its revocation or suspension or expiry status has been posted and published on the Repository and/or Certificate Revocation List (where applicable).

4.4 Computer Security Audit Procedures

4.4.1 Types of Events Recorded

Significant security events in the HKPost CA system are manually or automatically recorded to protected audit trail files. These events include, but are not limited to, the following examples:

- Suspicious network activity
- Repeated failed access attempts
- Events related to equipment and software installation, modification, and configuration of the CA operation
- Privileged accesses to all CA components
- Regular certificate management operations including: -

- Certificate revocation and suspension requests
- Actual issuance, suspension and revocation of certificates
- Certificate renewals
- Updates to repositories
- CRL generation and posting
- CA Key rollover
- Backups
- Emergency key recoveries

4.4.2 Frequency of Processing Log
Audit logs are processed and reviewed on a daily basis to provide audit trails of actions, transactions and processes of the HKPost CA.

4.4.3 Retention Period for Audit Logs
Archived audit log files are retained for 7 years.

4.4.4 Protection of Audit Logs
HKPost implements multi-person control on processing audit logs which are afforded adequate protection against accidental damage or deliberate modifications.

4.4.5 Audit Log Backup Procedures
Adequate backup of audit logs is performed on a daily basis under pre-defined procedures including multi-person control. The backups will be stored off-line and are afforded adequate protection against theft, destruction and media degradation. The backups will be retained for not less than one week before they are archived.

4.4.6 Audit information Collection System
HKPost CA audit records and files are under the control of an automated audit collection system that cannot be modified by any application, program, or other system function. Any modification to the audit collection system is itself an auditable event.

4.4.7 Notification of Event-Causing Subject to HKPost
HKPost has an automated process in place to report critical audited events to the appropriate person or system.

4.4.8 Vulnerability Assessments
Vulnerability assessments are conducted as part of HKPost's CA security procedures.

4.5 Records Archival

4.5.1 Types of Records Archived
HKPost shall ensure that archived Records are detailed enough to establish the validity of a certificate and the proper operation of it in the past. The following data are archived by (or on behalf of) HKPost:

- System equipment configuration files;
- Results of assessments and/or review for accreditation of the equipment (if conducted);
- Certification Practice Statement and its modifications or updates;
- Contractual agreements to which HKPost is bound;
- All certificates and CRLs as issued or published;
- Periodic event logs; and
- Other data necessary for verifying archive contents.

4.5.2 Archive Retention Period
Key and certificate information is securely maintained for at least 7 years. Audit trail files are maintained in the CA systems as deemed appropriate by HKPost.

4.5.3 Archive Protection
Archived media maintained by HKPost is protected from unauthorised access by various physical and

cryptographic means. Protective measures are used to protect the archiving media from environmental threats such as temperature, humidity and magnetism.

4.5.4 Archive Backup Procedures
Backup copies of the archives will be created and maintained when necessary.

4.5.5 Timestamping
Archived information is marked with the date at which the archive item was created. HKPost utilizes controls to prevent the unauthorised manipulation of the system clocks.

4.6 Key Changeover

The lifespan of the HKPost CA and signing root key and certificates created by HKPost (See **Appendix F**) for the purpose of certifying certificates issued under this CPS is no more than 25 years starting from the creation of the HKPost's CA root certificate as specified in **Appendix F**. HKPost CA keys and certificates will be renewed at least 3 months before their certificates expire. Upon renewal of a root key, the associated root certificate will be published in HKPost web site http://www.eCert.gov.hk for public access. The original root keys will be kept for a minimum period as specified in Section 4.5.2 for verification of any signatures generated by the original root keys.

4.7 Disaster Recovery and Key Compromise Plans

4.7.1 Disaster Recovery Plan
A managed process, including daily backup of essential business information and CA system data and proper backup of CA system software, is in place for maintaining business continuity plans to protect critical business processes from the effect of major failures or disasters. Business continuity plans exist to enable the complete recovery of all HKPost CA services. This incorporates a tested independent disaster recovery site which is currently located at least 10km from the primary CA operational site within the territory of Hong Kong Special Administrative Region. The business continuity plans are reviewed and exercised annually.

HKPost will promptly notify the Government Chief Information Officer and make public announcement of the switchover of operation from the production site to the disaster recovery site as a result of major failures or disasters.

During the period of time following a disaster and before a secure environment is re-established:-

a) Sensitive material or equipment will be locked up safely in the facility;
b) Sensitive material or equipment will be removed from the facility if it is not possible to lock them up safely in the facility or if there is a risk of damage to the material or equipment, and such material or equipment will be locked up in other temporary facilities; and
c) Access control will be enforced at all entrances and exits of the facility to protect the facility from theft and unauthorised access.

During the period of time following a disaster and before a secure environment is re-established, HKPost will not able to update the CRL. Subscriber may still continue to use Bank-Cert but at their risks. HKPost will also not be able to issue certificate, to revoke certificate, or to make available the public repository to enable download of public keys and certificates.

4.7.2 Key Compromise Plan
Formal procedures of handling key compromise are included in the business continuity plans and are reviewed and exercised annually.

HKPost will promptly notify the Government Chief Information Officerand make public announcement if a HKPost Private Key for the issuance of Bank-Cert certificates under this CPS has been compromised. The compromise of a HKPost Private Key will result in prompt revocation of the certificates issued under that Private Key and the issuance of new and replacement certificates.

4.7.3 Key Replacement

In the event of key compromise or disaster where a HKPost Private Key for the issuance of Bank-Cert certificates under this CPS has been compromised or corrupted and cannot be recovered, HKPost will promptly notify the Government Chief Information Officer and make a public announcement as to which certificates have been revoked, and how the new HKPost Public Key is provided to Subscribers, and how Subscribers are re-issued with new certificates.

4.8 CA Termination

In the event that HKPost ceases to operate as a CA, notification to the Government Chief Information Officerand public announcement will be made in accordance with the procedures set out in the HKPost termination plan.Upon termination of service, HKPost will properly archive the CA Records including certificates issued, root certificates, Certification Practice Statements and Certificate Revocation Lists for at least 7 years after the date of service termination.

According to the HKPost termination plan, HKPCA will inform the GCIO its intention to terminate its services in relation to Bank-Certs at least 90 days before the termination takes effect. HKPCA will inform, by e-mail or letter mail, all its subscribers HKPCA's intention to terminate its service as a recognized CA at least 60 days before the termination takes effect. HKPCA will advertise its intention to terminate its service as a recognized CA in one English language daily newspaper (if available) and one Chinese language newspaper in circulation in HKSAR for at least three consecutive days at least 60 days before the termination takes effect.

4.9 Registration Bank Termination

In the event that the Bank-Cert (Bank) held by a Registration Bank for conducting Designated Transaction which is creation of Digital Signature on e-cheque as the drawee bank is suspended or revoked by HKPost, the Bank-Cert (Personal) and Bank-Cert (Corporate) Issued through the Registration Bank will also be suspended or revoked at the same time. HKPost shall not be responsible for any claim, legal proceeding, liability, loss (including any direct or indirect loss, any loss of revenue, profit, business, contract or anticipated saving), damage (including any direct, special, indirect or consequential damage of whatsoever nature) or any cost or expense, suffered or incurred by any person whomsoever due to the suspension or revocation. To avoid business disruption, the Registration Bank should apply for separate Bank-Certs (Bank) to cover different types of Designated Transactions. The Bank-Cert (Bank) to be used for creation of Digital Signature on e-cheque as the drawee bank should be used solely for such purpose.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 Physical Security

5.1.1 Site Location and Construction
The HKPost CA operation is located in a site that affords commercially reasonably practical physical security.

5.1.2 Access Controls
HKPost has implemented commercially reasonably practical physical security controls that limit access to the hardware and software (including the CA server, workstations, and any external cryptographic hardware modules under HKPost's control) used in connection with providing the HKPost CA services. Access to such hardware and software is limited to those personnel performing in a trusted role as described in Section 5.2.1 of this CPS. Access is controlled and manually or electronically monitored for unauthorised intrusion at all times.

5.1.3 Power and Air Conditioning
Power and air conditioning resources available to the CA facility include dedicated air-conditioning system, uninterruptible power supply (UPS) system and a back-up independent power generator to provide power in the event of the failure of the city power system.

5.1.4 Natural Disasters
The CA facility is protected to the extent reasonably possible from natural disasters.

5.1.5 Fire Prevention and Protection
The CA facility has a fire prevention plan and suppression system in place.

5.1.6 Media Storage
Media storage and disposition processes have been developed and are in place.

5.1.7 Off-site Backup
Adequate backups of the HKPost CA system data will be stored off-site and are afforded adequate protection against theft, destruction and media degradation (See also Section 4.7.1)

5.1.8 Protection of Paper Documents
Paper documents including photocopies of identity confirmation documents are maintained by the Registration Bank in a secure fashion. Only authorised personnel are permitted access to the paper records.

5.2 Procedural Controls

5.2.1 Trusted Role
Employees, contractors, and consultants of HKPost, of the Contractor and of RBs (collectively "Personnel") that have access to or control of cryptographic or other operations that may materially affect the issuance, use, or revocation of certificates, including access to restricted operations of HKPost's CA database, are considered to be serving in a trusted role. Such Personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are assigned to oversee HKPost's CA operation.

Procedures are established, documented and implemented for all trusted roles in relation to HKPost Bank-Cert services. The procedural integrity is maintained by enforcing:
- different levels of physical and systems access control based on role and responsibility, and
- segregation of duties.

5.2.2 Transfer of Document and Data between HKPost, Contractors and Registration Banks
All documents and data transmitted between HKPost, Contractors and Registration Banks are delivered in a control and secure manner using a protocol prescribed by HKPost from time to time.

5.2.3 Annual Assessment
An annual assessment is undertaken to confirm compliance with policy and procedural controls (see Section 2.5).

5.3 Personnel Controls

5.3.1 Background and Qualifications
HKPost and the Contractor follow personnel and management policies that provide reasonable assurance of the trustworthiness and competence of such personnel and that of Registration Banks acting on behalf of HKPost, including employees, contractors and consultants and of the satisfactory performance of their duties in a manner consistent with this CPS.

5.3.2 Background Investigation
HKPost conducts and/or requires the Contractor and Registration Banks to conduct investigations of personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary) to verify such employees' trustworthiness and competence in accordance with the requirements of this CPS. Personnel who fail an initial or periodic investigation are not permitted to serve or to continue to serve in a trusted role.

5.3.3 Training Requirements
HKPost personnel and those of the Contractor's and of Registration Bank's have received the initial training needed to perform their duties. HKPost, the Contractor and Registration Banks also provide ongoing training as necessary to enable their respective personnel to remain current in required skills.

5.3.4 Documentation Supplied To Personnel
HKPost personnel and those of the Contractor's and of Registration Bank's receive comprehensive user manuals detailing the procedures for certificate creation, issuance, updating, renewal, and revocation, and other software functionality relative to their role.

6. TECHNICAL SECURITY CONTROLS

This Section is to describe the technical measures established by HKPost to specifically protect its cryptographic keys and associated data. Control of HKPost CA keys is implemented through physical security and secure key storage. The HKPost CA keys are generated, stored, used and destructed only within a tamper-proof hardware device, which is under multi-person access control.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation
Key pairs for HKPost are generated through a procedure such that the Private Key cannot be accessed by anyone other than the authorised user of the Private Key unless there is some compromise of the procedure by the authorised user. HKPost generates the root key pairs for issuing certificates that conform to this CPS. Applicants' key pairs for Bank-Certs may be generated under the central key generation by the Registration Bank, on behalf of the Applicants, in a HSM and an environment within the Registration Bank's premises.

6.1.2 Subscriber Public Key Delivery
In case of central key generation by the Registration Bank on behalf of the Applicant/Subscriber, the Registration Bank will generate the Certificate Signing Request (CSR) containing the Public Key and transmits the CSR to HKPost through a system interface.

6.1.3 Public Key Delivery to Subscriber
The Public Key of each HKPost key pair used for the CA's Digital Signatures is available on-line at http://www.eCert.gov.hk. HKPost utilizes protection to prevent alteration of those keys.

6.1.4 Key Sizes
The HKPost signing key pair is 2048-bit RSA. Subscriber key pairs for Bank-Cert certificates are 2048-bit RSA.

6.1.5 Standards for Cryptographic Module
Signing key generation, storage, and signing operations performed by HKPost are conducted within a hardware cryptographic module.

6.1.6 Key Usage Purposes
Keys used in Bank-Cert certificates are only used for Digital Signatures in the Designated Transactions for the corresponding Bank-Cert as specified in **Appendix E**. HKPost Root Key (the key used to create or issue certificates that conform to this CPS) is used only for signing (a) certificates and (b) Certificate Revocation Lists.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module
HKPost Private Keys are created in a crypto module validated to at least FIPS 140-1 Level 3.

6.2.2 Private Key Multi-Person Control
HKPost Private Keys are stored in tamper-proof hardware cryptographic devices. HKPost implements multi-person control over the activation, usage, deactivation of HKPost Private Keys.

6.2.3 Private Key Escrow
No private key escrow process is planned for HKPost Private Keys in the Bank-Cert system used by HKPost. For backup of HKPost Private Keys, see Section 6.2.4 below.

6.2.4 Backup of HKPost Private Keys
Each HKPost Private Key is backed up by encrypting and storing it in devices which conform to FIPS 140-1 Level 2 security standard. Backup of the HKPost Private Key is performed in a manner that

requires more than one person to complete. The backup Private Keys must be activated by more than one person. No other Private Keys are backed-up. All Private Keys will not be archived.

6.3 Other Aspects of Key Pair Management

HKPost CA root keys will be used for no more than 25years (see also Section 4.6). All HKPost key generation, key destruction, key storage, and certificate revocation list signing operations are performed in a hardware cryptographic module. Archival of HKPost Public Keys is performed as specified in Section 4.5.

6.4 Computer Security Controls

HKPost implements multi-person control over the life cycle of activation data such as PINs and passwords for accessing the CA systems. Security procedures are in place to prevent and detect unauthorised access, modification, or compromise of the CA systems. Such security controls are subject to compliance assessment as specified in Section 2.5.

6.5 Life Cycle Technical Security Controls

HKPost implements controls over the procedures for the procurement and development of software and hardware for HKPost CA systems. Change control procedures are in place to control and monitor all revisions and enhancements to be made to the components of such systems.

6.6 Network Security Controls

The HKPost CA systems are protected by firewalls and other access control mechanisms configured to allow only authorised access required for the CA services set forth in this CPS.

6.7 Cryptographic Module Engineering Controls

The cryptographic devices used by HKPost are rated to at least FIPS 140-1 Level 2.

7. CERTIFICATE AND CERTIFICATE REVOCATION LIST PROFILES

7.1 Certificate Profile

Certificates referred to in this CPS contain the Public Key used for confirming the identity of the sender of an electronic message and verifying the integrity of such messages, i.e., the Public Key used to verify a Digital Signature. All certificates referred to in this CPS are issued in the X.509 version 3 format (See **Appendix B**). A summary of the features of the Bank-Cert certificates is in **Appendix D**.

7.2 Certificate Revocation List Profile

The HKPost Certificate Revocation List is in the X.509 version 2 format (see **Appendix C**).

8. CPS ADMINISTRATION

All changes to this CPS must be approved and published by HKPost. The CPS changes will be effective upon publication by HKPost in the HKPost CA web site at http://www.eCert.gov.hk or in the HKPost Repository and are binding on all Applicants and Subscribers to whom certificates are issued. HKPost will notify the Government Chief Information Officer any subsequent changes to this CPS as soon as practicable. A copy of this CPS and its predecessors are available for viewing by Applicants, Subscribers and Relying Parties on the HKPost CA web site at http://www.eCert.gov.hk.

9. OTHER BUSINESS AND LEGAL MATTERS

This part describes the legal representations, warranties and limitations associated with Bank-Certs.

9.1 Fees

9.1.1 Certificate issuance or renewal fees
Subscriber fees for certificate issuance and renewal are chargeable. Such fees are detailed on its website (http://www.eCert.gov.hk). The charging rates of these fees are subject to change; and announced on the same web site. HKPost as the certification authority reserves the right to review the fees (for application and renewal) from time to time and at any time. These fees chargeable are not necessarily aligned with other certificates issued by the HKPost under separate CPS. HKPost may from time to time introduce new types of fees chargeable whether one-time or recurrent, including on a per Designated Transaction basis with reference to the value of the Designated Transaction or any other basis.

9.1.2 Certificate access fees
HKPost reserves the right to establish and charge a reasonable fee for access to its database of certificates.

9.1.3 Revocation or status information access fees
HKPost does not charge fees for the revocation of a certificate or for a Relying Party to check the validity status of a HKPost issued certificate through the use of Certificate Revocation Lists.

9.1.4 HKPost's Liability for Received but Defective Certificates
Notwithstanding the limitation of HKPost's liability set out further below, if, after it or a Registration Bank on its behalf has received a certificate, a Subscriber or Registration Bank finds that, in respect of Bank-Cert (Personal), Bank-Cert (Corporate) or Bank-Cert (Bank), because of any error in the Private Key or Public Key of the certificate generated by HKPost on behalf of the Subscriber, no transactions contemplated by the PKI can be completed properly or at all, and that Subscriber notifies the REGISTRATION BANK of this immediately or HKPost of this immediately to permit the certificate to be revoked and (if desired) re-issued, then, if such notification has occurred within 3 months after receiving the certificate and the Subscriber no longer wants a certificate, HKPost on being satisfied of the existence of any such error will refund the fee paid. If the Subscriber waits longer than 3 months after receiving the certificate before notifying HKPost of any such error, the fee paid will not be refunded as of right, but only at the discretion of HKPost. In case that Subscriber's key pair is generated under the central key generation by the Registration Bank on behalf of the Subscriber, no refund will be payable to the Subscriber.

9.2 Financial responsibility

9.2.1 Insurance coverage
An insurance policy is in place to cover the potential or actual liabilities and claims against Reliance Limit on the certificates.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information
Without any intention to detract from its obligations under Section 46 of the Ordinance, specifically, HKPost keeps the following types of information confidential (collectively, confidential information") and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- All private keys of root-CA/sub-CA certificates owned and kept by HKPost for signing and issuance of entity certificates to Subscribers;
- Any business continuity, incident response, contingency, and disaster recovery plans
- Any other security practices, measures, mechanisms, plans, or procedures used to protect the confidentiality, integrity or availability of information

- Any information held by HKPost as private information in accordance with Section 9.4
- Any transactional, audit log and archive record identified in Section 4.5.1, including certificate
- application records and documentation submitted in support of certificate applications whether successful or rejected.
- Transaction records, financial audit records and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CPS)

9.3.2 Information not within the scope of confidential information

9.3.2.1 Subscriber application data which is published in a Bank-Cert is considered public and not within the scope of confidential information. Subscribers acknowledge that suspension or revocation data of all certificates issued by the HKPost CA is public information and is periodically published every 24 hours at the Repository.

9.3.2.2 HKPost does not possess the Private Keys of any of the Bank-Certs (regardless of the types) as they are retained by the Registration Banks. Applicants and Subscribers are reminded that they should satisfy themselves concerning the security measures put in place by the Registration Bank for ensuring the confidentiality and security of the Private Keys before applying or renewing or accepting or using the Bank-Certs.

9.4 Privacy of personal information

9.4.1 Privacy plan
HKPost has implemented a privacy policy, which is in compliance with this CPS. The HKPost privacy policy is published at https://www.hongkongpost.hk/en/privacy/index.html.

9.4.2 Information treated as private
Personal information about an individual that is not publicly available in the contents of a certificate or CRL is considered private (collectively "private information").

9.4.3 Information not deemed private
Certificates, CRLs, and personal or corporate information appearing in them are not considered private.

9.4.4 Notice and consent to use private information
HKPost may use private information with the subject's express written consent or as required by applicable law or court order or under other circumstances as set out in Section 46(2) of the Ordinance.

9.4.5 Disclosure pursuant to judicial or administrative process

HKPost shall not release any confidential information, unless as otherwise required under the circumstances specified in Sections 46(2)(a) to (d) of the Ordinance. Without intending to depart from the scope of the exceptions specified in Section 46(2) of the Ordinance, specifically, HKPost may disclose confidential information to its Contractor or other contractor or consultant or advisor from time to time with a need to know in order to perform a function under or for the purpose of the Ordinance, confidential information in relation to a Subscriber to the Registration Bank as specified in the certificate issued to that Subscriber, or confidential information in relation to an Application to the Registration Bank via which an application for a certificate is made on behalf of that Applicant.

9.5 Intellectual property rights
HKPost, and its Contractor own all their respective intellectual property rights associated with their databases, web sites and any other publication originating from HKPost including this CPS.

The trademarks "HKPost" and "Hongkong Post e-Cert" are registered trademarks of HKPost. HKPost may have other trade and service marks that have not been registered, but that nonetheless are and shall remain the property of HKPost.

Certificates are the exclusive property of HKPost. HKPost gives permission to reproduce and distribute certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full. HKPost reserves the right to revoke the certificate at any time and at its sole discretion.

Private and public keys are the property of the Subscribers who rightfully issue and hold them.

9.6 Representations and Warranties

9.6.1 HKPost Representations and Warranties

9.6.1.1 HKPost makes the following warranties and representations solely to Subscribers, and all Relying Parties that actually rely on such Certificate during the period when it is valid, that it followed the requirements of this CPS in issuing the Certificate ("Certificate Warranties").

9.6.1.2 Subject to the limitations below, the Certificate Warranties specifically include, but are not limited to, warranties that:

By issuing a certificate that refers to this CPS, HKPost represents to any person who reasonably relies on the information contained in the Bank-Cert certificate or a digital signature verifiable by the public key listed in the Bank-Cert certificate, that HKPost has issued the certificate in accordance with this CPS. By publishing a Bank-Cert certificate, HKPost represents to any person who reasonably relies on the information contained in the Bank-Cert certificate, that HKPost has issued the certificate to the Subscriber identified in it.

9.6.1.3 HKPost does not warrant the accuracy, authenticity, completeness or fitness of any other information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of HKPost.

9.6.1.4 HKPost does not warrant the quality, functions or performance of any software or hardware device.

9.6.1.5 HKPost shall have no liability if it cannot execute the revocation of a certificate for reasons outside its own control.

9.6.2 Registration Bank representations and warranties

Each Registration Bank makes the following warranties and representations to each of HKPost, Subscribers whose Certificates are issued via such Registration Bank, and all Relying Parties that actually rely on such Certificate during the period when it is valid and not suspended or terminated or expired, that it followed the requirements of this CPS in applying for the Certificate on behalf of the Applicant and in verifying the accuracy of the information contained in the Certificate and in keeping, hosting and operating the Private Key of the Certificate ("Certificate Warranties"). The Certificate Warranties specifically include, but are not limited to, all of the following warranties that:

(A) Legal Existence: It has confirmed in accordance with the CPS and its KYC that, as at the date the Certificate was issued and thereafter whilst the Certificate continues to be valid and not expired or revoked or suspended ("validity of the Certificate"), the Subscriber named in the Certificate legally exists and in the case of the Subscriber being an organisation, it is a valid organisation in the jurisdiction of incorporation or registration;

(B) Identity: The Registration Bank has confirmed that, as at the date the Certificate was issued and thereafter throughout the validity of the Certificate, the legal name of the Subscriber named in the Certificate matches the name on the official government records of the government agency in the Subscriber's domicile (in the case of an individual) or in the Subscriber's jurisdiction of incorporation or registration(in the case of an organisation), and if an assumed name is also included, that the assumed name is properly registered by the Subscriber in the aforesaid place;

(C) Holder of bank account: The Registration Bank has confirmed that, as of the date the Certificate was issued and throughout the validity of the Certificate, the Subscriber named in the Certificate has a bank account with the Registration Bank;

(D) Authorisation for Certificate: The Registration Bank has taken all steps reasonably necessary to verify that the Subscriber named in the Certificate has authorised the application and issuance of the Certificate and that such application has not been withdrawn or revoked throughout the validity of the Certificate;

(E) Accuracy of information: The Registration Bank has taken all steps reasonably necessary to verify that all of the other information in the Certificate is accurate, as at the date the Certificate was issued and thereafter throughout the validity of the Certificate;

(F) Subscriber Agreement: The Registration Bank has taken all steps reasonably necessary to ensure that the Subscriber named in the Certificate has entered into a legally valid and enforceable Subscriber Agreement with HKPost throughout the validity of the Certificate;

(G) Protection of Private Key**:** The Registration Bank has taken all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the Certificate issued via the Registration Bank. The Registration Bank retains control of the Subscriber's private key, uses a trustworthy system (as defined in the Ordinance), and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorised use and that no unauthorised person has ever had access to the Subscriber's private key.

(H) Reporting and Revocation Upon Compromise: The Registration Bank shall promptly cease using a Bank-Cert and its associated Private Key, and promptly request that HKPost revoke the Certificate, in the event that: (a) any information in the Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key; and

(I) Revocation: The Registration Bank will inform HKPost as soon as possible in relation to any occurrence of any event specified in Section 4.3.1.5 in accordance with Section 4.3.1.4 and other applicable provision or within the applicable time limit when the Subscriber has notified the Registration Bank via prescribed channel that it wishes to revoke the Certificate in accordance with Section 4.3.2 and other applicable provision;

(J) Termination of bank account: The Registration Bank will notify the HKPost as soon as the Subscriber no longer owes a bank account with the Registration Bank;

(K) The Registration Bank makes all necessary efforts to independently confirm the information provided by the Applicant fora Bank-Cert;

(L) Checking of Information in Designated Transaction: Each Time a Bank-Cert(Personal) or (Corporate) issued via it is used in a Designated Transaction, verifying the identity of the Subscriber and where applicable the Authorised User; ensuring the name of the drawer of the e-cheque matches the name of the Subscriber as stated in that Bank-Cert; and in the case of Bank-Cert (Corporate) ensuring the name of the Authorised User as stated in the e-cheque matches the name of the Authorised User as stated in the Bank-Cert; and ensuring that the Bank-Cert has not expired or revoked or suspended based on the information as published in the latest Repository and the CRL. Where such Bank-Cert is expired or revoked or suspended, ensuring that the Designated Transaction will not be processed or completed using such Bank-Cert.

9.6.3 Subscriber representations and warranties

9.6.3.1 The Subscriber Agreement is confirmed acceptance by the Authorised Representative of the Subscriber on behalf of the Subscriber (in the case of Bank-Cert (Corporate) or Bank-Cert (Bank) or the Subscriber personally (in the case of Bank-Cert (Personal). In the case of Bank-Cert (Corporate) or (Bank). The Applicant/Subscriber organisation confirms that the Authorised Representative has authority to represent and bind Applicant/Subscriber organisation in its certificate procurement process with respect to signing Subscriber Agreements on behalf of Applicant/Subscriber organisation, and

binding Applicant/Subscriber organisation to all such Subscriber Agreements and related documents. The Applicant/Subscriber organisation confirms that the Authorised User as stated in the Bank-Cert (Corporate) has the authority to use the Bank-Cert for and on behalf of the Applicant/Subscriber organisation. As part of the standard Subscriber Agreement agreed to by a Subscriber, all of the following commitments and warranties are made and are deemed to have been made by that Subscriber for the express benefit of HKPost the Registration Bank and all Relying Parties and are to be ensured to be true complete and accurate by that Subscriber throughout the period of application, issuance and validity of the Certificate issued in its name:

(A) Accuracy of information: An obligation and warranty to provide accurate and complete information and other representations at all times to HKPost and the Registration Bank both in the application for a Bank-Cert and as otherwise from time to time requested by HKPost (whether directly or via the Registration Bank) including without limitation those information and representations required in connection with the Issuance and Acceptance of the Certificate(s) to be supplied by HKPost;

(B) Acceptance of Certificate: An obligation and warranty that it will not use the Certificate until it has reviewed and verified the accuracy of the data in the Certificate;

(C) Protection of Private Key: In the case of Bank-Cert (Bank), an obligation and warranty by the Registration Bank to take all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the Certificate;

(D) Use of Certificate: An obligation and warranty to use the Certificate solely incompliance with all applicable laws, solely for authorised company business (in the case of Bank-Cert (Corporate) or (Bank)), and solely in accordance with the Subscriber Agreement;

(E) Reporting and Revocation Upon Compromise: An obligation and warranty to request that HKPost revoke the Certificate (whether via the Registration Bank or directly) upon occurrence of any of the events specified in Section 4.3.1.5.; and

(F) Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Certificate and its Private Key in accordance with Section 4.3.3(b).

9.6.3.2 Without limiting other Subscriber obligations stated in this CPS, Subscribers are solely liable for any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein.

9.6.3.3 Upon Accepting a certificate the Subscriber (regardless of the type of Bank-Cert) represents, warrants and covenants to HKPost, the Registration Bank (in the case the Subscriber is the Subscriber of Bank-Cert (Personal) or Bank-Cert (Corporate)) and to Relying Parties that at the time of Acceptance and throughout the validity of the Certificate all of the following:

(A) Transactions effectuated using the private key corresponding to the public key included in the certificate are the acts of the Subscriber and that the certificate has been accepted and is properly operational at that time throughout the validity of the certificate.

(B) All representations made by the Subscriber to the Registration Bank or HKPost (whether directly or via the Registration Bank) are true, accurate and complete.

(C) All information contained in the certificate are true, accurate and complete.

(D) The certificate is used exclusively for authorised and legal purposes, consistent with this CPS, and that the Subscriber will use the certificate in Designated Transactions specified opposite the name of the Registration Bank in Appendix E for the Bank-Cert type to which the certificate belongs. In the case of Bank-Cert (Bank) issued in the name of a Registration Bank, it is only to be used by the Registration Bank for Designated Transactions specified opposite its name in Appendix E for such type to which the certificate belongs.

(E) The Subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of HKPost.

(F) The Subscriber (being an organisation or bank) abides by the laws applicable in the place of its incorporation or registration and the place of its business including those related to intellectual property protection, fair trade practices and computer fraud and abuse. The Subscriber (being an individual) abide by the laws applicable to his country or territory.

(G) The Subscriber (in the case of Bank-Cert (Personal) or (Corporate)) has authorised the Registration Bank to access the Subscriber's Private Key of the Certificate whenever the Subscriber makes a digitally signature in a Designated Transaction specified opposite the name of that Registration Bank in Appendix E for such Certificate.

(H) The Subscriber has prior to the use of Subscriber's Private Key of the Certificate submitted to a strong authentication procedure stipulated by the Registration Bank for verifying his identity (in the case of holder of Bank-Cert (Personal)) or for verifying the identity of its Authorised User (in the case of holder of Bank-Cert (Corporate)).

(I) Each Digital Signature generated using the Subscriber's Private Key, which corresponds to the Public Key contained in the Subscriber's Bank-Cert, is the Digital Signature of the Subscriber.

(J) The Certificate will be used exclusively for authorised and legal purposes consistent with this CPS; and

(K) All information supplied does not infringe or violate in any way the trademarks, service marks, trade name, company name, or any other intellectual property rights of any third party upon Issuance, Acceptance, throughout the validity of the Certificate.

9.6.4 Relying party representations and warranties

A Relying Party accepts that in order to reasonably rely on a Bank-Cert, the Relying Party must perform all of the following:

(A) Make reasonable efforts to acquire sufficient knowledge on using digital certificates and PKI.

(B) Study the limitations to the usage of digital certificates and be aware through this CPS of the limitations of liability of HKPost for reliance on a HKPost-issued certificate.

(C) Verify that the drawer of the e-cheque (i.e., the person who makes a payment by the e-cheque) indeed has a valid and unexpired Bank-Cert by searching the Repository using the name of that person (in the case of individual), or using the name of the Authorised User as shown on the e-cheque (in the case of organisation). An expired Bank-Cert will be shown as such in the Repository. Refrain from relying in a Bank-Cert which is expired.

(D) Verify the validity of the above-mentioned Bank-Cert by referring to the CRL. A certificate which is suspended or revoked will have the corresponding status being be shown as such in CRL. Refrain from relying on a Bank-Cert which is suspended or revoked.

(E) Take any other reasonable steps to minimize the risk of relying on a digital signature created by an invalid, suspended, revoked, expired or rejected Bank-Cert or a Bank-Cert which has been used in an unauthorised manner; and finally,

(F) Rely on a Bank-Cert, only as may be reasonable under the circumstances given:

(a) any legal requirements for the identification of a party, the protection of the confidentiality or privacy of information, or the legal enforceability of the transaction in accordance with any laws that may apply;

(b) all facts listed in the Certificate, or of which the Relying Party has or should have notice, including this CPS;

(c) the economic value of the transaction;

(d) the potential losses or damage which might be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction or communication;

(e) the applicability of the laws of a particular jurisdiction, including the jurisdiction specified in an agreement with the Subscriber or in this CPS;

(f) the Relying Party's previous course of dealing with the Subscriber, if any;

(g) usage of trade, including experience with computer-based methods of trade; and

(h) any other indicia of reliability or unreliability, or other facts of which the Relying Party knows or has notice, pertaining to the Subscriber and/or the application, communication or transaction.

9.7 Limitations of liability

9.7.1. It is the discretion of the Subscriber to determine within the mechanism provided by Registration Bank (if any) the maximum value of the Designated Transaction which can be effected through the use of the Bank-Cert. The Bank-Cert itself poses no limit on the value of the Designated Transaction.

9.7.2 General Disclaimer: To the maximum extent permissible by law, HKPost shall not be responsible for any claim, legal proceeding, liability, loss (including any direct or indirect loss, any loss of revenue, profit, business, contract or anticipated saving), damage (including any direct, special, indirect or consequential damage of whatsoever nature) or any cost or expense, suffered or incurred by any person whomsoever arising from or due to or in connection with or in relation to (a) the exercise of any function or power by the HKPost as stated in this CPS; and (b) the use or reliance on any Bank Certificate and (c) reliance or use of a false or forged Bank-Cert or where the HKPost has complied with the requirements of this Ordinance and the code of practice with respect to that certificate; and (d) unauthorised or dishonest or fraudulent use of a Bank-Cert; (e) any information in the Certificate or in the Repository (other than the information required to be represented in Section 40 of the Ordinance) is untrue, inaccurate or incomplete.

9.7.3 Other than the representations specified in Sections 39 and 40 of the Ordinance, notwithstanding anything herein to the contrary, the HKPost makes no other representation or warranty to any person (including any Subscriber, any Registration Bank, any Relying Parties, and any Contractor) including (a) any confirmation that any information on the Certificate or in the Repository (other than the information required to be confirmed in Section40 of the Ordinance) is accurate, correct or complete; and (b) the validity or legality of any Designated Transaction transacted through the use of a Digital Signature through a Bank-Cert (of whatever type).

9.7.4 Other than the representations specified in Sections 39 and 40 of the Ordinance, to the maximum extent permissible by law, HKPost disclaims any duty of care owed to any person (including any Subscriber, any Registration Bank, any Relying Party and any Contractor) whether under this CPS, under the Ordinance, or the Code of Practice or any Subscriber Agreement or otherwise at law. No action or omission of the HKPost or its officers acting in the course of employment shall be considered as negligence or willful default actionable at the suit of any of them provided that there is no breach of the representations specified in Sections 39 and 40 of the Ordinance.

9.7.5 Apart from the representations set out in Sections 38 and 40 of the Ordinance and any other representation or warranty which cannot be excluded by law, HKPost disclaims all representations, warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided.

9.7.6 In case of any non-compliance with or breach of the CPS or the Subscriber Agreement or Section 39 or 40 of the Ordinance, HKPost's liability to the Subscriber for legally recognized and provable claims for losses or damage suffered by the Subscriber as a result of any of the above-mentioned non-compliance or breach shall not exceed HK$200,000 per non-compliance or breach or non-compliances or breaches arising from one event.

9.7.7 In case of any non-compliance with or breach of the CPS or any representation specified in

Section 39 or 40 of the Ordinance, HKPost's liability to a Relying Party for legally recognized and provable claims for losses or damage suffered by the Relying Party as a result of any of the above-mentioned non-compliance or breach shall not exceed HK$200,000 per non-compliance or breach or non-compliances or breaches arising from one event.

9.7.8 In case of any non-compliance with or breach of the CPS or any representation specified in Section 39 of the Ordinance, HKPost's liability to a Registration Bank for legally recognized and provable claims for losses or damage suffered by the Registration Bank as a result of any of the above-mentioned non-compliance or breach shall not exceed HK$200,000 per non-compliance or breach or non-compliances or breaches arising from one event. HKPost will have no liability to any Registration for breach of Section 40 of the Ordinance for it is HKPost which relies on the representation from the Registration Bank that a Bank-Cert is issued to the person named therein. It is not a person who reasonably relies on the information contained in the certificate as mentioned in Section 40 of the Ordinance.

9.7.9 The Contractor is a contractor appointed by the HKPost pursuant to a separate contract between HKPost and the Contractor and the appointment is on the terms of that separate contract alone. Nothing in this CPS shall give any additional right to the Contractor, or impose additional obligation on HKPost to the Contractor. As for the representations in Sections 39 and 40 of the Ordinance, it is the duty of the Contractor (and also the Registration Bank as a sub-contractor) to ensure that they are complied with to the extent that the Contractor performs any function for the HKPost as stated therein. They are not persons who reasonably rely on the information contained in the certificate as mentioned in Section 40 of the Ordinance.

9.7.10 All Applicants, Subscribers, Registration Banks, the Contractor, Relying Parties, and other persons, entities, and organisations acknowledge that but for HKPost's disclaimers of representations, warranties, and conditions in Sections 9.7 and 9.8 and the limitations of liability in this Section 9.7, HKPost would not issue Certificates to Subscribers, that neither would HKPost provide services in respect to Certificates, and that these provisions are necessary to provide for a reasonable allocation of risk.

9.7.11 Whilst the Registration Bank acting as a sub-contractor of the Contractor and therefore also for HKPost, performs verification of the identity of the Applicant and in case of Bank-Cert (Corporate), also the identity and due authorisation of the Authorised Representative(s) and Authorised User(s) of the Applicant both in first time application and renewal (as more particularly specified in Sections 3.1.1, 3.15 and 3.2.1), and also similar verification of identity in the case of revocation request as specified in Section 4.3.2.3, HKPost will not be responsible or liable to any person including a Registration Bank's customer or a Relying Party for any act or default or omission or negligence on the part of the Registration Bank in performing any such functions. To the maximum extent permitted by the law and unless there is any breach of the representations specified in Sections 39 and 40 of the Ordinance, all and any liabilities are disclaimed to the fullest possible extent. In the event of any claim or legal proceedings against the HKPost or the Government arising from any such act or default or omission or negligence on the part of the Registration Bank, whether based on a breach of Section 39 or 40 of the Ordinance or otherwise, the Registration Bank shall indemnify each of HKPost and the Government from all such claims and proceedings, and all liabilities, losses, expenses, costs and charges (including legal fees on a full indemnity basis) suffered and incurred by HKPost arising from such claims or legal proceedings.

9.7.12 For all other functions and obligations performed by the Registration Bank whether as stated in this CPS or otherwise, none of them are performed by it as sub-contractor or agent for the Contractor or for HKPost. Under no circumstances will HKPost be responsible for any act, omission, default or negligence on the part of the Registration Bank or its contractors or agents in the performance or non-performance of any such functions or obligations.

9.7.13 Each of provisions in this Section 9.7 and 9.8 below shall be construed independently and without prejudice to any other provision of this CPS and, except where expressly stated otherwise, shall not be limited by reference to or inference from any other provision of this CPS.

9.8 Disclaimers of warranties and limitation on the types of recoverable losses

9.8.1 Without prejudice to the generality of the disclaimer set out in Section 9.7, in no event and under no circumstances (except for fraud or willful misconduct) shall HKPost be liable for any or all of the following and the results thereof:

9.8.1.1 Any indirect, incidental or consequential losses or damage (even if HKPost has been advised of the likelihood of such loss or damage in advance);

9.8.1.2 (whether considered as direct or indirect loss) Any loss of profits or loss or injury to reputation or goodwill or loss of opportunity or chance, loss of project;

9.8.1.3 Any death or personal injury (save and except for any Negligence of the HKPost and "Negligence" as defined in the Control of Exemption Clauses Ordinance (Cap 71 of the Laws of Hong Kong);

9.8.1.4 Any loss of data;

9.8.1.5 Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, licence, performance or non-performance of certificates or digital signatures;

9.8.1.6 Any claim, proceeding, loss or damage (direct or indirect or incidental or consequential special) except for those due to reliance on, the representations set out in Sections 39 and 40 of the Ordinance;

9.8.1.7 Any claim liability incurred arising from reliance on the Certificate or any information in the Certificate or Repository where any irregularity is due to fraud or willful misconduct of the Applicant or Subscriber or Registration Bank or any other person;

9.8.1.8 Any liability that arises from the usage of a Certificate that has not been used in conformance with this CPS;

9.8.1.9 Any liability that arises from the usage of a Certificate that is not valid (which has expired or revoked or suspended);

9.8.1.10 Any liability that arises from usage of a Certificate that exceeds any applicable limitations in usage and value and transactions; without prejudice to the generality of the foregoing, including usage of a Certificate in a transaction or any other application purpose which is not a Designated Transaction specified opposite the name of the Registration Bank in Appendix E for such type of Certificate;

9.8.1.11 Any liability that arises from security, usability, integrity of products, including hardware and software a Subscriber uses;

9.8.1.12 Any liability that arises from compromise of the Private Key in relation to any Certificate.

9.8.2 No Supply of Goods

For the avoidance of doubt, a Subscriber Agreement is not a contract for the supply of goods of any description or at all. Any and all certificates issued pursuant to it remain the property of and in the possession and control of HKPost and no right, title or interest in the certificates is transferred to the Subscriber, who merely has the right to procure the issue of a certificate and to rely upon it and the certificates of other Subscribers in accordance with the terms of the Subscriber Agreements. Accordingly the Subscriber Agreements contain (or are to contain) no express or implied terms or warranties as to the merchantability or fitness of a certificate for a particular purpose or any other terms or conditions appropriate in a contract for the supply of goods. Equally HKPost, in making available the certificates in a public Repository accessible by Relying Parties is not supplying any goods or services to Relying Parties and likewise gives no warranty to Relying Parties as to the merchantability or fitness for a particular purpose of a certificate nor makes any other representation or warranty as if it were supplying goods or services to Relying Parties.

9.8.3 Time Limit For Making Claims

Without prejudice to the disclaimers and limitations set out in Sections 9.7 and 9.8 and elsewhere in this CPS, any Subscriber or Relying Party or Registration Bank or any other person who wishes to make any legal claim upon HKPost arising out of or in any way connected with the issuance, suspension, revocation or publication of a Bank-Cert must do so within one year of the date upon which it becomes aware of any facts giving rise to the right to make such a claim or (if earlier) within one year of the date when, with the exercise of reasonable diligence, it could have become aware of such facts. For the avoidance of doubt, ignorance of the legal significance of those facts is immaterial. After the expiration of this one-year time limit the claim shall be waived and absolutely barred.

9.8.4 Hong Kong Post Office, the Contractor, Registration Banks and their Personnel

Neither the Government, nor any officer or employee or other agent of the Government (apart from the Postmaster General), is to be a party to the Subscriber Agreement, and the Subscriber, the Registration Bank and Relying Parties must acknowledge that, as far as the Subscriber, the Registration Bank, and Relying Parties are aware, neither the Government, nor any of its officers (apart from Postmaster General), employees or agents (including those officers employees and agents of HKPost) voluntarily accepts or will accept any personal responsibility or duty of care to the Subscriber or the Registration Bank or Relying Parties in connection with any action or omission done in good faith by any of them in any way connected either with the performance of HKPost of a Subscriber Agreement or any certificate issued by HKPost as a CA and each and every Subscriber Registration Bank Contractor and Relying Party accepts and will continue to accept that and undertakes to the Government and its officers and employees and agents (including those officers, employees and agents of HKPost) not to sue or seek any form of recovery or redress by other legal means whatsoever from any of them in respect of any act or omission done by that person in good faith (whether done negligently or not) in any way connected with either the performance of HKPost of a Subscriber Agreement or any certificate issued by HKPost as a CA and acknowledges that HKPost has a sufficient legal and financial interest to protect these organisations and individuals from such actions.

9.8.5 Liability for Fraud
Any liability for fraud of HKPost is not within the scope of any limitation or exclusionary provision of this CPS, any Subscriber Agreement or certificate issued by HKPost and is not limited or excluded by any such provision.

9.8.6 Certificate Notices, Limitations and Reliance Limit
Without prejudice to the binding effect of the remaining provisions of this CPS, Bank-Certs issued by HKPost shall be deemed to have contained all provisions set out in Sections 9.6 to 9.15 of this CPS.

9.9 Indemnities
By accepting or using or relying on a certificate, each Subscriber, Registration Bank and Relying Party agrees to indemnify and hold HKPost, as well as the Government, and the officers, employees, agents, and contractors of the Government (including those of HKPost) harmless from all and any liabilities, all and any losses damage and indebtedness, and all and any claims, legal proceedings, and costs, charges and expenses of any kind, including legal fees on a full indemnity basis, that HKPost, and/or the above mentioned parties may incur, that are caused by the use or publication of a certificate, and that arises from that party's: (i) misrepresentation or omission of material fact in order to obtain or use a Certificate (whether such misrepresentation or omission was intentional or due to negligence or recklessness); (ii) violation of the Subscriber Agreement, this CPS, or any applicable law; (iii) compromise or unauthorised use of a Certificate or Private Key caused by the negligence of that party and not by HKPost; or (iv) misuse of the Certificate or Private Key.

9.10 Term and termination

9.10.1 Term
This CPS and any amendments hereto shall become effective upon publication in the Repository and shall remain in effect perpetually until terminated in accordance with this Section 9.10.

9.10.2 Termination

This CPS as amended from time to time shall remain in force until it is replaced by a new version or is otherwise terminated in accordance with this Section 9.10.

9.10.3 Effect of termination and survival
The conditions and effect resulting from termination of this CPS will be communicated via the HKPost Repository (http://www.eCert.gov.hk) upon termination. That communication will outline the provisions that may survive termination of this CPS and remain in force. The responsibilities for protecting business confidential and private personal information shall survive termination, and the terms and conditions for all existing Certificates shall remain valid for the remainder of the validity periods of such Certificates.

It is hereby declared that no person's consent is required for the HKPost's termination of this CPS.

9.11 Individual notices and communications with participants
HKPost accepts notices related to this CPS by means in electronic form or in paper form addressed to the locations specified in Section 1.3of this CPS. Upon receipt of a valid acknowledgment of receipt from HKPost, the sender of the notice shall deem their communication effective.

9.12 Amendments

9.12.1 All changes to this CPS will be published by HKPost who has the power to determine such changes. **It is hereby declared that no person's consent is required for the HKPost's changes to this CPS.** The CPS changes will be effective upon publication by HKPost in the HKPost CA web site at http://www.eCert.gov.hk or in the HKPost Repository and are binding on all Applicants, Subscribers, Registration Banks, Relying Parties, the Contractor and other parties who may be treated as third parties under the Subscriber Agreement without any prior reference to, or consent from, any of them. HKPost will notify the Government Chief Information Officer any subsequent changes to this CPS as soon as practicable. A copy of this CPS and its predecessors are available for viewing by Applicants, Subscribers, Registration Banks, and Relying Parties on the HKPost CA web site at http://www.eCert.gov.hk. For those Subscribers or Registration Banks which do not agree with any changes to the CPS as aforementioned, they have a period of one month following from such changes coming into effect to issue a notice to HKPost to cease using the Bank-Cert under Section 4.3.2.1 and Section 4.3.2.2 respectively and early terminate the Bank-Cert (via the Registration Bank in the case of Subscriber being a holder of Bank-Cert (Personal) or (Corporate)). The absence of any such notice on the part of a Subscriber or Registration Bank within the aforesaid one-month period shall be taken as agreement of the Subscriber or Registration Bank with such changes.

9.12.2 The Subscriber Agreement cannot be varied, amended or changed unilaterally by any party except by HKPost to comply with a variation or change in this CPS. Subject to the foregoing, all other changes must be agreed by the parties to the Subscriber Agreement. No consent from any of the third parties as mentioned in paragraph 6.8 of the Subscriber Agreement shall be required for any amendment as mentioned above (whether by HKPost unilaterally or by agreement between the Subscriber and HKPost).

9.12.3 No consent from any of the third parties as mentioned in paragraph 6.8 in the Subscriber Agreement shall be required for any termination of the Subscriber Agreement or termination or revocation or suspension of any Bank-Cert by a party in accordance with the terms of the CPS (whether by HKPost or by a Subscriber unilaterally or by agreement between HKPost and the Subscriber).

9.12.4 Reasonable steps have been taken to make these third parties to be aware of this Section 9.12 through publication of the CPS.

9.12.5 **Appendix E** may be amended by HKPost from time to time by adding to it new Registration Bank which have successfully become Subscriber of a Bank-Cert (Bank).

9.13 Dispute Resolution

Any dispute or difference arising out of or in connection with this CPS or the Subscriber Agreement shall first be referred to mediation at Hong Kong International Arbitration Centre (HKIAC) and in accordance with its then current Mediation Rules. If the mediation is abandoned by the mediator or is otherwise concluded without the dispute or difference being resolved, then each of the parties hereto submit to the exclusive jurisdiction of the courts of Hong Kong for resolving such dispute or difference.

9.14 Governing law

This CPS is governed by, and construed in accordance with the law of the Hong Kong. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of HKPost digital certificates.

Each party, including HKPost, Subscribers, Registration Banks, Contractor and Relying Parties, irrevocably agree that a court of Hong Kong shall have exclusive jurisdiction to hear and decide any suit, action or proceedings, and to settle any disputes, which may arise out of or in connection with this CPS or the Subscriber Agreement.

9.15 Entire agreement

9.15.1 This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances, and intended usage of the product or service described herein. In interpreting this CPS the parties shall also take into account the scope and application of the services and products of HKPost as well as the principle of good faith as it is applied in commercial transactions. Notwithstanding the foregoing, the Certification Practice Statement issued by HKPost for other types of certificates shall not be referred to in the interpretation of the provisions set out in this CPS.

9.15.2 The headings, subheadings, and other captions in this CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS.

9.15.3 Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS.

9.15.4 If/when this CPS (as from time to time amended) conflicts with other rules, guidelines, or contracts, this CPS shall prevail (save to the extent the provisions of this CPS are prohibited by the Ordinance) and bind the Subscriber and other parties. If there is any conflict between the sections of this CPS and any other document that relate to HKPost, then the sections benefiting HKPost and preserving HKPost's best interests, at HKPost's sole determination, shall prevail and bind the applicable parties.

9.16 Assignment

Parties to this CPS may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent of HKPost.

9.17 Severability

9.17.1 If any provision of this CPS or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall remain in full force and effect and shall be interpreted in such manner as to implement the original intention of the parties to the fullest extent possible.

9.17.2 Each and every provision of this CPS that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

9.18 Enforcement (attorneys' fees and waiver of rights)

HKPost reserves the right to seek indemnification and legal fees from any party related to that party's conduct described in Section 9.9. Except where an express time frame is set forth in this CPS, no delay or omission by any party to exercise any right, remedy or power it has under this CPS shall impair or be construed as a waiver of such right, remedy or power. A waiver by any party of any breach or covenant in this CPS shall not be construed to be a waiver of any other or succeeding breach or covenant. Bilateral agreements between HKPost and the parties to this CPS may contain additional provisions governing enforcement.

9.19 Force Majeure

HKPOST INCURS NO LIABILITY IF IT IS PREVENTED, FORBIDDEN OR DELAYED FROMPERFORMING, OR OMITS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF: ANYPROVISION OF ANY APPLICABLE LAW, REGULATION OR ORDER; CIVIL, GOVERNMENTAL ORMILITARY AUTHORITY; THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER SYSTEMOPERATED BY ANY OTHER PARTY OVER WHICH IT HAS NO CONTROL; FIRE, FLOOD, OR OTHEREMERGENCY CONDITION; STRIKE; ACTS OF TERRORISM OR WAR; ACT OF GOD; OR OTHERSIMILAR CAUSES BEYOND ITS REASONABLE CONTROL AND WITHOUT ITS FAULT ORNEGLIGENCE.

9.20 Other provisions

9.20.1 This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties that this CPS applies to. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this CPS articles on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

9.20.2 Retention of Title

The title, physical, copyright, and intellectual property rights to the certificate are and will remain vested in HKPost.

9.20.3 Fiduciary Relationships

None of HKPost nor the Contractor is an agent, fiduciary, trustee or other representative of the Subscribers or the Registration Bank or Relying Parties at any time. Subscribers Registration Bank and Relying Parties have no authority to bind HKPost or the Contractor, by contract or otherwise, to any obligation as an agent, fiduciary, trustee or other representative.

9.20.4 Interpretation

Where there is a conflict of interpretation of wording between the English and Chinese versions of this CPS, the English version shall prevail.

Appendix A - Glossary

Definitions

1. Unless the context otherwise requires, the following expressions have the following meanings in this CPS

"Accept" (upper or lower case), in relation to a certificate

(a) in the case of a person named or identified in the certificate as the person to whom the certificate is issued, means to –
   (i) confirm the accuracy of the information on the person as contained in the certificate;
   (ii) authorise the publication of the certificate to any other person or in a repository;
   (iii) use the certificate; or
   (iv) otherwise demonstrate the approval of the certificate; or

(b) in the case of a person **to be** named or identified in the certificate as the person to whom the certificate is issued, means to –
   (i) confirm the accuracy of the information on the person that is to be contained in the certificate;
   (ii) authorise the publication of the certificate to any other person or in a repository; or
   (iii) otherwise demonstrate the approval of the certificate.

   For the avoidance of doubt, acceptance as defined above may be done by a Registration Bank on behalf of the person named or identified in the certificate as the person to whom the certificate is issued.

"Applicant" means a natural person or organisation or bank who has applied for any certification types of Bank-Cert. Once the Bank-Cert is issued, the Applicant is referred to as the Subscriber.

"Asymmetric Cryptosystem" means a system capable of generating a secure key pair, consisting of a Private Key for generating a Digital Signature and a Public Key to verify the Digital Signature.

"Authorised Representative"means the duly authorised representative of a Subscriber which is organisation or a bank.

"Authorised Unit" means an identified unit within the Registration Bank which has been duly authorised to configure, operate and maintain the Bank-Cert (Bank) issued to that Registration Bank including its Private Key and associated IT system.

"Authorised User" means in the case of Subscriber being an organisation, the individual whose name is stated in the Bank-Cert (Corporate) and who is authorised to use the Bank-Cert (Corporate) on behalf of that organisation in Designated Transactions.

"Authority Revocation List" or **"ARL"** means a data structure that enumerates public-key certificates of Sub CAs that have been invalidated by the Root CA prior to the time at which they were scheduled to expire.

"bank" has the meaning given to the term in the Banking Ordinance, Cap 155 of the laws of Hong Kong;

"Certificate" (upper or lower case) **or "Bank-Cert"** means a Record which:-

a) is issued by HKPost for the purpose of supporting a Digital Signature which purports to confirm the name of the person stated therein is the person authorised to use the Private Key corresponding to the Public Key contained in the certificate.

b) identifies the HKPost as the Certification Authority 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 HKPost as the Certification Authority issuing it.

"Certification Authority" or "CA" means a person who issues a certificate to a person (who may be another Certification Authority).

"Certification Practice Statement" or "CPS" means this document including all Appendices thereto.

"Certificate Revocation List" or "CRL" means a data structure that enumerates public-key certificates (or other kinds of certificates) that have been invalidated by their issuer prior to the time at which they were scheduled to expire.

"cheque" has the meaning given to it in Section 73 of the Bills of Exchange Ordinance (Cap 19 of the Laws of Hong Kong).

"Contract" means the outsourcing contract which HKPost from time to time enters into with a contractor for performing all or any of the functions of the HKPost CA as stipulated in this CPS on behalf of HKPost under the overall supervision and management of HKPost .

"Contractor" means the contractor to the Contract as from time to time entered into by HKPost; and all sub-contractors of such contractor;

"Correspond", in relation to Private or Public Keys, means to belong to the same key pair.

"COP" means the Code of Practice for Recognized Certification Authorities published by the Government Chief Information Officer under Section 33 of the Ordinance.

"CRL" means Certificate Revocation List.

"**Certificate Signing Request**" or "**CSR**" means a message sent by the Registration Bank for an Applicant to HKPost in order to apply for a Certificate.

"Designated Transaction" means, in relation to Bank-Cert (Bank) issued to a bank, the transactions specified opposite the name of that bank for such type of Bank-Cert; and
In relation to a Bank-Cert (Personal) or (Corporate) issued via a Registration Bank, the transactions specified opposite the name of that Registration Bank for such type of Bank-Cert;

"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.

"e-cheque" means a cheque in the form of an Electronic Record.

"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.

"Electronic Signature" means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an Electronic Record, and executed or adopted for the purpose of authenticating or approving the Electronic Record.

"HKID Card" means the Hong Kong Identity Card issued by the Immigration Department of the Hong Kong Special Administrative Region.

"Hardware Security Module", or "HSM" means a hardware security device used for central storage and management of Bank-Cert and protection of key pairs from being exported or duplicated.

"HKD" or "HK$" or Hong Kong Dollars" means the lawful currency of Hong Kong.

"information" includes data, text, images, sound, 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" (upper or lower case) in relation to a certificate, means to:

(a) create the certificate, and then notify directly or indirectly via the Registration Bank 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 directly or indirectly via the Registration Bank 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, key pair means a Private Key and its mathematically related Public Key, where the Public Key can verify a Digital Signature that the Private Key generates.

"Know Your Customer" or "KYC" has the meaning given to the term in Section 3.1.1.

"Ordinance" means the Electronic Transactions Ordinance (Cap. 553).

"organisation" means any entity other than an individual;

"Postmaster General" or "HKPost" means the Postmaster General within the meaning of the Post Office Ordinance (Cap.98).

"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.

"RB" means Registration Bank.

"Recognized Certificate" means

(a) a certificate recognized under Section 22 of Electronic Transactions Ordinance;
(b) a certificate of a type, class or description of certificate recognized under Section 22 of Electronic Transactions Ordinance; or
(c) a certificate designated as a recognized certificate issued by the Certification Authority referred to in Section 34 of Electronic Transactions Ordinance.

"Recognized Certification Authority" means a Certification Authority recognized under Section 21 or the Certification Authority referred to in Section 34 of Electronic Transactions Ordinance.

"Record" (upper or lower case) 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.

"Registration Bank" means in relation to a Bank-Cert (Bank), any bank as listed in **Appendix E**.

In relation to a Bank-Cert (Personal) or Bank-Cert (Organisation) and the Applicant or Subscriber of such Bank-Cert, a bank which is listed in Appendix E via which the application for such Bank-Cert is submitted or via which the Bank-Cert is issued.

"Reliance Limit" means the monetary limit specified for reliance on a Bank-Cert in the amount as specified in Section 9.7.

"Relying Parties" means a person who may reasonably relies on the information contained in a Bank-Cert by complying with the warranties and representations specified in Section 9.6.4

"**RMB**" or "**Renminbi**" means the lawful currency of the People's Republic of China.

"Repository" means an Information System for storing and retrieving certificates and other information relevant to certificates.

"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.

"**SRN**" means a Subscriber Reference Number generated by the HKPost system.

"Sub CA" means the subordinate Certification Authority certificate which is issued by the Root CA "Hongkong Post Root CA 2" and is used to Sign the HKPost Recognized Certificates.

"Subscriber" means a person who:-

(i) is named or identified in a certificate as the person to whom the certificate is issued;
(ii) has accepted that certificate; and
(iii) in the case of Bank-Cert (Bank) only, holds a Private Key which corresponds to a Public Key listed in that certificate; and
(iv) in the case of Bank-Cert (Personal) or (Corporate) has authorised the Registration Bank to hold the Private Key which corresponds to a Public Key listed in that certificate.

Note:- "holds", in connection to a Private Key as referred in this CPS, means to keep in one's custody such that only the person named or identified in a certificate can use that Private Key.

"Subscriber Agreement", in respect of Bank-Cert (Personal)/(Corporate),means an agreement between HKPost and the Subscriber of such certificate, which comprises the subscriber terms and conditions and this CPS . In respect of Bank-Cert (Bank), it means an agreement between the Registration Bank of such certificate and HKPost which comprises the subscriber terms and conditions specified and this CPS.

"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.

"USD" or "US$" or "US Dollars" means the lawful currency of the United States of America.

Interpretation Principles

2. In this CPS, unless the context otherwise requires, the following rules of interpretation shall apply:

2.1 references to statutes or statutory provisions shall be construed as references to those statutes or statutory provisions as replaced, amended, modified or re-enacted from time to

time; and shall include all subordinate legislation made under those statutes;

2.2 words importing the singular shall include the plural and vice versa; words importing a gender shall include all other genders; references to any person shall include references to any individual, firm, body corporate or unincorporate (wherever established or incorporated);

2.3 clauses headings are inserted for convenience of reference only and shall not affect the construction of this CPS;

2.4 references to a document shall:

(a) include all schedules, appendices and annexures attached to such document; and

(b) mean the same as from time to time validly amended or supplemented;

2.5 references to "Registration Bank" or "Subscriber" or "Applicant" or "Relying Party" or "Contractor" shall include its permitted assigns, successors-in-title, or any persons deriving title under it;

2.6 references to "HKPost" shall include its assigns, successors-in-title, and persons deriving title under it, regardless of whether or not any of these persons are mentioned separately in the relevant provisions;

2.7 references to Sections of, and Appendices or Annexes to this CPS shall, unless otherwise specified, mean the sections of, and appendices and annexes to, this CPS;

2.8 references to "laws" and "regulations" or "law" shall include any constitutional provisions, treaties, conventions, ordinances, subsidiary legislation, orders, rules and regulations having the force of law and rules of civil and common law and equity;

2.9 a time of day shall be construed as a reference to Hong Kong time;

2.10 references to a month or a monthly period mean a calendar month;

2.11 any negative obligation imposed on any party shall be construed as if it were also an obligation not to permit or suffer the act or thing in question, and any positive obligation imposed on any party shall be construed as if it were also an obligation to procure that the act or thing in question be done;

2.12 any act, default, neglect or omission of any employee, licensee, agent or sub-contractor of the Registration Bank or Applicant or Subscriber or Contractor shall be deemed to be the act, default, neglect or omission of that person;

2.13 words importing the whole shall be treated as including a reference to any part of the whole;

2.14 the expressions "include" and "including" shall mean including without limitation basis regardless of whether it is expressly so provided;

2.15 words and expressions extend to their grammatical variations and cognate expressions where those words and expressions are defined in this CPS or by reference to any other definition;

2.16 references to "writing" include typewriting, printing, lithography, photography, facsimile and the printed out version of a communication by electronic mail and other modes of representing and reproducing words in a legible form;

2.17 References to "Cap" or "Chapter" followed by a number mean a chapter of the Laws of Hong Kong.

2.18 Nothing in this CPS shall be taken to restrict, derogate from or otherwise interfere with any

power or duty, or the exercise or performance of any power or duty conferred or imposed by or under any law upon HKPost.

Appendix B - Hongkong Post Bank-Cert Format

This appendix provides the formats of Bank-Cert issued by the Sub CA "Hongkong Post e-Cert CA 2 - 15" under this CPS.

A. Bank-Cert (Personal) Certificate Format

Field Name		Field Content
Standard fields		
Version		X.509 v3
Serial number		[Set by HKPost CA system]
Signature algorithm ID		sha256RSA
Issuer name		cn=Hongkong Post e-Cert CA 2 - 15, o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK
Validity period	**Not before**	[UTC time set by HKPost CA system]
	Not after	[UTC time set by HKPost CA system]
Subject name		cn=[Subscriber's name registered with the Registration Bank](Note 1) e=[email address] (Note 2) ou=[SRN](Note 3) o=Hongkong Post Bank-Cert (XXX-Personal) (Note 4) c=HK
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size
Issuer unique identifier		Not used
Subject unique identifier		Not used
Standard extension (Note 5)		
Authority key identifier	**Issuer**	cn=Hongkong Post Root CA 2, o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK
	Serial number	[Inherited from Issuer]
Key usage		Non-repudiation, Digital Signature **(This field will be set Critical.)**
Certificate policies		[1]Certificate Policy: Policy Identifier = [OID](Note 6) [1,1]Policy QualifierID = CPS Qualifier : [URL of CPS] [2]Certificate Policy: Policy Identifier = [1.3.6.1.4.1.16030.1.4] (Note 7) [2,1]Policy QualifierID = CPS Qualifier : [URL of CPS]
Subject alternative name	**1st DNS**	Encrypted(an identity number of the Applicant given by the Registration Bank)(Note 8)
	2nd DNS	[For bank reference only](Note 9)
	1st Directory Name	cn=Subscriber's Chinese name registered with the Registration Bank(Note 10)
	rfc822	[Applicant's email address](Note 2)
Issuer alternate name		Not used
Basic constraint	**Subject type**	End Entity

Field Name		Field Content
	Path length constraint	None
Extended key usage		Not used
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point](Note 11)
Netscape extension (Note 5)		
Netscape cert type		SSL Client, S/MIME
Netscape SSL server name		Not used
Netscape comment		Not used

Note

1. Applicant name registered with the Registration Bank, for example, Surname (in capital) + Given name (e.g. CHAN Tai Man David).
2. Email address is optionally provided by Applicant (blank if null).
3. SRN: 10-digit Subscriber Reference Number
4. XXX is the name of Registration Bank as specified in **Appendix E**.
5. All standard extensions and Netscape extensions are set as "non-critical" unless otherwise specified.
6. The OID of this CPS is included in this field. Please refer to Section1.1 of this CPS for the OID of this CPS.
7. The OID that indicates a certificate is in compliance with the Adobe Approved Trust List ("AATL") technical requirement is included in this field.
8. The Applicant's identity number given by the Bank (**id_number**) will be stored in the certificate in the form of a hash value of that identity number (**cert_id_hash**) which has been signed by the Private Key of the Applicant:-

   cert_id_hash = *SHA-256*($RSA_{privatekey,\ sha\text{-}256}$(id_number))

   where the *SHA-256 i*s a hash function and *RSA* is the signing function

9. Upon pre-arrangement with the Registration Bank, a value as given by the Registration Bank will be stored for bank reference only.
10. Where the Applicant/Subscriber has a Chinese name, the Registration Bank shall provide that Chinese name to HKPost. In doing so, it must adopt the international coding standard ISO/IEC 10646. Where such Chinese name is provided, the name will be stored in this field.
11. URL of CRL Distribution Point is http://crl1.eCert.gov.hk/crl/eCertCA2-15CRL1_<xxxxx>.crl which are partitioned CRLs issued by the Sub CA "Hongkong Post e-Cert CA 2 - 15", where <xxxxx> is a string of five alphanumeric characters generated by the CA system. (For certificates issued before 1 July 2019, URL of CRL Distribution Point is http://crl1.hongkongpost.gov.hk/crl/eCertCA2-15CRL1_<xxxxx>.crl) HKPost CA publishes a number of partitioned CRLs. If a certificate is suspended or revoked, its information will be published in the partitioned CRL at the URL specified in this CRL Distribution Point field.

B. Bank-Cert (Corporate)Certificate Format

Field Name		Field Content
Standard fields		
Version		X.509 v3
Serial number		[Set by HKPost CA system]
Signature algorithm ID		sha256RSA
Issuer name		cn=Hongkong Post e-Cert CA 2 - 15, o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK
Validity period	**Not before**	[UTC time set by HKPost CA system]
	Not after	[UTC time set by HKPost CA system]
Subject name		cn=[Authorised User's name registered with the Registration Bank](Note 1) e=[email address] (Note 2) ou=[SRN](Note 3) ou=[An identifier of Subscriber organisation as given by the Registration Bank] (Note 4) ou=[Subscriber organisation Name] (Note 5) ou=[Subscriber organisation branch/dept] o=Hongkong Post Bank-Cert (XXX-Corporate)(Note 6) c=HK
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size
Issuer unique identifier		Not used
Subject unique identifier		Not used
Standard extension (Note 7)		
Authority key identifier	**Issuer**	cn=Hongkong Post Root CA 2, o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK
	Serial number	[Inherited from Issuer]
Key usage		Non-repudiation, Digital Signature **(This field will be set Critical.)**
Certificate policies		[1]Certificate Policy: Policy Identifier = [OID](Note 8) [1,1]PolicyQualifierID = CPS Qualifier : [URL of CPS] [2]Certificate Policy: Policy Identifier = [1.3.6.1.4.1.16030.1.4] (Note 9) [2,1]Policy QualifierID = CPS Qualifier : [URL of CPS]
Subject alternative name	**1st DNS**	Encrypted(an identity number of Authorised User given by the Registration Bank)(Note 10)
	2nd DNS	[For bank reference only] (Note 11)
	1st Directory Name	cn=Authorised User's Chinese name registered with the Registration Bank(Note 12) ou=Subscriber organisation's Chinese name ou=Subscriber organisation's Chinese branch/dept name
	rfc822	[Authorised User's email address](Note 2)
Issuer alternate name		Not used
Basic constraint	**Subject type**	End Entity
	Path length constraint	None

Field Name		Field Content
Extended key usage		Not used
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point](Note13)
Netscape extension (Note 7)		
Netscape cert type		SSL Client, S/MIME
Netscape SSL server name		Not used
Netscape comment		Not used

Note

1. Authorised Username registered with the Registration Bank with format, for example, Surname (in capital) + Given name (e.g. CHAN Tai Man David).
2. Email address of the Authorised User is optionally provided by Subscriber organisation(blank if null)
3. SRN: 10-digit Subscriber Reference Number
4. The identifier of Subscriber organisation that can uniquely reference to the evidence of identity of the Subscriber organisation.
5. For organisations who subscribe to Bank-Cert and are organisations with names in the Chinese language only or who have provided their Chinese names only, their Chinese names will be included in this field (see Section 3.1.6of this CPS).
6. XXX is the name of Registration Bank as specified in **Appendix E**.
7. All standard extensions and Netscape extensions are set as "non-critical" unless otherwise specified.
8. The OID of this CPS is included in this field. Please refer to Section 1.1 of this CPS for the OID of this CPS.
9. The OID that indicates a certificate is in compliance with the AATL technical requirement is included in this field.
10. The Authorised User's identity number given by the Bank (**id_number**) will be stored in the certificate in the form of a hash value of that identity number (**cert_id_hash**) which has been signed by the Private Key of the Authorised User:-

    cert_id_hash = *SHA-256*($RSA_{privatekey,\ sha\text{-}256}$ (id_number))

    where the *SHA-256* is a hash function and *RSA* is the signing function
11. Upon pre-arrangement with the Registration Bank, a value as given by the Registration Bank will be stored for bank reference only.
12. Where the Authorised User has a Chinese name and/or the Subscriber organization has Chinese name, the name shall be provided by the Registration Bank to HKPost by adopting the international coding standard ISO/IEC 10646.Where provided, this name will be published in this field in addition to the name in English published in the field annotated by Note 5.
13. URL of CRL Distribution Point is http://crl1.eCert.gov.hk/crl/eCertCA2-15CRL2.crl which is a partitioned CRL issued by the Sub CA "Hongkong Post e-Cert CA 2 - 15". (For certificates issued before 1 July 2019, URL of CRL Distribution Point is http://crl1.hongkongpost.gov.hk/crl/eCertCA2-15CRL2.crl)

C. Bank-Cert (Bank) Certificate Format

Field Name		Field Content
Standard fields		
Version		X.509 v3
Serial number		[Set by HKPost CA system]
Signature algorithm ID		sha256RSA
Issuer name		cn=Hongkong Post e-Cert CA 2 - 15, o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK
Validity period	**Not before**	[UTC time set by HKPost CA system]
	Not after	[UTC time set by HKPost CA system]
Subject name		cn=[Authorised Unit's name](Note 1) e=[email address] (Note 2) ou=[SRN](Note 3) ou=[BRN+CI/CR+Others] (Note 4) ou=[Bank Name] (Note 5) ou=[Bank branch/dept] o=Hongkong Post Bank-Cert (XXX-Bank)(Note 6) c=HK
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size
Issuer unique identifier		Not used
Subject unique identifier		Not used
Standard extension (Note 7)		
Authority key identifier	**Issuer**	cn=Hongkong Post Root CA 2, o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK
	Serial number	[Inherited from Issuer]
Key usage		Non-repudiation, Digital Signature **(This field will be set Critical.)**
Certificate policies		[1]Certificate Policy: Policy Identifier = [OID](Note 8) [1,1]Policy QualifierID = CPS Qualifier : [URL of CPS] [2]Certificate Policy: Policy Identifier = [1.3.6.1.4.1.16030.1.4] (Note 9) [2,1]Policy QualifierID = CPS Qualifier : [URL of CPS]
Subject alternative name	**DNS**	Not used
	1st Directory Name	cn=Authorised Unit's Chinese name(Note 10) ou=Bank's Chinese name ou=Bank's Chinese branch/dept name
	rfc822	[email address](Note 2)
Issuer alternate name		Not used
Basic constraint	**Subject type**	End Entity
	Path length constraint	None
Extended key usage		Not used

Field Name		Field Content
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point](Note 11)
Netscape extension (Note 7)		
Netscape cert type		SSL Client, S/MIME
Netscape SSL server name		Not used
Netscape comment		Not used

Note

1. Name of the Authorised Unit of the Registration Bank, or the Registration Bank name if Authorised Unit is not provided.
2. Email address is optionally provided by the Authorised Unit of the Registration Bank (blank if null)
3. SRN: 10-digit Subscriber Reference Number
4. Business Registration Certificate Number (BRN): a string of 16 digits/alphabets [filled with all zeroes if BRN is not available]. Certificate of Incorporation (CI)/ Certificate of Registration (CR): a string of 8 digits/alphabets [filled with leading zeros if CI/CR is shorter than 8 digits/alphabets, or all zeroes if CI/CR is not available]. Others: a string of max. 30 digits/alphabets (blank if null).
5. For organisations who subscribe to Bank-Cert and are originations with names in the Chinese language only or who have provided their Chinese names only, their Chinese names will be included in this field (see Section 3.1.6 of this CPS).
6. XXX is the name of Registration Bank as specified in **Appendix E**.
7. All standard extensions and Netscape extensions are set as “non-critical” unless otherwise specified.
8. The OID of this CPS is included in this field. Please refer to Section 1.1 of this CPS for the OID of this CPS.
9. The OID that indicates a certificate is in compliance with the AATL technical requirement is included in this field.
10. Chinese name of the Authorised Unit and the Bank Chinese name are optionally provided by the Registration Bank. If it is provided, it must adopt the international coding standard ISO/IEC 10646.
11. URL of CRL Distribution Point is http://crl1.eCert.gov.hk/crl/eCertCA2-15CRL2.crl which is a partitioned CRL issued by the Sub CA “Hongkong Post e-Cert CA 2 - 15”. (For certificates issued before 1 July 2019, URL of CRL Distribution Point is http://crl1.hongkongpost.gov.hk/crl/eCertCA2-15CRL2.crl)

Appendix C - Hongkong Post Certificate Revocation Lists (CRLs)and Authority Revocation List (ARL) Format

The Appendix C of this CPS provides the arrangement of updating and publishing as well as the format of the Certificate Revocation Lists (CRLs) that are issued by the Sub CA "Hongkong Post e-Cert CA 2 - 15", and the Authority Revocation List (ARL) that is issued by the root CA "Hongkong Post Root CA 2".

HKPost updates and publishes the following Certificate Revocation Lists (CRLs) containing information of Bank-Certs suspended or revoked under this CPS 3 times daily at 09:15, 14:15 and 19:00 Hong Kong Time (i.e. 01:15, 06:15 and 11:00 Greenwich Mean Time (GMT or UTC)):-

a) **Partitioned CRLs** that contain information of suspended or revoked certificates in groups. Each of the partitioned CRLs is available for public access at the following locations (URLs):-

i. Bank-Cert (Personal):
http://crl1.eCert.gov.hk/crl/eCertCA2-15CRL1_<xxxxx>.crl issued by the Sub CA "Hongkong Post e-Cert CA 2 - 15" where <xxxxx> is a string of five alphanumberic characters. (For certificates issued before 1 July 2019, URL of CRL Distribution Point is http://crl1.hongkongpost.gov.hk/crl/eCertCA2-15CRL1_<xxxxx>.crl)

ii. Bank-Cert (Corporate) and Bank-Cert (Bank):
http://crl1.eCert.gov.hk/crl/eCertCA2-15CRL2.crl issued by the Sub CA "Hongkong Post e-Cert CA 2 - 15". (For certificates issued before 1 July 2019, URL of CRL Distribution Point is http://crl1.hongkongpost.gov.hk/crl/eCertCA2-15CRL2.crl)

b) **Full CRL** that contains information of all suspended or revoked certificates that are issued by the Sub CA "Hongkong Post e-Cert CA 2 - 15". The Full CRL is available at :-

http://crl1.eCert.gov.hk/crl/eCertCA2-15CRL1.crl; or
ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post e-Cert CA2 - 15 CRL1, o=Hongkong Post, c=HK)

The URL for accessing the relevant CRL that contains the information of the suspended or revoked certificate is specified in the "CRL Distribution Points" field of the certificate.

Under normal circumstances, HKPost will publish the latest CRL as soon as possible after the update time. HKPost may need to change the above updating and publishing schedule of the CRL without prior notice if such changes are considered to be necessary under unforeseeable circumstances. Where circumstances warrant, HKPost may also publish supplementary update of CRLs at the HKPost web site at http://www.eCert.gov.hk/ on ad hoc basis without prior notice.

Format of Partitioned and Full CRL issued by the Sub CA "Hongkong Post e-Cert CA 2 - 15" under this CPS:-

Standard Fields	Sub-fields	Field Contents of Partitioned CRL	Field Contents of Full CRL	Remarks
Version		v2		This field describes the version of encoded CRL as X.509 v2.
Signature algorithm ID		sha256RSA		This field contains the algorithm identifier for the algorithm used to sign the CRL.
Issuer name		cn=Hongkong Post e-Cert CA 2 - 15, o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK		This field identifies the entity who has signed and issued the CRL.
This update		[UTC time]		"This Update" indicates the date the CRL was generated.

Standard Fields	Sub-fields	Field Contents of Partitioned CRL	Field Contents of Full CRL	Remarks
Next update		[UTC time]		"Next Update" contains the date by which the next CRL will be issued, but it will not be issued any later than the indicated date. Notwithstanding this, the CRL is updated and issued on a **daily** basis as stated in the CPS.
Revoked certificates	**User certificate**	[Certificate Serial Number]		Revoked certificates are listed by their serial numbers.
	Revocation date	[UTC time]		The date on which the revocation occurred is specified.
	CRL entry extensions			
	Reason code	[Revocation Reason Code]		(Note 1)
Standard extension (Note 2)				
Authority key identifier	**Issuer**	cn=Hongkong Post Root CA 2 o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK		This field provides a means of identifying the Public Key corresponding to the Private Key used to sign a CRL.
	Serial number	[Inherited from Issuer]		This field indicates the serial number of the issuer certificate.
CRL number		[Generated by CA system – each partitioned CRL has its own sequence]		The CRL Number is generated in sequence for each CRL issued by a CA.
Issuer distribution point		[DER Encoded CRL Distribution Point] **(This field will be set Critical.)**	Not used	This field is used for Partitioned CRLs only.

HKPost updates and publishes the Authority Revocation Lists (ARL) containing information of suspended or revoked Sub CA certificates under this CPS. HKPost shall update and publish the ARL annually before its next update date or when necessary. The latest ARL is available at the following location:

http://crl1.eCert.gov.hk/crl/RootCA2ARL.crl or
ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post Root CA 2, o=Hongkong Post, c=HK)

Format of ARL issued by the root CA "Hongkong Post Root CA 2" under this CPS :

Standard Fields	Sub-fields	Field Contents of ARL	Remarks
Version		v2	This field describes the version of encoded ARL as X.509 v2.
Signature algorithm ID		sha256RSA	This field contains the algorithm identifier for the algorithm used to sign the ARL.
Issuer name		cn=Hongkong Post Root CA 2 o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK	This field identifies the entity who has signed and issued the ARL.

Standard Fields	Sub-fields	Field Contents of ARL	Remarks
This update		[UTC time]	"This Update" indicates the date the ARL was generated.
Next update		[UTC time]	"Next Update" contains the date by which the next ARL will be issued, but it will not be issued any later than the indicated date. Notwithstanding this, the ARL is updated and issued on an **annual** basis as stated in the CPS.
Revoked certificates	User certificate	[Certificate Serial Number]	Revoked certificates are listed by their serial numbers.
	Revocation date	[UTC time]	The date on which the revocation occurred is specified.
	CRL entry extensions		
	Reason code	[Revocation Reason Code]	(Note 1)
Standard extension (Note 2)			
Authority key identifier	Issuer	cn=Hongkong Post Root CA2 o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK	This field provides a means of identifying the Public Key corresponding to the Private Key used to sign a ARL.
	Serial number	[Inherited from Issuer]	This field indicates the serial number of the issuer certificate.
CRL number		[Generated by CA system]	The CRL Number is generated in sequence for each ARL issued by a CA.
Issuer distribution point		Only Contains User Certs=No Only Contains CA Certs=Yes Indirect CRL=No **(This field will be set Critical.)**	

Note

1. The following reason codes may be included in the field:

   0=Unspecified, 1=Key compromise, 2=CA compromise, 3=Affiliation changed,
   4 = Superseded, 5=Cessation of operation, 6=Certificate hold

   The reason code "0" (i.e. unspecified) will be indicated since Applicants or Subscribers will not be required to give any particular reason of certificate revocation.

2. All fields will be set "non-critical" unless otherwise specified.

Appendix D - Summary of Hongkong Post Bank-Cert Features

Features	Bank-Cert (Personal) Certificate	Bank-Cert (Corporate) Certificate	Bank-Cert (Bank) Certificate
Subscriber	Individuals who has a bank account with the Registration Bank and who is 18 years of age or over(refer to Section 1.2.4.1)	organisations who holds a bank account with the Registration Bank identified in the certificate (refer to Section 1.2.4.2)	licensed banks with a banking licence issued under the Banking Ordinance(Cap 155 of the Laws of Hong Kong)
Authorised user of the Certificate	Same as Subscriber	Individuals identified and duly authorised by organisations (whether acting singly or jointly) to use the Bank-Cert (Corporate) issued to that organisation (viz., Authorised User(s)).	The use of the Bank-Cert (Bank) will be automated through the use of IT system but the IT system including the Bank-Cert (Bank) and its Private Key will only be configured, operated and maintained by authorised personnel passing through strong authentication process. Where applicable, such personnel are identified as the Authorised Unit in the certificate.
Reliance Limit	HK$200,000		
Recognized Certificate	Yes		
Key pair size	2048-bit RSA		
Registration Bank	See **Appendix E**	See **Appendix E**	Not Applicable
Key pair generation	Key generation by Registration Bank		
Identity verification at the time of application for the Bank-Cert	as mentioned in Section 3.1	As mentioned in Section 3.1	Authentication of the identity of the Bank and its Authorised Representative as mentioned in Section 3.1
Usage of certificate	Non-repudiable Digital Signature in Designated Transactions specified opposite the name of the Registration Bank via which it is issued.	Non-repudiable Digital Signature in Designated Transactions specified opposite the name of the Registration Bank via which it is issued.	Non-repudiable Digital Signature in Designated Transactions specified opposite the name of the Subscriber bank.
Subscriber's information included in the certificate	▪ Name of the Subscriber; ▪ An identifier of the Subscriber as given by the Registration Bank that is encrypted as a hash value; ▪ Email address; and ▪ Subscriber Reference Number (SRN) generated by the HKPost system.	▪ Name of the Subscriber; ▪ Name of the Authorised User's name and email address; ▪ Subscriber Reference Number (SRN) generated by the HKPost system; ▪ An identifier of Subscriber organisation as given by the Registration Bank; and ▪ An identifier of Authorised User as given by the Registration Bank that is encrypted as a hash value.	▪ Bank's name; ▪ Authorised Unit's name and email address (where provided); ▪ Subscriber Reference Number (SRN) generated by the HKPost system; and ▪ Bank's company/business registration information;

Features	Bank-Cert (Personal) Certificate	Bank-Cert (Corporate) Certificate	Bank-Cert (Bank) Certificate
Subscription fees and Administration fees	(see the last column of Appendix E of this CPS)		
Certificate validity	Certificate validity ranges from one year to five years.	Certificate validity ranges from one year to five years.	Certificate validity ranges from one year to five years.

Appendix E – List of Registration Banks and the corresponding Designated Transactions of Hongkong Post Bank-Cert

Bank-Cert Type	Name of Registration Bank	Certificate Validity	Designated Transaction	Subscription Fees	Remarks
Bank-Cert (Personal)	The Hongkong and Shanghai Banking Corporation Limited	1 - 5 years	Creation of a digital signature by the Subscriber of the Bank-Cert on an e-cheque as the drawer which e-cheque for a sum in Hong Kong Dollars or US Dollars or Renminbi is drawn on the Registration Bank specified opposite	The Hongkong and Shanghai Banking Corporation Limited shall pay all subscription fees and administration fees	For handling suspension or revocation request from Subscribers, the Hongkong and Shanghai Banking Corporation Limited will, within five working days after the date of receipt, notify HKPost of the receipt of the request.
Bank-Cert (Personal)	CMB Wing Lung Bank Limited*	1 - 5 years	Creation of a digital signature by the Subscriber of the Bank-Cert on an e-cheque as the drawer which e-cheque for a sum in Hong Kong Dollars or US Dollars or Renminbi is drawn on the Registration Bank specified opposite	CMB Wing Lung Bank Limited shall pay all subscription fees and administration fees	
Bank-Cert (Corporate)	The Hongkong and Shanghai Banking Corporation Limited	1 - 5 years	Creation of a digital signature by the Subscriber of the Bank-Cert on an e-cheque as the drawer which e-cheque for a sum in Hong Kong Dollars or US Dollars or Renminbi is drawn on the Registration Bank specified opposite	The Hongkong and Shanghai Banking Corporation Limited shall pay all subscription fees and administration fees	For handling suspension or revocation request from Subscribers, the Hongkong and Shanghai Banking Corporation Limited will, within five working days after the date of receipt, notify HKPost of the receipt of the request.
Bank-Cert (Corporate)	CMB Wing Lung Bank Limited*	1 - 5 years	Creation of a digital signature by the Subscriber of the Bank-Cert on an e-cheque as the drawer which e-cheque for a sum in Hong Kong Dollars or US Dollars or Renminbi is drawn on the Registration Bank specified opposite	CMB Wing Lung Bank Limited* shall pay all subscription fees and administration fees	

Bank-Cert Type	Name of Registration Bank	Certificate Validity	Designated Transaction	Subscription Fees	Remarks
Bank-Cert (Bank)	The Hongkong and Shanghai Banking Corporation Limited	1 - 5 years	As a Registration Bank: Creation of a digital signature by the bank specified opposite on an e-cheque which is to be drawn on such bank	The Hongkong and Shanghai Banking Corporation Limited shall pay all subscription fees and administration fees	
			As a Subscriber: Nil		
Bank-Cert (Bank)	CMB Wing Lung Bank Limited*	1 - 5 years	As a Registration Bank: Creation of a digital signature by the bank specified opposite on an e-cheque which is to be drawn on such bank	CMB Wing Lung Bank Limited shall pay all subscription fees and administration fees	
			As a Subscriber: Nil		

Note
* "Wing Lung Bank Limited" is renamed to "CMB Wing Lung Bank Limited" with effective from 1 October 2018.

Appendix F- Lifespan of CA root certificates

Name of the root certificate	Date of creation	Remarks
Hongkong Post Root CA 2	5 September 2015	This root CA commences to issue Sub CAs with effect from 5 September 2015.
Hongkong Post e-Cert CA 2 - 15	5 September 2015	This Sub CA commences to issue Bank-Cert to applicants with effect from 30 November 2015.