THE CERTIFICATION PRACTICE STATEMENT

OF

THE POSTMASTER GENERAL

As

A Recognized Certification Authority
under the Electronic Transactions Ordinance

for

Hongkong Post Bank-Cert

Date : 31 March 2010
OID : 1.3.6.1.4.1.16030.1.2.10

Table of Contents

PREAMBLE

The Electronic Transactions Ordinance (Cap 553) (the "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 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. The Postmaster General has decided so to perform his functions, and he is therefore referred for the purposes of this document as **HKPost**.

With the Hong Kong SAR Government's decision to outsource the HKPost CA operations, the Hong Kong SAR Government has, through an open tender exercise, awarded a contract ("Contract") to E-Mice Solutions (HK) Limited ("Contractor") on 27 October 2006 for operating and maintaining the systems and services of the HKPost CA as stipulated in this CPS for a period from 1 April 2007 to 31 March 2011. The period of the Contract has subsequently been extended to 31 March 2012. HKPost remains a recognized CA under Section 34 of the Ordinance and the Contractor 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 certificates issued under this CPS are Recognized Certificates and are referred to as "certificates" or "Bank-Certs" in this CPS.**

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 sub-contractors to carry out some or all of its operations.

It is expedient for HKPost to appoint Registration Authorities (RAs) as its agent to carry out certain of the functions of HKPost as a recognized CA as set out in this CPS. A list of Registration Authorities can be found in **Appendix E**. Via these Registration Authorities, HKPost issues two types of Bank-Cert; to individual persons ("Bank-Cert (Personal)") and to certain organisations and employees or members of such organisations ("Bank-Cert (Corporate)"). HKPost is responsible for the conduct of the RAs in carrying out the functions or providing the services of HKPost as its agents as a recognized CA in respect of the issuing and revocation of Bank-Certs.

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

Section 1 of this CPS contains an overview and contact details
Section 2 sets out the responsibilities and liabilities of the parties
Section 3 sets out application and identity confirmation procedures
Section 4 describes some of the operational requirements
Section 5 presents the security controls
Section 6 sets out how the public/Private Key pairs will be generated and controlled
Section 7 describes some of the technical requirements
Section 8 documents how this CPS will be administered
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 Authorities
Appendix F describes lifespan of CA root certificates

The Bank-Certs issued under this CPS are Recognized Certificates. Outside this CPS, HKPost has also issued a root certificate named "Hongkong Post Commercial 1" which is not a Recognized Certificate under the Ordinance. The certificates issued by this root certificate are also not Recognized Certificates under the Ordinance. HKPost accepts no responsibility for any loss or damage to any person who relies upon these certificates which are not recognized under the Ordinance. The practices and standards as published in this CPS are also not applicable to such certificates which are not recognized under the Ordinance. The words "Hongkong Post Commercial 1" will be displayed in the "Issuer" field of such non-recognized certificates. Information of the root certificate "Hongkong Post Commercial 1" can be found in HKPost web site at http://www.hongkongpost.gov.hk/.

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") "1.3.6.1.4.1.16030.1.2.10" (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 each Relying Party's particular PKI application.

Under the Ordinance, HKPost is a recognized CA. HKPost has designated the Bank-Certs issued under this CPS as Recognized Certificates. This means for both Subscribers and Relying Parties, that HKPost has a legal obligation under the Ordinance to use a Trustworthy System for the issuance, revocation or suspension, and publication in a publicly available Repository of recognized and accepted digital certificates, including Bank-Certs. This also means that the certificates, such as Bank-Certs, that HKPost designates as Recognized Certificates are Recognized Certificates and, as such, have characteristics of accuracy and contain representations of fact which are defined in law by the Ordinance, including a representation (as further defined below) that such certificates have been issued in accordance with this CPS. The fact that HKPost has appointed Bank-Cert Registration Authorities as its agents does not diminish HKPost's obligation to use a Trustworthy System, nor does it alter the characteristics that Bank-Certs have as Recognized Certificates.

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 and assumes the obligations of a CA. HKPost is the only CA authorised to issue certificates under this CPS (see Section 2.1.1).

1.2.1.1 Representations by HKPost
By issuing a certificate that refers to this CPS, HKPost represents to Relying Parties who act in accordance with Section 2.1.5 and other relevant sections of this CPS, that HKPost has issued the certificate in accordance with this CPS. By publishing a certificate that refers to this CPS, HKPost represents to Relying Parties who act in accordance with Sections 2.1.5 and other relevant sections of this CPS, that HKPost has issued the certificate to the Subscriber identified in it.

1.2.1.2 Effect
HKPost publishes recognized certificates that are accepted by and issued to its Subscribers in a Repository. (See Section 2.5)

1.2.1.3 HKPost's Right to Subcontract
HKPost may further subcontract its obligations for performing some or all of the functions required by this CPS and the Subscriber Agreements provided that the subcontractor agrees to

Hongkong Post **e-Cert**
香港郵政電子核證

undertake to perform those functions and enters into a contract with HKPost to perform the services. In the event that such sub-contracting occurs, HKPost shall remain liable for the performance of the CPS and the Subscriber Agreements as if such sub-contracting had not occurred.

1.2.2 End Entities

Under this CPS there are two types of end entities, Subscribers and Relying Parties. A Subscriber is the "Subscriber" or "Subscriber Organisation" referred to in **Appendix A**. Relying Parties are entities that have relied on any class or category of certificate issued by HKPost, including but not limited to Bank-Cert, for use in a transaction. For the avoidance of doubt, Relying Parties should not rely on the RA. **Bank-Certs are issued via the RA as the agent of HKPost and consequently RAs do not owe a duty of care and are not responsible to the Relying Parties in anyway for the issue of Bank-Certs** (see also Section 2.1.2). Applicants or Subscribers who rely on a certificate, including a Bank-Cert, of another Subscriber, for use in a transaction will be Relying Parties in respect of such a certificate. **NOTE TO RELYING PARTIES: The Bank-Certs may not be issued to minors (see Appendix E).**

1.2.2.1 Warranties and Representations by Subscribers

Each Applicant (represented by Authorised Representative in the case of applying for a Bank-Cert (Corporate) certificate) must sign, or confirm his/her acceptance of, an agreement (in the terms specified in this CPS) which includes a term by which the Applicant agrees that by accepting a certificate issued under this CPS, the Applicant warrants (promises) to HKPost and represents to all other relevant parties (and in particular Relying Parties) that during the operational period of the certificate the following facts are and will remain true:

a)   No person other than the Subscriber of Bank-Cert (Personal) certificate and the Authorised User of Bank-Cert (Corporate) certificate has had access to the Subscriber's Private Key;

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

c)   All Information and representations made by the Subscriber included in the certificate are true;

d)   The certificate will be used exclusively for authorised and legal purposes consistent with the Bank-Cert CPS;

e)   All Information supplied in the certificate 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 third party; and

f)   Bank-Cert (Corporate) certificates are to be used only by the Authorised Users and for the Authorised Applications stipulated in Section 1.2.3.2 below.

1.2.3 Classes of Subscribers

HKPost issues certificates under this CPS only to Applicants whose application for a certificate has been approved and who have signed or confirmed their acceptance of a Subscriber Agreement in the appropriate form. Two classes of Bank-Certs may be issued under this CPS, but each RA can decide and agree with HKPost whether it will accept applications and be identified in certificates for both classes, or only one, and if one, which one.

For Bank-Cert (Corporate) certificates, only the Subscriber Organisation is required to become Subscribers under this CPS.

1.2.3.1 Bank-Cert (Personal) certificates

A Bank-Cert (Personal) certificate is issued to individuals who have a Hong Kong identity card and who are 18 or over. These certificates may be used to perform commercial operations.

1.2.3.2 Bank-Cert (Corporate) certificates

A Bank-Cert (Corporate) certificate is issued to organisations that hold a valid business registration certificate issued by the Government of the Hong Kong SAR and statutory bodies of Hong Kong whose existence is recognized by the laws of Hong Kong (a "Subscriber

Hongkong Post **e-Cert**
香港郵政電子核證

Organisation"); and identifies a members or employee of a Subscriber Organisation whom that Subscriber Organisation has duly authorised to use the Private Key of that Bank-Cert (Corporate) (an "Authorised User").

Bank-Cert (Corporate) certificates issued via a particular RA can only be used by Authorised Users in respect of the services or systems set out against the name of that RA in **Appendix E** (the "Authorised Applications").

1.2.4 Certificate Lifespan

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

Certificates issued under this CPS may have different lifespans depending upon which RA has acted in connection with which certificate. HKPost will agree with the RA the length of the validity to Bank-Certs in relation to which that RA will act. The lifespan of certificates is set out in **Appendix E. (See Section 3.2 for Certificate Renewal).**

1.2.5 Application at HKPost's Approved Premises

All first applications and applications of a new Bank-Cert following the revocation or expiration of Bank-Cert will require the Applicants to submit their applications as described in section 3 and 4 of this CPS.

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@hongkongpost.gov.hk

1.4 Complaints Handling Procedures

HKPost will handle all written and verbal complaints expeditiously. A full reply will be given to the complainant within 10 days. In the cases where full replies cannot be issued within 10 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 Obligations

HKPost's obligations to Subscribers are defined and limited by this CPS and by the terms of the contracts with Subscribers in the form of a Subscriber Agreement. This is so whether the Subscriber is also a Relying Party in relation to a certificate of another Subscriber. In relation to Relying Parties who are not Subscribers, this CPS gives them notice that HKPost undertakes only to exercise reasonable care and skill to avoid causing certain categories of loss and damage to Relying Parties in issuing, suspending or revoking and publishing certificates in conformity with the Ordinance and the CPS, and places a monetary limit in respect of such liability as it may have as set out in below and in the certificates issued.

2.1.1 CA Obligations

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. In accordance with this CPS, HKPost has the obligation to:

a)   issue and publish certificates in a timely manner (see Section 2.5);
b)   notify Applicants approval or rejection of their applications (see Section 4.1);
c)   suspend or revoke certificates and publish Certificate Revocation Lists in a timely manner (see Section 4.4); and
d)   notify Subscribers of the suspension or revocation of their certificates (see Section 4.4.).

2.1.2 RA Obligations and Liability

Registration Authorities are responsible only to HKPost under the terms of the agreement (the "RA Agreement") under which they are appointed by HKPost as its agents to carry out on HKPost's behalf certain of HKPost's obligations as detailed in this CPS. RAs, on behalf of HKPost, collect and keep documents and Information supplied under the terms of the CPS and Subscriber Agreements. HKPost is and remains responsible for the activities of its Registration Authorities in the performance or purported performance by them of the functions, power, rights and duties of HKPost.

RAs shall not become parties to any Subscriber Agreement, nor shall they accept any duty of care to Subscribers or Relying Parties, in connection with the issue, revocation, suspension or publication of Bank-Certs, nor in relation to the collection and keeping of documents or Information. RAs only carry out on HKPost's behalf HKPost's obligations and duties in these matters. RAs have the authority to act on behalf of HKPost to enforce the terms of the Subscriber Agreements (unless and until that authority is withdrawn and Subscribers duly notified of any such withdrawal). **RAs shall not be liable in any circumstances to Subscribers or Relying Parties in any way connected either with the performance of a Subscriber Agreement or any certificate issued by RAs on behalf of HKPost as a CA.**

2.1.3 Contractor Obligations

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 set up, modify, provide, supply, deliver, operate, administer, promote and maintain the HKPost CA systems and services as stipulated in this CPS. HKPost is and remains responsible for the activities of the Contractor in the performance or purported performance by the Contractor of the functions, power, rights and duties of HKPost.

2.1.4 Subscriber Obligations

Subscribers are responsible for:
   a) Agreeing that the key pair is generated by HKPost in a Trustworthy System and environment within HKPost's premises on behalf of the Subscriber.
   b) Completing the application procedures properly and signing, or confirming acceptance of, a Subscriber Agreement (by the Authorised Representative in the case of applying

Bank-Cert (Corporate) certificate) in the appropriate form and performing the obligations placed upon them by that Agreement, and ensuring accuracy of representations in certificate application.

c) Accurately following the procedures specified in this CPS as to the completion of certificates.

d) Acknowledging that they are undertaking an obligation to protect the confidentiality (i.e. keep it secret) and the integrity of their Private Key using reasonable precautions to prevent its loss, disclosure, or unauthorised use, and that they are responsible for any consequences under any circumstances for the compromise of the Private Key.

e) Reporting any loss or compromise of their Private Key immediately to the RA identified in the relevant certificate upon discovery of the loss or compromise (a compromise is a security violation in which Information is exposed to potential unauthorised access, such that unauthorised disclosure, alteration, or use of the Information may have occurred).

f) Notifying the RA 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 User.

g) Notifying the RA identified in the relevant certificate immediately from time to time of any change in the appointment and information of the Authorised Representative in the case of Bank-Cert (Corporate) certificates.

h) Notifying the RA identified in the relevant certificate immediately of any fact which may give rise to HKPost, upon the grounds set out in Section 4 below, having the right to revoke the certificate for which that Subscriber is responsible.

i) Agreeing that by having been issued or accepting a certificate they warrant (promise) to HKPost and represent to all Relying Parties that during the operational period of the certificate, the facts stated in Section 1.2.2.1 above are and will remain true.

j) Not using a certificate in a transaction on becoming aware of any ground upon which HKPost or the RA identified on the relevant certificate, on HKPost's behalf, could revoke it under the terms of the CPS, or after the Subscriber has made a revocation request or been notified by the RA of the RA's intention (acting on behalf of HKPost) to suspend or revoke the certificate under the terms of this CPS.

k) Upon becoming so aware of any ground upon which the RA could revoke the certificate, or upon the Subscriber making a revocation request or upon being notified by the RA of its intention to revoke the certificate as referred to in g) above, 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 revoked 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.

l) In the case of Bank-Cert (Corporate) certificates using these for Authorised Applications only.

m) Acknowledging that by submitting a Bank-Cert application form, they authorize the publication of the Bank-Cert to any other person or in the Repository.

2.1.4.1 Subscriber's Liability
Each Subscriber acknowledges that if they do not discharge their responsibilities as set out above properly or at all, each Subscriber may become liable under the Subscriber Agreements and/or in law to pay HKPost and/or, under the law, other persons (including Relying Parties) damages in respect of liabilities or loss and damage they may incur or suffer in consequence.

2.1.5 Relying Party Obligations
Relying Parties relying upon Bank-Cert certificates are responsible for:

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 certificate determining that the use of the certificate is appropriate for its purposes under this CPS while the RA identified in the Certificate (see **Appendix E**) does not undertake any duty of care to Relying Parties at all.

c) Checking the status of the certificate on the certificate revocation list prior to reliance.

d) Performing all appropriate certificate path validation procedures.

2.2 Further Provisions

Obligations of HKPost to Subscribers and Relying Parties

2.2.1 Reasonable Skill and Care

HKPost undertakes to each Subscriber and to each Relying Party that a reasonable degree of skill and care will be exercised by HKPost, by the Contractor or by a RA when acting on its behalf in performing the obligations and exercising the rights it has as a CA set out in this CPS. **HKPost does not undertake any absolute obligations to the Subscriber(s) or Relying Parties. It does not warrant that the services it provides under this CPS by itself, by the Contractor or by a RA or otherwise howsoever will be uninterrupted or error free or of a higher or different standard than that which should be achieved by the exercise by HKPost, or the officers, employees or agents of Hong Kong Post Office of a reasonable degree and skill and care.**

The implications of this are that, if, despite the exercise of a reasonable degree of skill and care by HKPost, by the Contractor or by a RA acting on behalf of HKPost, in carrying out this contract and in exercising its rights and discharging its obligations under the CPS, a Subscriber, either as a Subscriber or Relying Party as defined in this CPS, or a Relying Party who is not a Subscriber suffers any liability, loss or damage of whatsoever nature arising out of or in connection with the PKI system as described in this CPS, including loss and damage consequent upon reasonable reliance upon a certificate of another Subscriber, each Subscriber agrees and each Relying Party must accept that HKPost, the Hong Kong Post Office, the Contractor and any RA are under no liability of any kind in respect of such liability, loss or damage.

This means, for example, that provided that the HKPost, the Contractor or a RA acting on HKPost's behalf has exercised a reasonable degree of skill and care, HKPost, Hong Kong Post Office, the Contractor and any such RA will not be liable for any loss to a Subscriber or Relying Party caused by his reliance upon a false or forged Digital Signature supported by another Subscriber's Bank-Cert issued by HKPost.

This means, also, that, provided HKPost (by the Hong Kong Post Office, the Contractor or a RA acting on HKPost's behalf) has exercised a reasonable degree of skill and care to avoid and/or mitigate the effects of matters beyond its control, neither HKPost, the Hong Kong Post Office, the Contractor nor any such RA is liable for the adverse effects to Subscribers or Relying Parties of any matters outside HKPost's control whatsoever, including (without limitation) the availability of the Internet, or telecommunications or other infrastructure systems or the adverse effects of the acts of God, war, military operations, national emergency, epidemic, fire, flood, earthquake, strike or riots or the negligence or deliberate wrongful conduct of other Subscribers or other third parties.

2.2.2 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 to Relying Parties and likewise gives to Relying Parties no warranty 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 to Relying Parties. HKPost agrees to transfer those articles into possession of Subscribers for the limited purposes set out in this CPS. Nonetheless HKPost will exercise reasonable care to see that the same is fit for the purposes of completing and accepting a certificate as set out in this CPS, and if it is not, then HKPost's liability shall be as set out in sections 2.2.3 - 2.2.4 below. In addition, the articles

Hongkong Post e-Cert
香港郵政電子核證

transferred from HKPost may contain other material not relevant to the completion and acceptance of a Bank-Cert and if it does, the legal position in relation to such material is not governed by the CPS or the Subscriber Agreement, but by separate terms and conditions that will be referred to in the terms and conditions enclosed in the articles.

2.2.3 Limitation of Liability

2.2.3.1 Reasonableness of Limitations
Each Subscriber and Relying Party must agree that it is reasonable for HKPost to limit its liabilities as set out in the Subscriber Agreement and in this CPS.

2.2.3.2 Limitation on Types of Recoverable Loss
In the event of HKPost's breach of :-

a)   the Subscriber Agreements; or
b)   any duty of care, and in particular its duty under the Subscriber Agreements to exercise reasonable skill and care and/or duties that may arise to a Subscriber or Relying Party when any certificate issued by or on behalf of HKPost under the PKI is relied upon or used by a Subscriber or Relying Party or anyone else or otherwise howsoever,

whether a Subscriber or Relying Party suffers loss and damage as a Subscriber or as a Relying Party as defined by the CPS or otherwise howsoever, **HKPost shall not be liable for any damages or other relief in respect of :-**

a)   **any direct or indirect loss of profits or revenue, loss or injury to reputation or goodwill, loss of any opportunity or chance, loss of projects, or the loss or loss of use of any data, equipment or software; or**
b)   **for any indirect, consequential or incidental loss or damage even if, in respect of the latter, HKPost has been advised of the likelihood of such loss or damage in advance**.

2.2.3.3 HK$200,000 Limit
Subject to the exceptions that appear below, in the event of HKPost's breach of:-

a)   **the Subscriber Agreement and provision of this CPS; or**
b)   **any duty of care, and in particular, of any duty under the Subscriber Agreements, under this CPS or in law to exercise reasonable skill and care and/or breach of any duties that may arise to a Subscriber or Relying Party when any certificate issued by HKPost under the Public Key infrastructure initiative is relied upon or used by a Subscriber or Relying Party or anyone else or otherwise howsoever, whether a Subscriber or Relying Party suffers loss and damage as a Subscriber or as a Relying Party as defined by the CPS or otherwise howsoever;**

the liability of HKPost to any Subscriber and any Relying Party, whether as Subscriber or Relying Party as defined by the CPS or in any other capacity at all, is limited to, and shall not under any circumstances exceed, HK $200,000 in respect of one Bank-Cert (Personal) certificate or one Bank-Cert (Corporate) certificate.

2.2.3.4 Time Limit For Making Claims
Any Subscriber or Relying Party 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 HKPost Bank-Cert must do so within one year of the date upon which that Subscriber or Relying Party 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, they 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.

2.2.3.5 Hong Kong Post Office, the Contractor, RAs and their Personnel

Hongkong Post e-Cert
香港郵政電子核證

None of the Hong Kong Post Office, the Contractor nor any RA nor any officer or employee or other agent of the Hong Kong Post Office, the Contractor or any RA is to be a party to the Subscriber Agreements, and the Subscriber and Relying Parties must acknowledge to HKPost that, as far as the Subscriber and Relying Parties are aware, none of the Hong Kong Post Office, the Contractor nor any RA nor any of their officers, employees or agents voluntarily accepts or will accept any personal responsibility or duty of care to the Subscriber 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 and Relying Party accepts and will continue to accept that and undertakes to HKPost not to sue or seek any form of recovery or redress by other legal means whatsoever from any of the foregoing 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.

2.2.3.6 Liability For Wilful Misconduct, Personal Injury or Death

Any liability for fraud or wilful misconduct, personal injury and death is not within the scope of any limitation or exclusionary provision or notice of this CPS, any Subscriber Agreement or certificate issued by HKPost and is not limited or excluded by any such provision or notice.

2.2.3.7 Certificate Notices, Limitations and Reliance Limit

Bank-Certs issued by HKPost shall be deemed to have contained the following Reliance Limit and/or limitation of liability notice:

> *"The Postmaster General acting by the officers of the Hong Kong Post Office and the Contractor has issued this certificate as a recognized CA under the Electronic Transactions Ordinance upon the terms and conditions set out in the Postmaster General's Certification Practice Statement (CPS) that applies to this certificate.*
>
> *Accordingly, any person, before relying upon this certificate should read the CPS that applies to Bank-Certs which may be read on the HKPost CA web site at www.hongkongpost.gov.hk and also at the premises and on the web site of the Registration Authority identified in this certificate (please refer to **Appendix E**) acting on behalf of HKPost in connection with this certificate. The laws of Hong Kong SAR apply to this certificate and Relying Parties must submit any dispute or issue arising as a result of their reliance upon this certificate to the non-exclusive jurisdiction of the Courts of Hong Kong SAR.*
>
> *If you, as a Relying Party, do not accept the terms and conditions upon which this certificate is issued, then do not rely upon it.*
>
> *The Postmaster General (by the Hong Kong Post Office, the Contractor, and their respective officers, employees and agents including, without limitation, the Registration Authority) issues this certificate without undertaking any responsibility or duty of care to Relying Parties save as set out in the CPS.*
>
> *Relying Parties, before relying upon this certificate are responsible for:-*
> a) *Relying on it only when reliance is reasonable and in good faith in the light of all the circumstances known to the Relying Party at the time of reliance;*
> b) *Before relying upon this certificate, determining that the use of the certificate is appropriate for its purposes under the CPS;*
> c) *Checking the status of this certificate on the certificate revocation list prior to reliance; and*
> d) *Performing all appropriate certificate path validation procedures.*

Certification Practice Statement
Hongkong Post Bank-Cert
31 March 2010
OID : 1.3.6.1.4.1.16030.1.2.10

13

Hongkong Post e-Cert
香港郵政電子核證

If, despite the exercise of reasonable skill and care by the Postmaster General, the Hong Kong Post Office, the Contractor, any Registration Authority identified in this certificate and their respective officers, employees or agents, this certificate is in any way inaccurate or misleading, the Postmaster General, Hong Kong Post Office, the Contractor, any Registration Authority identified in this certificate and their respective officers, employees or agents, accept no responsibility for any loss or damage to the Relying Parties and the applicable Reliance Limit that applies to this certificate under the Ordinance in these circumstances is HK$0.

If this certificate is in any way inaccurate or misleading and this is the result of the negligence of the Postmaster General, Hong Kong Post Office, the Contractor, any Registration Authority identified in this certificate or their respective officers, employees or agents, then the Postmaster General will pay a Relying Party up to HK$200,000 in respect of proved loss caused by reasonable reliance upon such inaccurate or misleading matters in this certificate where such losses are not and do not include (1) any direct or indirect loss of profits or revenue, loss or injury to reputation or goodwill, loss of any opportunity or chance, loss of projects, or the loss or loss of use of any data, equipment or software or (2) any indirect, consequential or incidental loss or damage even if, in respect of the latter, HKPost has been advised of the likelihood of such loss or damage in advance. The applicable Reliance Limit that applies to this certificate under the Ordinance in these circumstances is HK$200,000 and in all cases in relation to categories of loss (1) and (2), is HK$0.

None of the Hong Kong Post Office, the Contractor, any Registration Authority identified in this certificate nor any of their respective officers, employees or agents undertakes any duty of care to Relying Parties in any circumstances in relation to this certificate.

<u>*Time Limit For Making Claims*</u>
Any Relying Party who wishes to make any legal claim upon the Postmaster General arising out of or in any way connected with the issuance, suspension, revocation or publication of this Bank-Cert must do so within one year of the date upon which that Relying Party 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, they 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.

If this certificate contains any intentional or reckless misrepresentation by the Postmaster General, the Hong Kong Post Office, any Registration Authority identified in this certificate and their officers, employees or agents, this certificate does not impose any limit upon their liability to Relying Parties who suffer loss in consequence of reasonable reliance upon such misrepresentations in this certificate.

The limits of liability contained herein do not apply in the (unlikely) event of liability for personal injury or death".

2.2.4 HKPost's Liability for Received but Defective Certificates

Notwithstanding the limitation of liability set out above, if, after receiving the certificate, a Subscriber finds that, in respect of Bank-Cert (Personal) certificates or Bank-Cert (Corporate) certificates, because of any error in the Private Key or Public Key of the certificate, no transactions contemplated by the PKI can be completed properly or at all, and that Subscriber notifies the RA identified in the Certificate 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 by the RA identified in the Certificate, on being satisfied of the existence of any such error, will refund the fee. If the Subscriber waits longer than 3 months after receiving the certificate before notifying the RA identified in the Certificate of any such error, the fee will not be refunded as of right, but only at the discretion of HKPost or of the RA identified in the certificate on HKPost's behalf.

2.2.5 Assignment by Subscriber
Subscribers may not assign their rights under Subscriber Agreements or certificates. Any attempted assignment will be void.

2.2.6 Authority to Make Representations
Except expressly authorised by HKPost, none of the Contractor, any RA, agent or employee of the Hong Kong Post Office, the Contractor or of any RA has authority to make any representations on behalf of HKPost as to the meaning or interpretation of this CPS.

2.2.7 Variation
HKPost has the right to vary this CPS without notice *(See Section 8)*. Subscriber Agreements cannot be varied, amended or changed except to comply with a variation or change in this CPS or with the express written consent of the Postmaster General.

2.2.8 Retention of Title
The physical, copyright, and intellectual property rights to all Information on the certificate issued under this CPS are and will remain vested in HKPost.

2.2.9 Conflict of Provisions
In the event of a conflict between this CPS and the Subscriber Agreement, other rules, guidelines, or contracts, the Subscriber and Relying Parties shall be bound by the provisions of this CPS, except to the extent that the provisions are prohibited by law.

2.2.10 Fiduciary Relationships
None of HKPost, the Contractor nor any RA acting on behalf of HKPost is an agent, fiduciary, trustee or other representative of the Subscribers or Relying Parties at any time. Subscribers and Relying Parties have no authority to bind HKPost, the Contractor or any RA acting on HKPost's behalf, by contract or otherwise, to any obligation as an agent, fiduciary, trustee or other representative of the Subscribers or Relying Parties.

2.2.11 Cross Certification
HKPost reserves the right in all instances to define and determine suitable grounds for cross-certification with another CA.

2.2.12 Financial Responsibility
An insurance policy is in place to cover the liabilities and claims against Reliance Limit on the certificates.

2.3 Interpretation and Enforcement (Governing Law)

2.3.1 Governing Law
The laws of Hong Kong SAR govern this CPS. Subscribers and Relying Parties agree to submit to the non-exclusive jurisdiction of the Courts of Hong Kong SAR.

2.3.2 Severability, Survival, Merger, and Notice
If any provision of this CPS is declared or found to be illegal, unenforceable, or void, then any offending words in it will be deleted to the extent necessary to make it legal and enforceable while preserving its intent. The unenforceability of any provision of this CPS will not impair the enforceability of any other provision of this CPS.

2.3.3 Dispute Resolution Procedures
The decisions of HKPost pertaining to matters within the scope of this CPS are final. Any

claims should be submitted to HKPost at the following address:

Hongkong Post Certification Authority
Kowloon East Post Office Box 68777
Email: enquiry@hongkongpost.gov.hk

2.3.4 Interpretation

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

2.4 Subscription Fees

For details of the fees charged in respect of Bank-Certs, please see **Appendix E** under the heading of the relevant RA. HKPost reserves its absolute right to review and determine the subscription fee and administration fee from time to time and will notify the Subscribers and the public at the HKPost web site http://www.hongkongpost.gov.hk. Under the terms of the Contract between HKPost and the Contractor, the Contractor is entitled to receive subscription and renewal fees from Bank-Cert subscribers.

2.5 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, the HKPost Public Key, a copy of this CPS, and other Information related to Bank-Cert certificates which reference this CPS. The Repository is available on a substantially 24 hours per day, 7 days per week basis, subject to scheduled maintenance of up to 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 URL as follows:-

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

2.5.1 Certificate Repository Controls

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

2.5.2 Certificate Repository Access Requirements

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

2.5.3 Certificate Repository Update Cycle

The Repository is updated promptly after each certificate is accepted by and issued to the Subscriber and any other applicable events such as revocation of certificates or other CA disclosure records.

2.5.4 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.

2.6 Compliance Assessment

Compliance assessments conducted on the HKPost's system of issuing, revoking or suspending and publishing Bank-Certs 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.

2.7 Confidentiality

HKPost will ensure that the restrictions in this subsection will be adhered to by itself and any persons of HKPost, the Contractor, RAs and any HKPost subcontractors who have access to any record, book, register, correspondence, Information, document or other material in performing tasks related to HKPost's system of issuing, revoking or suspending and publishing Bank-Certs shall not disclose or permit or suffer to be disclosed any information relating to another person as contained in such record, book, register, correspondence, Information, document or other material to any other person. Information about Subscribers that is submitted as part of an application for a Bank-Cert certificate under this CPS will be used only for the purposes collected and is kept confidential except to the extent necessary for HKPost or the Contractor to perform HKPost's obligations under this CPS. Such Information will not be released without the prior consent of the Subscriber except when required by a court-issued subpoena or order, or when otherwise required by the laws of Hong Kong SAR. HKPost is specifically precluded from releasing lists of Subscribers or Subscriber Information (except for compiled data which is not traceable to an individual Subscriber in accordance with the laws of Hong Kong SAR) unless required by a court-issued subpoena or order, or when otherwise required by the laws of Hong Kong SAR.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Application

In respect of Bank-Cert (Personal) certificate applications, each Applicant must appear in person at the premises of a RA, or premises of other organisations designated by HKPost, and present proof of identity as described in section 3.1.9.

In respect of Bank-Cert (Corporate) certificate applications, the Authorised Representative must appear in person at the premises of a RA, or premises of other organisations designated by HKPost, and present proof of identity as described in section 3.1.8. Attendance of the Authorised Users to be named in Bank-Cert (Corporate) certificates is not required.

All Applicants for a HKPost Bank-Cert must submit a completed and signed application form to the RA identified in the application form. Bank-Cert (Corporate) certificate applications require the Authorised Representative of the organisation to complete and sign the application form and the Subscriber Organisation will become a Subscriber.   Following approval of the application by the RA identified in the application form on behalf of HKPost, HKPost prepares a Bank-Cert certificate and notifies the Applicant either directly or, at the Subscriber's choice, by the RA identified in the application form of how the certificate may be issued.

3.1.1 Types of Names

3.1.1.1 Bank-Cert (Personal) certificates
The Subscriber for a Bank-Cert (Personal) certificate is identified in the certificate with a Subject Name (referred to in **Appendix B**) consisting of the Subscriber's name as it appears on the Subscriber's HKID Card. The Subscriber's HKID Card number will be stored in the certificate as a hash value (see **Appendix B**).

3.1.1.2 Bank-Cert (Corporate) certificates
The Subscriber Organisation for a Bank-Cert (Corporate) certificate is identified in the certificate with a Subject Name (referred to in **Appendix B**) consisting of:
a)   The Authorised User's name as it appears on the Authorised User's HKID Card /or passport;
b)   The Subscriber Organisation's name as it is registered with the appropriate Hong Kong Government Department or registration agency; and
c)   The Subscriber Organisation's Hong Kong Company/Business Registration Number as it appears on their certificate of incorporation/business registration certificate.

3.1.1.3 The Authorised Representative
Although the Authorised Representative of the Subscriber Organisation is responsible for administering on behalf of the Organisation the application for a Bank-Cert (Corporate) certificate, that person will not be identified in the Bank-Cert (Corporate) certificate.

3.1.1.4 Organisation Names in Chinese Language
All Bank-Certs are issued in English language only. For organisations who subscribe to Bank-Cert and are companies with company names in the Chinese language only or who have provided their company's Chinese name only, their company names will not be displayed on the Bank-Cert.

3.1.2 Need for Names to be Meaningful
All names must be meaningful using commonly understood semantics to determine the identity of the Subscriber.

3.1.3 Rules for Interpreting Various Names
The types of names of the Subscriber (Subject Name) to be included in the Bank-Cert certificates are described in Section 3.1.1. **Appendix B** should be referred to for interpretation of the Subject Name of the Bank-Cert certificates.

3.1.4 Name Uniqueness

The Subject Name (referred to in Appendix B) shall be unambiguous and unique to a Subscriber. However, this CPS does not require that a specific component or element of a name be unique or unambiguous by itself.

3.1.5 Name Claim Dispute Resolution Procedure

The decisions of HKPost or a RA on its behalf in matters concerning name disputes are discretionary and final.

3.1.6 Infringement and Violation of Trademarks

Applicants and Subscribers warrant (promise) to HKPost and represent to RAs and Relying Parties 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 third party.

3.1.7 Method to Prove Possession of the Private Key

Subscribers will have their Private Key generated using HKPost's central key generation service. With central key generation service, HKPost will generate the key pair and certificate on behalf of the Subscriber in a Trustworthy System and environment within HKPost's premises to ensure that the Private Key is not tampered with. The Private Key together with the certificate will be stored on a floppy disk, e-Cert File Card or alternative storage medium and delivered to the Subscriber in a secure manner designated on the application form.   All Subscribers acknowledge that it is their sole responsibility to maintain the security of the Private Key related to the Public Key included in the Bank-Cert.

3.1.8 Authentication of Identity of Organisational Applicant

Applications for Bank-Cert (Corporate) 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.

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

a) an authorisation letter bearing the "For and on behalf of" chop and the authorised signature(s) of the organisation giving authority to the Authorised Representative to make the application and identify the Authorised Users to be identified in the Bank-Cert (Corporate) certificates;
b) photocopies of the HKID Cards or passports of all Authorised Users to be so identified. If Authorised Users are not Hong Kong citizen, photocopies of valid travel documents of Authorised Users are accepted;
c) documentation issued by the appropriate Hong Kong registration agency attesting to the existence of the organisation. The validity of the documentation should not expire within one month by the time the application is submitted.

3.1.9 Authentication of Identity of Personal Applicant

Confirmation of the identity of each individual Applicant of Bank-Cert (Personal) certificate will be accomplished through an in-person process that operates as follows:

Each Applicant for a certificate must appear at the premises of a RA and submit a completed and signed Bank-Cert application form and the Applicant's HKID Card. Personnel at the aforementioned premises will review and certify the application package, and forward the application to HKPost CA Centre for processing.

3.2 Certificate Renewal

The certificates can be renewed before expiry of their validity at the request of the Subscriber and the discretion of HKPost. The RA identified in the certificate will issue renewal notice in the form of emails or lettermails to the Subscribers prior to the expiry of the certificates.

Hongkong Post **e-Cert**
香港郵政電子核證

3.2.1 Bank-Cert (Personal) certificates

To apply for renewal, the Subscriber is required to submit a completed and signed renewal application form to the RA with the appropriate fee. Upon renewal, a new key pair must be generated using HKPost's central key generation service. The responsibilities of the Subscribers and HKPost are the same in respect of the generation of the new keys as for the original ones, as set out above. The Certificate Renewal Form is available at the RA's web site (see Appendix E) or its premises. 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 CPS current at the date of renewal. In the case of any incompatibility, the terms of the current CPS will prevail. Applicants for renewal should read the terms of the CPS current at the date of renewal before submitting the renewal forms.

3.2.2 Bank-Cert (Corporate) certificates

There is no automatic renewal of a Bank-Cert (Corporate) certificate. The process of "Authentication of identity of Organisational Applicant" as described under Section 3.1.8 will be conducted as if a new application is received.

3.2.3 Validity Period of Renewed Bank-Cert

At the discretion of HKPost, the new Bank-Cert certificate to be issued to the Subscriber may be valid as from the date the new certificate is generated and expired on the date that is 3 years (for Bank-Cert (Personal) certificates) or 1 year (for Bank-Cert (Corporate) certificates) after the expiry date of the old certificate being renewed. Accordingly, the new Bank-Cert (Personal) certificate may have a validity period of more than 3 years but no more than 3 years and one month. The new Bank-Cert (Corporate) certificate may have a validity period of more than 1 year but no more than 1 year and one month.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1   Applicants for Bank-Certs under this CPS must complete and submit an application on a form created jointly by HKPost and the RA at the premises of a RA, a designated HKPost premises, or premises of other organisations designated by HKPost.

4.1.2   The Applicant may, at the time of submitting an application form, request an additional copy of the Bank-Cert to be stored in each of a recordable CD, an USB flash drive and/or a PKCS#11 compliant device that is provided by the Applicant. If HKPost considers the request acceptable, HKPost will store the additional copy of the Bank-Cert in each of the recordable CD, the USB flash drive and/or the PKCS#11 compliant device. In such case, the process in section 4.2 is also applicable to the additional copy of the Bank-Cert. In particular, the additional copy of the Bank-Cert will be protected by Bank-Cert PIN and delivered to the Applicant in a secure manner.

4.1.3   The documentation required for proving the identity of the Applicant is stipulated in Section 3.1.8 (Authentication of Identity of Organisational Applicant) and 3.1.9 (Authentication of Identity of Personal Applicant) of this CPS. The RA, on behalf of HKPost, will verify the identity of each Applicant and in the case of Bank-Cert (Corporate) certificates, the identity of the Authorised Representative. Upon satisfactory completion of the identity verification process, the Bank-Cert PIN envelope will be delivered to the Applicant or the Authorised Representative (for Bank-Cert (Corporate) certificate application).

4.1.4   The RA will notify the Applicant of the approval of an application and the Applicant may be requested to confirm in a printed form that all the Information and each representation made by the Applicant(s) to be included in the certificate is accurate and true. In the event HKPost/RA is not successful in validating an application in accordance with the requirements stipulated in this CPS, HKPost/RA will notify the Applicant the rejection of his/her application. All application Information transmitted electronically between the RA and HKPost must use a protocol prescribed by HKPost from time to time.

4.1.5   By submitting a Bank-Cert application form, the Applicant authorizes the publication of the Bank-Cert to any other person or in the Repository and thus accepts the Bank-Cert to be issued to the Applicant.

4.2 Certificate Issuance

4.2.1   The key pair generation and certificate creation are performed by HKPost. This is done in a Trustworthy System and environment within HKPost's premises to ensure that the Private Key will not be tampered with.

4.2.2   The Private Key and certificate, which are protected by a PIN, will then be stored on a floppy disk, e-Cert File Card or alternative storage medium as mentioned in Section 3.1.7. The floppy disk, e-Cert File Card or alternative storage medium, which will be sealed up in a tamper-proof envelope or other forms of containers, will then be delivered to the Applicant in a secure manner such as by registered mail.

4.2.3   The Applicant agree that it is fully accountable for the safe custody of the Private Key upon receipt of the floppy disk, e-Cert File Card or alternative storage medium and agree that they will be responsible for any consequences under any circumstances for the compromise of the Private Key.

4.2.4   All Private Keys stored in the HKPost system are in an encrypted form. Proper security controls are in place to guard against unauthorized access to and disclosure of the encrypted Private Keys. Upon completion of delivery of the Bank-Certs and Private Keys to the Applicants/Subscribers, the respective Private Keys will be purged from the HKPost system.

4.2.5   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 Publication of Bank-Cert

Under the Ordinance, HKPost's system will promptly publish the accepted and issued Bank-Cert in the Repository (see Section 2.5)

4.4 Certificate Revocation

4.4.1 Circumstances for Revocation

The compromise of a HKPost Private Key will result in prompt revocation of the certificates issued under that Private Key. Procedures stipulated in the business continuity plans will be exercised to facilitate rapid revocation of all Subscriber certificates in the event of compromise of the HKPost Private Keys (see Section 4.8.2).

Each Subscriber may make a request to revoke the certificate for which they are responsible under a Subscriber Agreement at any time for any reason by following the revocation procedure set out in this CPS.

Each Subscriber **MUST** apply to either HKPost directly or to the RA identified in the certificate for the revocation of the certificate in accordance with the revocation procedures in this CPS **immediately after the Subscriber's Private Key, or the media containing the Private Key corresponding to the Public Key contained in a Bank-Cert has been, or is suspected of having been, compromised (see also Section 2.1.4(h)).**

HKPost and the RA identified in the certificate, on behalf of HKPost, may suspend or revoke a certificate and will notify the Subscriber in writing of such suspension or revocation ("Notice of Revocation") in accordance with the procedures in the CPS whenever it:-

  a) knows or reasonably suspects that a Subscriber's Private Key has been compromised;
  b) knows or reasonably suspects that any details upon a certificate are not true or have become untrue or that the certificate is otherwise unreliable;
  c) determines that a certificate was not properly issued in accordance with the CPS;
  d) determines that the Subscriber had failed to meet any of the obligations set out in the CPS or the Subscriber Agreement;
  e) is required to do so by any regulation, or law applicable to the certificate;
  f) determines that the Subscriber has failed to pay the subscription fee; or
  g) knows or has reasonable cause to believe that the Subscriber whose details appear on the Bank-Cert (Personal) certificate:

      (i) Is dead or has died;
      (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.

  h) knows or has reasonable cause to believe that the Authorised User named in a Bank-Cert (Corporate) certificate has ceased to be a member or employee of the Subscriber Organisation; or
  i) knows or has reasonable cause to believe that the Subscriber whose details

appear on the Bank-Cert (Corporate) certificate:-

(i) The Subscriber is in liquidation, or a winding up order relating to the Subscriber has been made by any Court of competent jurisdiction;

(ii) The Subscriber 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 acted fraudulently, corruptly or dishonestly or committed an offence under the Ordinance; or

(iv) A receiver or administrator has been appointed over any part of the Subscriber's assets within 5 years preceding the date of revocation.

4.4.2 Revocation Request Procedure

A Subscriber, or the Authorised Representative of a Subscriber Organisation, may submit a certificate revocation request to HKPost through a designated web page on the HKPost web site at http://www.hongkongpost.gov.hk, by fax, letter mail, email or in-person. A Subscriber may alternatively submit a revocation request to the RA identified in the certificate by fax, letter mail, email or in-person, depending upon which of these methods the RA to be contacted can accept (see **Appendix E**), and the RA will forward such revocation requests to HKPost.

Based on the revocation request, HKPost will suspend the validity of the certificate. The certificate will be revoked, which terminates the validity of the certificate permanently, upon receipt of the final confirmation of revocation from the Subscriber or through the RA to which the request for revocation was first submitted. Such final confirmation of revocation can be an email digitally signed by the Subscriber's Private Key, an original letter signed by the Subscriber or a Request for Certificate Revocation Form signed by the Subscriber. If no final confirmation of revocation is received from the Subscriber, the validity of the certificate will remain suspended and will be included 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.hongkongpost.gov.hk or the RA's web site (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.

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.

Where a revocation request or final confirmation of revocation has been submitted to the RA identified in the certificate, that RA (as the agent of HKPost) will, within one working day of receipt, notify HKPost of the receipt of the same to enable HKPost to post the suspension or revocation to the Certificate Revocation List.

If the RA receives the revocation request or final confirmation on a day before a day which is not a business day upon which that RA operates, the RA will immediately notify Subscribers that they should send their request or final confirmation directly to HKPost.

Requests for revocation and confirmation of revocation can only be actioned by RA and HKPost within their usual business hours. For details of the RA's business hours for revocation please refer to Appendix E.

The business hours for revocation submitted by fax, letter mail, email or in-person are as follows:

Monday - Friday	09:00 am - 5:00 pm
Saturday	09:00 am - 12:00 noon

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

4.4.3 Service Pledge & Certificate Revocation List Update

a)   HKPost will exercise reasonable endeavours to ensure that within 2 working days of (1) receiving a revocation request or final confirmation of revocation from either the Subscriber directly or from the RA identified in the certificate or (2) in the absence of such a request, the decision by HKPost and/or the notification from a RA of a decision by that RA on HKPost's behalf, to suspend or revoke the certificate, the suspension or revocation is posted to 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 and are archived for 7 years.

For the avoidance of doubt, Sundays, public holidays and days on which a tropical cyclone and rainstorm warning signal is hoisted, are not working days for the purpose of this section 4.4.3(a).

The RA, on behalf of HKPost, or HKPost will exercise reasonable endeavours to send to relevant Subscribers a Notice of Revocation by email or by post within one week following the suspension or revocation.

b)   Subscribers must not use a certificate in a transaction on becoming aware of any ground upon which HKPost and/or the RA identified in the certificate could revoke it under the terms of the CPS and must not use it in a transaction after the Subscriber has made a revocation request or been notified of the intention of HKPost or of a RA on HKPost's behalf to suspend or revoke the certificate. HKPost and the RA shall be under no liability to Subscribers or Relying Parties in respect of any such transactions if, despite the foregoing, they do use the certificate in a transaction.

c)   Further, upon becoming so aware of any ground upon which HKPost and/or the RA identified in the certificate could revoke the certificate, or upon making a revocation request or upon being notified by HKPost or the RA of its intention to revoke the certificate, Subscribers must immediately notify Relying Parties in any transaction that remains to be completed at the time, that the certificate used in that transaction is liable to be revoked (either by HKPost, the RA or at the Subscriber's request) and state in clear terms that, as this is the case, the Relying Parties should not rely upon the certificate in respect of the transaction. HKPost and the RA shall be under no liability in respect of such transactions to Subscribers who fail to notify Relying Parties, and under no liability to Relying Parties who receive such a notification from Subscribers but complete the transaction despite such notification.

HKPost and the RA shall be under no liability to Relying Parties in respect of the transactions in the period between HKPost or the RA's decision to suspend or revoke a certificate (either in response to a request or otherwise) and the appearance of this Information on the Certificate Revocation List, unless HKPost or the RA on HKPost's behalf has failed to exercise reasonable skill and care and the Subscriber has failed to notify the Relying Party as required by these provisions. Any such liability is limited as set out elsewhere in this CPS. In no circumstances does the RA itself undertake a separate duty of care to Relying Parties (the RA is simply discharging HKPost's duty of

care), and accordingly, even if negligent, the RA itself cannot be held liable to Relying Parties.

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

e) HKPost's policy concerning the situation where a relying party is temporarily unable to obtain Information on revoked certificate is stipulated in Section 2.1.5 (Relying Parties Obligations) and Section 2.2.1 (Reasonable Skill and Care) of this CPS.

4.4.4 Effect of Revocation
Revocation terminates a certificate as of the time that HKPost posts the suspension/revocation status to the Certificate Revocation List.

4.5 Computer Security Audit Procedures

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

4.5.2 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.

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

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

4.5.5 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.

4.5.6 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.

4.5.7 Notification of Event-Causing Subject to HKPost
HKPost has an automated process in place to report critical audited events to the appropriate

Hongkong Post e-Cert
香港郵政電子核證

person or system.

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

4.6 Records Archival

4.6.1 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.

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

4.6.3 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.

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

4.6.5 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.

4.7 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 20 years. 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.hongkongpost.gov.hk for public access. The original root keys will be kept for a minimum period as specified in Section 4.6.2 for verification of any signatures generated by the original root keys.

4.8 Disaster Recovery and Key Compromise Plans

4.8.1 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

Hongkong Post **e-Cert**
香港郵政電子核證

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.

4.8.2 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 Officer and make public announcement if a HKPost Private Key for the issuance of Bank-Cert certificates under this CPS has been compromised. The compromise of an HKPost Private Key will result in prompt revocation of the certificates issued under that Private Key and the issuance of new and replacement certificates.

4.8.3 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.

4.9 CA Termination

In the event that HKPost ceases to operate as a CA, notification to the Government Chief Information Officer and 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 7 years after the date of service termination.

4.10 RA Termination

In the event that a RA ceases to be a RA and its authority to act on behalf of HKPost is withdrawn, HKPost or the RA concerned will notify Subscribers of certificates which identify that RA. Despite the termination of the RA's authority to further represent HKPost, the Bank-Certs will remain in effect in accordance with their terms until expiry (save that Subscribers must deal directly with HKPost rather than the former RA in matters connected with the Bank-Cert formerly handled by the RA) and, until expiry, the former RA must recognise the continuing validity of the Bank-Cert. The Bank-Certs identifying a RA whose authority to act on behalf of HKPost has been withdrawn cannot be renewed after expiry.

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 reasonable physical security. During construction of the site, HKPost took appropriate precautions to prepare the site for CA operations.

5.1.2 Access Controls
HKPost has implemented commercially reasonable physical security controls that limit access to the hardware and software (including the CA server, workstations, and any external cryptographic hardware modules or tokens 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 4.8.1)

5.1.8 Protection of Paper Documents
Paper documents including Subscriber Agreements and photocopies of identity confirmation documents are maintained by HKPost, the Contractor or RAs 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 RA acting on behalf of HKPost (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 and RAs
All documents and data transmitted between HKPost and RAs are delivered in a control and secure manner.

5.2.3 Annual Assessment
An annual audit is undertaken to confirm compliance with policy and procedural controls (see Section 2.6).

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 RAs 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 RAs 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 RAs have received the initial training needed to perform their duties. HKPost, the Contractor and RAs also provide ongoing training as necessary to enable their personnel to remain current in required skills.

5.3.4 Documentation Supplied To Personnel
HKPost personnel and those of the Contractor's and of RAs 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 and Applicants/Subscribers are generated through a procedure such that the Private Key cannot be accessed by anyone other than the authorised user of the key pair 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. In the case of central key generation by HKPost on behalf of the Applicants, the Applicants' Private Keys will be purged from the HKPost system upon completion of delivery of the Bank-Certs and Private Keys to the Applicants.

6.1.2 Subscriber Public Key Delivery
Key pairs Bank-Cert (Personal) and Bank-Cert (Corporate) certificates will be generated under the central key generation by HKPost on behalf of the Applicant/Subscriber.

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.hongkongpost.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 are 1024-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 (Personal) certificates and Bank-Cert (Corporate) certificates may be used for Digital Signatures and conducting enciphered electronic communications. 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 over-all key escrow process is planned for HKPost Private Keys and Subscribers' 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 public and Private Keys will be used for no more than 20 years. 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 4.6.

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 2.6.

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.hongkongpost.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.hongkongpost.gov.hk or RA website.

Appendix A - Glossary

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

"Accept", 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) authorize 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) authorize the publication of the certificate to any other person or in a repository; or
   (iii) otherwise demonstrate the approval of the certificate.

"Applicant" means a natural or legal person who applies for a Bank-Cert.

"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 Application" means, relation to an RA, a service or system, if any, set out against the name of that RA in column 5 of Appendix E in respect of which Bank-Cert (Corporate) certificates issued by that RA may be used.

"Authorised Representative" means the duly authorised representative of a Subscriber Organisation.

"Authorised User" means a member or employee of a Subscriber Organisation whom that Subscriber Organisation has duly authorised to use the Bank-Cert (Corporate) certificate issued to that Subscriber Organisation.

"Certificate" or "Bank-Cert" means a Record which:-
   a) is issued by a Certification Authority for the purpose of supporting a Digital Signature which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair;
   b) identifies the 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 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 a statement issued by a Certification Authority to specify the practices and standards that the Certification Authority employs in issuing certificates.

"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

Certification Practice Statement
Hongkong Post Bank-Cert
31 March 2010
OID : 1.3.6.1.4.1.16030.1.2.10

34

Hongkong Post **e-Cert**
香港郵政電子核證

time at which they were scheduled to expire.

"Contractor" means E-Mice Solutions (HK) Limited, being an agent of HKPost CA appointed pursuant to Section 3.2 of the COP for operating and maintaining the systems and services of the HKPost CA as stipulated in this CPS on behalf of HKPost for a period from 1 April 2007 to 31 March 2012.

"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 issued by the Government Chief Information Officer under Section 33 of the Ordinance.

"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-Cert File Card" means a smart card which is a storage medium for the Bank-Cert.

"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.

"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).

"Intermediary" in relation to a particular Electronic Record, means a person who on behalf of a person, sends, receives or stores that Electronic Record or provides other incidental services with respect to that Electronic Record.

"Issue" in relation to a certificate, means to:
(a)   create the certificate, and then notify the person named or identified in the certificate as the person to whom the certificate is issued of the information on the person as contained in the certificate; or
(b)   notify the person to be named or identified in the certificate as the person to whom the certificate is issued of the information on the person that is to be contained in the certificate, and then create the certificate,
and then make the certificate available for use by the person.

"Key Pair", in an asymmetric crypto system, 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.

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

"Originator" in relation to an Electronic Record, means a person, by whom, or on whose behalf, the Electronic Record is sent or generated but does not include an Intermediary.

"PKCS#11 compliant device" means a device, such as smart card, which is a storage medium of Bank-Cert and supports cryptographic functions, and also complies to the eleventh specification of the Public-Key Cryptography Standards (PKCS) published by RSA Laboratories, in respect of cryptographic token interface standard. Such device should also be certified with FIPS 140-2 Level 3 or above.

"Postmaster General" 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.

"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" 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 Authority" or **"RA"** means an organisation that has been appointed by HKPost to act on its behalf in carrying out certain of HKPost CA functions, and providing certain of HKPost CA services.

"Reliance Limit" means the monetary limit specified for reliance on a Recognized Certificate.

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

"Responsible Officer" in relation to a certification authority, means a person occupying a position of responsibility in relation to the activities of the certification authority relevant to the Ordinance.

"Sign" and **"Signature"** include any symbol executed or adopted, or any methodology or procedure employed or adopted, by a person with the intention of authenticating or approving a record.

"Sub CA" means the subordinate certification authority certificate which is issued by the Root CA "Hongkong Post Root CA 1" and is used to sign the Hongkong Post Recognized Certificates.

Certification Practice Statement
Hongkong Post Bank-Cert
31 March 2010
OID : 1.3.6.1.4.1.16030.1.2.10

36

Hongkong Post e-Cert
香港郵政電子核證

"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) holds a Private Key which corresponds to a Public Key listed in that Certificate.

"Subscriber Agreement" means an agreement which comprises the subscriber terms and conditions specified in the application form entered between the Subscriber and HKPost and the provisions in this CPS.

"Subscriber Organisation" means a Subscriber which is an organisation whose Authorised Representative has signed a Subscriber Agreement and to whom a Bank-Cert (Corporate) certificate has been issued in accordance with the eligibility criteria set out in 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.

For the purpose of the Electronic Transactions Ordinance, a Digital Signature is taken to be supported by a Certificate if the Digital Signature is verifiable with reference to the Public Key listed in a Certificate the Subscriber of which is the signer.

Hongkong Post e-Cert
香港郵政電子核證

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 1 - 10" under this CPS. For the format of Bank-Cert issued by the other Sub CA(s) of HKPost or issued under other CPS, please refer to the prevailing CPS in respect of the issuance date of the Bank-Cert or the OID as specified in the "Certificate Policies" of the Bank-Cert concerned.

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		sha1RSA
Issuer name		cn=Hongkong Post e-Cert CA 1 - 10, o=Hongkong Post, 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=[HKID name] [(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: 1024-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 1, o=Hongkong Post, c=HK
	Serial number	[Inherited from Issuer]
Key usage		Non-repudiation, Digital Signature, Key Encipherment **(This field will be set Critical.)**
Certificate policies		PolicyIdentifier = [OID] [(Note 6)] PolicyQualifierID = CPS Qualifier = www.hongkongpost.gov.hk
Subject alternative name	**DNS**	encrypted(HKID) [(Note 7)]
	rfc822	[Applicant's email address] [(Note 2)]
	1st Directory Name CN	[RA's reference information]
Issuer alternate name		Not used
Basic constraint	**Subject type**	End Entity
	Path length constraint	None
Extended key usage		Not used
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] [(Note 8)]
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 format: Surname (in capital) + Given name (e.g. CHAN Tai Man David).

2. Email address provided by Applicant (blank if null).

3. SRN: 10-digit Subscriber Reference Number

4. XXX is the name of Registration Authority 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 section 1.1 of this CPS for the OID of this CPS.

7. The Applicant's HKID number (**hkid_number** - including the check digit) will be stored in the certificate in the form of a hash value of the HKID number (**cert_hkid_hash**) which has been signed by the Private Key of the Applicant:-

   cert_hkid_hash = $SHA\text{-}1$ ($RSA_{privatekey,\ sha\text{-}1}$ (hkid_number))

   where the $SHA\text{-}1$ is a hash function and RSA is the signing function

   With Central Key Generation, hkid_number will be signed during the key generation process at HKPost premises and the CA system will create a hash of the signed HKID number - **$SHA\text{-}1$ ($RSA_{privatekey,\ sha\text{-}1}$ (hkid_number))**. The hash value will then be put into the designated extension field of the certificate being generated.

8. URL of CRL Distribution Point is http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL2.crl which is a partitioned CRL issued by the Sub CA "Hongkong Post e-Cert CA 1 - 10".

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		sha1RSA
Issuer name		cn=Hongkong Post e-Cert CA 1 - 10, o=Hongkong Post, 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 HKID name] (Note 1) e=[email address] (Note 2) ou=[SRN] (Note 3) ou=[BRN+CI/CR+Others] (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: 1024-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 1, o=Hongkong Post, c=HK
	Serial number	[Inherited from Issuer]
Key usage		Non-repudiation, Digital Signature, Key Encipherment **(This field will be set Critical.)**
Certificate policies		PolicyIdentifier = [OID] (Note 8) PolicyQualifierID = CPS Qualifier = www.hongkongpost.gov.hk
Subject alternative name	**DNS**	Not used
	rfc822	[Applicant's email address] (Note 2)
	1st Directory Name CN	[RA's reference information]
Issuer alternate name		Not used
Basic constraint	**Subject type**	End Entity
	Path length constraint	None
Extended key usage		Not used
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 9)
Netscape extension (Note 7)		
Netscape cert type		SSL Client, S/MIME
Netscape SSL server name		Not used
Netscape comment		Not used

Note

1. Authorised user name format: Surname (in capital) + Given name (e.g. CHAN Tai Man David).

2. Email address provided by Authorised User (blank if null)

3. SRN: 10-digit Subscriber Reference Number

4. Business Registration Certificate Number (BRN): a string of 16 digits/alphabets (the first 11 digits/alphabets represent the Business Registration Number) [filled with zeroes if BRN is not available], Certificate of Incorporation (CI)/ Certificate of Registration (CR): a string of 8 digits/alphabets [filled with zeroes if CI/CR is not available], a string of max. 30 digits/alphabets (blank if null). For HKSAR government departments, BRN and CI/CR are filled with zeroes, department name in abbreviation (e.g. HKPO for Hongkong Post) is placed in Others.

5. For organisations who subscribe to Bank-Cert and are companies with company names in the Chinese language only or who have provided their company's Chinese name only, their company names will not be included in this field (see section 3.1.1.4 of this CPS).

6. XXX is the name of Registration Authority 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. URL of CRL Distribution Point is http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL2.crl which is a partitioned CRL issued by the Sub CA "Hongkong Post e-Cert CA 1 - 10".

Appendix C - Hongkong Post Certificate Revocation Lists (CRLs)

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 1 - 10". The Sub CA "Hongkong Post e-Cert CA 1" ceased to issue Recognized Certificates with effect from 26 February 2010, but continues to update and publish CRLs until its expiry. Regarding the arrangement of updating and publishing as well as the format of the CRLs issued by the Sub CA "Hongkong Post e-Cert CA 1", please refer to the prevailing CPS in respect of the issuance date of the Bank-Cert or the OID as specified in the "Certificate Policies" field of the Bank-Cert concerned.

HKPost updates and publishes the following 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. The partitioned CRL for Bank-Cert (Personal) and Bank-Cert (Corporate) is available at :-

> http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL2.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 1 - 10". The Full CRL is available at :-

> http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL1.crl; or
> ldap://ldap1.hongkongpost.gov.hk (port 389, cn=Hongkong Post e-Cert CA 1 - 10 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.

Format of Partitioned and Full CRL issued by the Sub CA "Hongkong Post e-Cert CA 1 - 10" 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		sha1RSA		This field contains the algorithm identifier for the algorithm used to sign the CRL.
Issuer name		cn=Hongkong Post e-Cert CA 1 - 10, o=Hongkong Post, 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.
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 Fields	Sub-fields	Field Contents of Partitioned CRL	Field Contents of Full CRL	Remarks
Standard extension (Note 2)				
Authority key identifier	**Issuer**	cn=Hongkong Post Root CA 1 o=Hongkong Post 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.

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
Subscriber	Holders of valid HKID card who are 18 or above	Organisations that hold a valid business registration certificate issued by the Government of the Hong Kong SAR and statutory bodies of Hong Kong whose existence is recognized by the laws of Hong Kong
Certificate holders	Same as Subscriber	Authorised Users who are members or employees of the Organisation as the Subscriber
Reliance Limit	HK$200,000	HK$200,000
Recognized Certificate	Yes	Yes
Key pair size	1024-bit RSA	1024-bit RSA
Registration Authority	See **Appendix E**	See **Appendix E**
Key pair generation	By Hongkong Post on behalf of the Subscriber through the central key generation service	By Hongkong Post on behalf of the Subscriber through the central key generation service
Identity verification	Authentication of the Subscriber's identity	Authentication of the identity of the organization and its Authorised Representative
Usage of certificate	Digital Signature and Encryption	Digital Signature and Encryption
Subscriber's information included in the certificate	▪ English name as appeared on the HKID Card; ▪ HKID number encrypted as a hash value; ▪ Email address; and ▪ Subscriber Reference Number (SRN) generated by the HKPost system	▪ Subscriber Organisation's name ▪ Authorised User's name and email address; ▪ Subscriber Reference Number (SRN) generated by the HKPost system ▪ Subscriber Organisation's company/business registration information
Subscription fees and certificate validity	See **Appendix E**	See **Appendix E**

Certification Practice Statement
Hongkong Post Bank-Cert
31 March 2010
OID : 1.3.6.1.4.1.16030.1.2.10

44

Hongkong Post e-Cert
香港郵政電子核證

Appendix E - List of Hongkong Post Bank-Cert Registration Authorities

With effect from the date of this CPS, no Registration Authority for Hongkong Post Bank-Cert is appointed, and Hongkong Post Certification Authority ceases to issue Bank-Cert.

For Bank-Cert issued before the date of this CPS, relying parties should make reference to the corresponding CPS of the Bank-Cert.

Appendix F - Lifespan of CA root certificates

Name of the root certificate	Lifespan	Remarks
Hongkong Post Root CA 1	15 May 2003 – 15 May 2023	
Hongkong Post e-Cert CA 1	15 May 2003 – 15 May 2013	This Sub CA ceased to issue Bank-Cert with effect from 26 February 2010.
Hongkong Post e-Cert CA 1 - 10	9 January 2010 – 15 May 2023	This Sub CA commences to issue Bank-Cert to applicants with effect from 26 February 2010.