THE CERTIFICATION PRACTICE STATEMENT

OF

THE POSTMASTER GENERAL

As

A Recognized Certification Authority under the Electronic Transactions Ordinance

for

Hongkong Post e-Cert

Date : 30 January 2002

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 (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 identified for the purposes of this document as **HKPost**.

HKPost, as a recognized CA, is responsible under the Ordinance for the use of a trustworthy system for the issuance, withdrawal, and publication in a publicly available repository of recognized and accepted digital certificates for secure on-line identification. Such certificates are called “certificates” or “e-Certs”. HKPost issues certificates to individual persons ("e-Cert (Personal) certificates"), organisations ("e-Cert (Organisational) certificates") and to organisations that wish to have a certificate issued in a server name owned by that organisation ("e-Cert (Server) certificates"). HKPost also issues certificates ("e-Cert (Encipherment) certificates") to certain organisations for the purpose of conducting enciphered electronic communications.

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 e-Cert format
Appendix C contains a Hongkong Post e-Cert CRL format
Appendix D contains a summary of Hongkong Post e-Cert features

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, withdrawing and publishing certificates.

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.

Except in the case of e-Cert (Encipherment) certificates (see Section 1.2.3(d)), 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 accepting 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. 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, withdrawal, and publication in a publicly available repository of recognized and accepted digital certificates. This also means that the certificates 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.

A summary of the Hongkong Post e-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 2.1.3 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 2.1.3 and other relevant sections of this CPS, that HKPost has issued the certificate to the Subscriber identified in it.

1.2.1.2 Effect

The issuance of a certificate signed by HKPost and acceptance of the certificate by the Subscriber indicates the complete and final approval of that certificate. HKPost will promptly publish issued certificates in a repository. (See Section 2.5).

1.2.1.3 HKPost's Right to Subcontract

HKPost may, with consent of its Subscribers given in the Subscriber Agreement, 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 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. Subscribers are individuals or organisations who have procured the issuance of an e-Cert. Relying Parties are entities that have accepted an e-Cert for use in a transaction. Subscribers who accept an e-Cert of another Subscriber for use in a transaction will be Relying Parties in respect of such a certificate. **NOTE TO RELYING PARTIES : The HKPost's e-Cert system is not age restricted and minors may apply for and receive e-Certs. Relying Parties should not use an e-Cert as proof-of-age for an e-Cert Subscriber.**

1.2.2.1 Warranties and Representations by Subscribers

Each Subscriber must sign an agreement (in the terms specified in this CPS) which includes a term by which the Subscriber agrees that by accepting a certificate issued under this CPS, the Subscriber 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 the certificates and the authorised users of an e-Cert (Encipherment) 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 e-Cert (Personal) certificate, e-Cert (Organisational) certificate or e-Cert (Server) certificate, is the digital signature of the Subscriber.
c) An e-Cert (Encipherment) certificate is to be used only for the purposes stipulated in Section 1.2.3(d) below.
d) All information and representations made by the Subscriber included in the certificate are true.
e) The certificate will be used exclusively for authorised and legal purposes.
f) 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.

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 a Subscriber Agreement in the appropriate form. Four classes of e-Certs are issued under this CPS and the Subscriber Agreement.

a) **e-Cert (Personal) certificates**

The first class of certificate is issued to individuals who have a Hong Kong identity card. These certificates may be used to perform commercial operations. e-Cert (Personal) certificates may be issued to persons under 18 who have a Hong Kong identity card, but only if one of the parents (or the legal guardian) of such persons become party to the relevant Subscriber Agreement. e-Cert (Personal) certificates issued in respect of minors may carry special warnings to Relying Parties as under the law minors might not be bound by certain contracts.

b) **e-Cert (Organisational) certificates**

The second class of certificate is issued to Bureaux and Departments of the Government of Hong Kong SAR, 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; and identifies members or employees of organisations whom the organisation has determined should have a certificate indicating the connection of the member or employee to the organisation. These certificates may be used for the same purposes as e-Cert (Personal) certificates.

c) **e-Cert (Server) certificates**

The third class of certificate is issued to Bureaux and Departments of the Government of Hong Kong SAR, 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 SAR; and that wish to have a certificate issued in a server name owned by that organisation.

d) **e-Cert (Encipherment) certificates**

The fourth class of certificate is issued to Bureaux and Departments of the Government of Hong Kong SAR, organisations that hold a valid business registration certificate issued by the Government of Hong Kong SAR and statutory bodies of Hong Kong SAR whose existence is recognized by the laws of Hong Kong SAR. Such a certificate is designed to be used by such officers, members and employees of the Subscriber Organisation as that Organisation has authorised to use it ("the authorised users").

Certificates of this class are to be used only:

i) to send encrypted electronic messages to the Subscriber Organisation;
ii) to permit the Subscriber Organisation to decrypt messages; and
iii) to permit the Subscriber Organisation to acknowledge receipt of the encrypted message by sending an acknowledgement with a digital signature added to it to confirm the identity of the receiving Subscriber Organisation.

SUBSCRIBING ORGANISATIONS UNDERTAKE TO HKPOST NOT TO GIVE AUTHORITY TO THE AUTHORISED USERS TO USE A DIGITAL SIGNATURE OF THIS CLASS OF CERTIFICATE FOR ANY OTHER PURPOSE AND ACCORDINGLY ANY DIGITAL SIGNATURE GENERATED BY THE PRIVATE KEY OF THIS CLASS OF CERTIFICATE USED OTHER THAN TO ACKNOWLEDGE RECEIPT OF A MESSAGE AS SET OUT ABOVE MUST BE TREATED AS A SIGNATURE GENERATED AND USED WITHOUT THE AUTHORITY OF THE SUBSCRIBER ORGANISATION WHOSE SIGNATURE IT IS

AND MUST BE TREATED FOR ALL PURPOSES AS AN UNAUTHORISED SIGNATURE.

Further, digital signatures generated by this class of certificate are only to be used to acknowledge the receipt of electronic messages in transactions which are not related to or connected with the payment of money on-line or the making of any investment on-line or the conferring on-line of any financial benefit on any person or persons or entities of whatsoever nature and under no circumstances are digital signatures generated by these certificates to be used to acknowledge the receipt of messages sent in connection with the negotiation or conclusion of a contract or any legally binding agreement.

1.2.4 Certificate Lifespan

Certificates issued under this CPS are valid for one year. (See Section 3.2 for Certificate Renewal).

1.2.5 Personal Application at HKPost Premises

All initial applications and applications following the revocation or expiration of an e-Cert will require the applicant personally to attend at a designated HKPost premises, or premises of other organisations designated by HKPost, to present the necessary documents of identification, application form and signed Subscriber Agreement (where applicable) and be prepared to answer any questions concerning the same. In respect of e-Cert (Personal) certificates this means that all applicants for such e-Certs must attend personally (except the parent or legal guardian of an applicant who is under 18). In respect of e-Cert (Organisational) certificates, members or employees to be named in the certificate need not attend personally, but the Authorised Representative of the organisation who is applying for the e-Cert (Organisational) certificate must attend personally. In respect of e-Cert (Server) certificates and e-Cert (Encipherment) certificates this means that the Authorised Representative of the organisation making the application must attend personally. Upon such personal attendance, the applicants will be required to produce evidence of identity. (See further Section 3 below).

1.3 Contact Details

Subscribers may send their enquiries, suggestions or complaints by:
Mail to : Electronic Services Division, Kowloon East Post Office Box 68777
Tel: 2921 6633
Fax: 2775 9130
Email: enquiry@hongkongpost.gov.hk

1.4 Complaints 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, withdrawing 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, withdrawal, 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 Subscribers rejection of their applications (see Section 4.1);
c) notify Subscribers the approval of the application and how the certificates may be retrieved (see Section 4.2 and 4.3);
d) revoke certificates and publish Certification Revocation Lists in a timely manner (see Section 4.4); and
e) notify Subscribers of the revocation of their certificates (see Section 4.4.1, 4.4.2 and 4.4.3)

2.1.2 Subscriber Obligations

Subscribers are responsible for:

a) Securely generating a key pair using a trustworthy system during the process of obtaining a certificate if the Subscribers do not require the Central key Generation service. **In the case of HKPost carrying out the central key generation service on behalf of the Subscriber, HKPost will generate the certificate in a trustworthy system and environment within HKPost's premises on behalf of the Subscriber to ensure that the private key is not tampered with.**
b) Completing the application procedures properly and signing a Subscriber Agreement in the appropriate form and performing the obligations placed upon them by that Agreement, and ensuring accuracy of representations in certificate application.
c) Procuring the issuance of a certificate by HKPost including accurately following the directions as to the completion of certificates given in the e-Cert Customer Kit and accompanied CD-ROM (or alternative storage medium) if the Subscribers do not require the Central Key Generation service.
d) Acknowledging that by accepting the certificate (which will occur during the process for completing the certificate) 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.
e) In the case of an e-Cert (Encipherment) certificate, ensuring that :
   - authorised users only have the Subscriber Organisation's authority to use and in fact use the certificate and digital signature associated with it only to decrypt incoming electronic

messages and to acknowledge the receipt of the same and for no other purposes whatsoever;

- such certificates are used only (i) to send encrypted electronic messages to the Subscriber; (ii) to permit the Subscriber Organisation to decrypt messages; and (iii) to permit the Subscriber Organisation to acknowledge receipt of the encrypted message by sending an acknowledgement with a digital signature added to it to confirm the identity of the receiving Subscriber Organisation;
- No attempt is made to use the private key relating to an e-Cert (Encipherment) certificate to generate a digital signature other than for the purpose of acknowledging receipt of an incoming electronic message;
- reasonable precautions are taken by the authorised users to maintain the security of the private key.

f) Reporting any loss or compromise of their private key immediately 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).

g) Notifying HKPost immediately from time to time of any change in the information in the certificate provided by the Subscriber.

h) Notifying HKPost 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 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 could revoke it under the terms of the CPS, or after the Subscriber has made a revocation request or been notified by HKPost of HKPost's intention to suspend or revoke the certificate under the terms of this CPS.

k) Upon becoming so aware of any ground upon which HKPost could revoke the certificate, or upon the Subscriber making a revocation request or upon being notified by HKPost of its intention to revoke the certificate, 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 (either by HKPost or at the Subscriber's request) and stating in clear terms that, as this is the case, the Relying Parties should not rely upon the certificate in respect of the transaction.

2.1.2.1 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.

2.1.3 Relying Party Obligations

Relying Parties relying upon HKPost e-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 in particular in view of the limited duty of care and limited

monetary liability that HKPost undertakes to Relying Parties as set out in this CPS and in the certificate and, in the case of an e-Cert (Encipherment) certificate, in view of the limited purposes for which such a certificate can be used, as set out in this CPS.

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 to exercise a reasonable degree of skill and care 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 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 in carrying out this contract and its rights and 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 and the Hong Kong Post Office are under no liability of any kind in respect of such liability, loss or damage.

This means, for example, that provided that the HKPost has exercised a reasonable degree of skill and care, HKPost and Hong Kong Post Office 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 recognized certificate issued by HKPost.

This means, also, that, provided HKPost (by the Hong Kong Post Office) has exercised a reasonable degree of skill and care to avoid and/or mitigate the effects of matters beyond its control, neither HKPost nor the Hong Kong Post Office 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, the Subscriber Agreements are not contracts 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 is 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. The only qualification upon the foregoing is with regard to the e-Cert Customer Kit and CD-ROM (or alternative storage medium) referred to in Section 4.3 below. No right, title or interest in the same is transferred to Subscribers: HKPost agrees to transfer, free of charge, those articles into possession of Subscribers for the limited purposes set out in Section 4.3, nonetheless HKPost does promise that it will exercise reasonable care to see that the same is fit for the purposes of completing and accepting a certificate as set out in Section 4.3 below, 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 CD-ROM (or alternative storage medium) may contain other material not relevant to the completion and acceptance of an e-Cert, 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 CD-ROM (or alternative storage medium) .

2.2.3 Limitation of Liability

2.2.3.1 Reasonableness of Limitations

Each Subscriber and Relying Party must acknowledge and agree that the PKI initiative and HKPost's role as a CA within that initiative are new and innovative ventures, in which the sum received by HKPost from Subscribers is modest compared to the burden that could be placed upon HKPost if HKPost were liable to Subscribers and Relying Parties without limit for damages under or in connection with Subscriber Agreements or the issue by HKPost of certificates under the PKI. Accordingly, each Subscriber and Relying Party must agree that it is reasonable for HKPost to limit its liabilities as set out in the Subscriber Agreements and in this CPS.

2.2.3.2 Limitation on Types of Recoverable Loss

In the event of HKPost's breach of the Subscriber Agreements or of any duty of care, and in particular, of 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 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 (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) 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$ 500,000 and HK $ 250,000 Limit

Subject to the exceptions that appear below, in the event of HKPost's breach of a Subscriber Agreement or of 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 $500,000 in respect of one e-Cert (Personal) certificate, e-Cert (Organisational) certificate or e-Cert (Server) certificate or HK $250,000 in respect of one e-Cert (Encipherment) 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, withdrawal or publication of an e-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 Personnel

Neither the Hong Kong Post Office nor any officer or employee or other agent of the Hong Kong Post Office 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, the Hong Kong Post Office and none of such 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 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 Liability to Consumers

In respect of Subscribers who do not enter into Subscriber Agreements in the course of a business or held themselves out as doing so, it is possible that, as a matter of law, some or all of the limitations of liability that apply in the event of HKPost's failure to carry out the Subscriber Agreements with them with reasonable skill and care do not apply to any claim they may have.

2.2.3.8 Certificate Notices, Limitations and Reliance Limit

Certificates issued by HKPost shall contain the following reliance limit and/or limitation of liability notice:

"The Postmaster General acting by the officers of the Hong Kong Post Office has issued this certificate as a 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 which may be read on the HKPost CA web site at http://www.hongkongpost.gov.hk. The laws of Hong Kong SAR applies 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, its officers, employees and agents) 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;
d) Performing all appropriate certificate validation procedures.

If, despite the exercise of reasonable skill and care by the Postmaster General and the Hong Kong Post Office, its officers, employees or agents, this certificate is in any way inaccurate or misleading, the Postmaster General, Hong Kong Post Office, its 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, its officers, employees or agents, then the Postmaster General will pay a Relying Party up to HK $500,000 or, if this certificate is an e-Cert (Encipherment) certificate, HK $ 250,000, 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 $500,000 or, if this certificate is an e-Cert (Encipherment) certificate, HK $ 250,000, and in all cases in relation to categories of loss (1) and (2), is HK $0.

Neither the Hong Kong Post Office nor any officer, employee or agent of the Hong Kong Post Office undertakes any duty of care to Relying Parties in any circumstances in relation to this certificate.

Time Limit For Making Claims

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, withdrawal or publication of this e-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, its 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 Defective e-Cert Customer Kit or CD-ROM (or alternative storage medium) or Floppy Disk or other Storage Medium and for Accepted but Defective Certificates

2.2.4.1 Notwithstanding the limitation of liability set out above, if the e-Cert Customer Kit or CD-ROM (or alternative storage medium) or floppy disk or other storage medium ("kit") referred to in Sections 3.1.7 or 4.3 (as applicable) below is defective so that the certificate in respect of which the same was supplied cannot be completed or accepted properly or at all, and the Subscriber to whom they were supplied notifies HKPost of this immediately to permit the supply (if desired) of a replacement "kit", then if such notification has occurred within 3 months of the Subscriber being sent the "kit" and the Subscriber no longer wants a certificate, HKPost, on being satisfied of the existence of any such defect, will refund the fee. If the Subscriber waits longer than 3 months after the date upon which the "kit" was sent to him before notifying HKPost of any such defect, the fee will not be refunded as of right, but only at the discretion of HKPost.

2.2.4.2 Notwithstanding the limitation of HKPost's liability set out above, if, after acceptance of the certificate, a Subscriber finds that, in respect of e-Cert (Personal) certificates, e-Cert (Organisational) certificates and e-Cert (Server) 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, or, in respect of an e-Cert (Encipherment) certificate, no enciphered electronic communications can be completed properly or at all, and that Subscriber notifies HKPost of this immediately to permit the certificate to be revoked and (if desired) re-issued, then, if such notification has occurred within 3 months of the acceptance of the certificate and the Subscriber no longer wants a certificate, HKPost, on being satisfied of the existence of any such error will refund the fee. If the Subscriber waits longer than 3 months after acceptance before notifying HKPost of any such error, the fee will not be refunded as of right, but only at the discretion of HKPost.

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

No agent or employee of the Hong Kong Post Office 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 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

HKPost is not 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, 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 or Postal 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. No alternative dispute resolution procedures regarding Subscriber or Relying Party disputes will be implemented by HKPost. Any claims should be submitted to HKPost at the following address:

Electronic Services Division
Hongkong Post
2 Connaught Place, Central
Hong Kong

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 Fees

e-Cert (Personal) certificates are available at the cost of HK$150 per certificate per year (although first time Subscribers will only be asked to pay HK$50 per certificate for the first year). Renewal of e-Cert (Personal) certificates is available at the cost of HK$50 per certificate per year.

e-Cert (Organisational) certificates are available at the cost of HK$150 per certificate per year (although first time Subscribers will only be asked to pay HK$50 per certificate for the first year). An additional administration fee of HK$150 per application (irrespective of the number of Subscribers) is payable.

e-Cert (Server) certificates are available at HK$2,500 per certificate per year.

e-Cert (Encipherment) certificates are available at HK$150 per certificate per year. An additional administration fee of HK$150 per application (irrespective of the number of Subscribers) is payable.

2.5 Publication and Repository

HKPost maintains a repository that contains a list of issued certificates, the current certificate revocation list, the HKPost public key, a copy of this CPS, and other information related to e-Cert certificates which reference this CPS. The repository is available on a substantially 24 hour 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 issued under this CPS in the repository following the processing of an approved e-Cert application. The HKPost repository can be accessed at URL ldap://ldap.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 authorised HKPost employees have access to the repository to update and modify the contents.

2.5.3 Certificate Repository Update Cycle

The repository is updated promptly upon the issuance of each certificate and any other applicable events described in Section 4.

2.6 Compliance Audit

Compliance audits conducted on the HKPost's system of issuing, withdrawing and publishing e-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 Electronic Transactions Ordinance (Cap.553) and the Code of Practice for Recognized Certification Authorities.

2.7 Confidentiality

The restrictions in this subsection apply to HKPost and any HKPost subcontractors performing tasks related to HKPost's system of issuing, withdrawing and publishing e-Certs. Information about Subscribers that is submitted as part of an application for an e-Cert certificate under this CPS will be used only for the purposes collected and is kept confidential except to the extent necessary for HKPost to perform its 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 Registration

Save in the case of applicants to be named in e-Cert (Organisational) certificates, each applicant for an e-Cert must appear in person at a designated HKPost premises, or premises of other organisations designated by HKPost, and present proof of identity as described in sections 3.1.8, 3.1.9, 3.1.10 and 3.1.11. In the case of applicants to be named in e-Cert (Organisational) certificates, their attendance is not required, but the Authorised Representative of the applicant organisation must appear in person.

All applicants for e-Certs must submit a completed and signed application form and Subscriber Agreement to HKPost. e-Cert (Organisational) certificate, e-Cert (Server) certificate and e-Cert (Encipherment) certificate applications also require the signature of an Authorised Representative of the organisation with which the applicant is affiliated and require such Authorised Representative as well as the applicant organisation to become a Subscriber (see also Section 3.1.1.5). Following approval of the application, HKPost prepares an e-Cert and notifies the applicant explaining how the certificate may be retrieved.

3.1.1 Types of Names

3.1.1.1 e-Cert (Personal) certificates

Subscribers for e-Cert (Personal) certificates will be identified in a certificate with a Subscriber Name consisting of:

a) The Subscriber's name as it appears on the Subscriber's Hong Kong identity card.
b) The Subscriber's Hong Kong identity card number which will be stored in the certificate as a hash value (see **Appendix B**).

3.1.1.1.1 e-Cert (Personal) certificates issued to Subscriber who are under 18

Such Subscribers will be identified in the certificate as above, but their parent or legal guardian, although they must become a Subscriber, will not be named in the certificate.

3.1.1.2 e-Cert (Organisational) certificates

Subscribers for e-Cert (Organisational) certificates will be identified in a certificate with a Subscriber Name consisting of:

a) The Subscriber's name as it appears on the applicant's Hong Kong identity card/passport.
b) The Subscriber organisation's name as it is registered with the appropriate Hong Kong Government Department or registration agency or as a statutory body whose existence is recognized by the laws of Hong Kong SAR, or the official name of that Bureau or Department where the Subscriber organisation is a Bureau or Department of the Government of Hong Kong SAR.
c) The organisation's Hong Kong Company/Business Registration Number where the Subscriber organisation is not a Bureau or Department of the Government of Hong Kong SAR or as a statutory body whose existence is recognized by the laws of Hong Kong SAR.

3.1.1.3 e-Cert (Server) certificates

Applicants for e-Cert (Server) certificates will be identified in a certificate with a Subscriber Name consisting of:

a) The Subscriber organisation's name as it is registered with the appropriate Hong Kong Government Department or registration agency or as a statutory body whose existence is recognized by the laws of Hong Kong SAR, or the official name of that Bureau or Department where the Subscriber organisation is a Bureau or Department of the Government of Hong Kong SAR.
b) The organisation's Hong Kong Company/Business Registration Number where the Subscriber organisation is not a Bureau or Department of the Government of Hong Kong SAR or a statutory body whose existence is recognized by the laws of Hong Kong SAR.
c) The server name (including domain name of the server) owned by the Subscriber organisation.

3.1.1.4 e-Cert (Encipherment) certificates

Applicants for e-Cert (Encipherment) certificates will be identified in the certificate with a Subscriber Name consisting of:

a) The Subscriber organisation's name as it is registered with the appropriate Hong Kong Government Department or registration agency or as a statutory body whose existence is recognized by the laws of Hong Kong SAR, or the official name of that Bureau or Department where the Subscriber organisation is a Bureau or Department of the Government of Hong Kong SAR.
b) The organisation's Hong Kong Company/Business Registration Number where the Subscriber organisation is not a Bureau or Department of the Government of Hong Kong SAR or a statutory body whose existence is recognized by the laws of Hong Kong SAR.
c) The name of Subscriber Unit of the Subscriber organisation.

3.1.1.5 The Authorised Representative

Although the Authorised Representative of the organisation must also become a Subscriber for an e-Cert (Organisational) certificate, e-Cert (Server) certificate or e-Cert (Encipherment) certificate, that person will not be identified in the e-Cert.

3.1.1.6 Organisation Names in Chinese Language

For Organisations who subscribe to e-Cert who 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 e-Cert since all e-Certs are issued in the English language only. Subscribers will however be able to search such Organisations' Chinese names by following the instruction provided on the web site at http://www.hongkongpost.gov.hk.

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 e-Cert certificates are described in Section 3.1.1. Appendix B should be referred to for interpretation of the subject name of the e-Cert certificates.

3.1.4 Name Uniqueness

Taking all components (including the Subscriber Reference Number (SRN)) of the name together, the Subscriber Name shall be unambiguous and unique. 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 in matters concerning name disputes are discretionary and final.

3.1.6 Authentication and Role of Trademarks

Subscribers warrant (promise) to HKPost and represent to Relying Parties that the information supplied by them in the e-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

a) **Key Generation by Subscribers**

In the case of key generation by Subscribers, Subscribers must generate their own key pairs and use a trustworthy system for such generation. 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 e-Cert. Upon receipt of the certificate request issued by the Subscriber for certificate generation, the HKPost system will check the signature on the certificate request structure containing the public key material to ensure possession of the private key.

b) **Central Key Generation**

The option of Central Key Generation service is available to Subscribers of e-Cert (Personal), e-Cert (Organisational) and e-Cert (Encipherment) certificates. In the case of HKPost carrying out the central key generation service on behalf of the Subscriber, HKPost will generate the certificate 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 and delivered to the Subscriber in a secure manner designated on the application form. HKPost fully reserves the right to store the private key and the certificate on alternative technological storage medium to the floppy disk as and when suitable technology is available. If alternative technological storage medium is used, it will still be delivered to the Subscriber in a secure manner designated on the application form.

3.1.8 Authentication of Organisation Identity

When an e-Cert (Organisational) certificate is applied for, HKPost will follow the procedures outlined in Section 3.1.9 except that only the Authorised Representative must complete the in-person process outlined below and must also become a Subscriber and present (1) 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 Subscribers to be identified in the e-Cert (Organisational) certificates; (2) photocopies of the Hong Kong identity cards or passports of all Subscribers to be so identified and the Authorised Representative's own Hong Kong identity card or passport; and (3) documentation issued by the appropriate Hong Kong registration agency attesting to the existence of the organisation.

Applications for e-Cert (Server) certificates must be made by the personal attendance at a designated HKPost premises, or premises of other organisations designated by HKPost, of the Subscriber organisation's Authorised Representative who must present (1) 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 where appropriate proving the ownership of the domain name to be identified in the e-Cert (Server) certificate; (2) the Authorised Representative's own Hong Kong identity card or passport; and (3) documentation issued by the appropriate Hong Kong registration agency attesting the existence of the organisation.

Applications for e-Cert (Encipherment) certificate must be made by the personal attendance at a designated HKPost premises, or premises of other organisations designated by HKPost, of the Subscriber organisation's Authorised Representative who must present (1) 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; (2) the Authorised Representative's own Hong Kong identity card or passport; and (3) documentation issued by the appropriate Hong Kong registration agency attesting the existence of the organisation.

In the case of applications from Bureaux or Departments of the Government of Hong Kong SAR, the Authorised Representative must personally present at a HKPost designated premises, or premises of other organisations designated by HKPost, a memo or letter impressed with the relevant Bureau or Department chop, appointing that person as the Authorised Representative to sign on behalf of the Bureau or Department, any documents relating to the application, revocation and renewal of certificate(s) issued by HKPost. The memo or letter must be signed by a Departmental Secretary or officer at equivalent level.

3.1.9 Authentication of Individual Identity

Confirmation of the identity of each individual Subscriber will be accomplished through an in-person process that operates as follows:

Each applicant for a certificate must appear at a designated HKPost premises, or premises of other organisations designated by HKPost, and submit a completed and signed e-Cert application form and the Subscriber Agreement and the applicant's Hong Kong identity card. Personnel at the aforementioned premises will retain a photocopy of the identity card, review and certify the application package, and forward the application to HKPost CA Centre for processing.

3.1.10 Authentication of Individual Identity Where Subscriber is Under 18

Each applicant who is under 18 (a minor) must attend at a designated HKPost premises, or premises of other organisations designated by HKPost, and present (1) the duly completed and signed application form and Subscriber Agreement, signed by the minor and the parent or guardian who is to be a Subscriber (2) the birth certificate of the minor (3) the Hong Kong identity card of the minor and a copy of the Hong Kong identity card or passport of the parent or legal guardian who is to be a Subscriber and, (4) in the case of legal guardianship, the official document bestowing such guardianship.

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. HKPost will not perform renewal of expired, suspended or revoked certificates. HKPost will issue renewal notice in the form of emails to the Subscribers prior to the expiry of the certificates.

3.2.1 e-Cert (Personal) certificates

An e-Cert (Personal) certificate may be renewed without going through the process of a face-to-face authentication of the identity of the Subscriber which is required when a new certificate application is made. To apply for renewal, the Subscriber may either submit the renewal application through electronic means or submit a completed and signed renewal application form to HKPost. Details of the renewal application are available at both post offices and HKPost's web site at http://www.hongkongpost.gov.hk. Upon renewal, the Subscriber can generate the key pair through HKPost's central key generation service by HKPost's personnel or by going through an electronic interactive process if the Subscriber requires such service at the time of the application for renewal. 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 such 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 e-Cert (Organisational), e-Cert (Server) and e-Cert (Encipherment) certificates

There is no automatic renewal of an e-Cert (Organisational), e-Cert (Server) and e-Cert (Encipherment) certificates. The process of "Authentication of Organisation Identity" as described under Section 3.1.8 will be conducted as if a new application is received. The Authorised Representative of the Organisation will need to complete and submit a Certificate Renewal Form (available at HKPost web site at http://www.hongkongpost.gov.hk) along with the other documentation referred to in the application form and appropriate renewal fee. In circumstances where Authorised Representatives are replaced, they will need to also complete, sign and submit a Subscriber Agreement. 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 such 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.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Applicants for e-Certs under this CPS must complete and submit an application on a form created by HKPost. The documentation required for proving the identity of the Subscriber is stipulated in Section 3.1.8 (Authentication of Organisation Identity), 3.1.9 (Authentication of Individual Identity) and 3.1.10 (Authentication of Individual Identity where Subscriber is Under 18) of this CPS. The information provided to the Subscribers for obtaining new certificates is stipulated in Section 4.3 of this CPS and in the Subscriber Agreement which the Subscriber signs and submits with the application form. All application information transmitted electronically between the applicant and HKPost must use Secure Sockets Layer or a similar protocol prescribed by HKPost from time to time.

In the event HKPost is not successful in validating an application in accordance with the requirements stipulated in this CPS, HKPost will notify the applicant the rejection of his/her application.

4.2 Certificate Creation and Issuance

a) **Key Generation by Subscribers**

HKPost will notify the applicant approval of an application by email or letter mail. The certificate issuance process is as follows:-

- The applicant generates the private key and public key on his/her own devices.
- The public key, which will be contained in a certificate request, will be transmitted to HKPost. Upon receipt of the certificate request, HKPost will verify that the applicant is in possession of the corresponding private key as set out in Section 3.1.7 of this CPS. HKPost will not have possession of the applicants' private keys.
- Upon verifying the applicant's possession of his/her private key, HKPost will generate the certificate in which the applicant's public key will be included.

b) **Central Key Generation**

In the case of the central key generation service, the key pair generation and certificate creation is performed by HKPost on behalf of the Subscriber. This is done in a trustworthy system and environment within HKPost's premises to ensure that the private key will not be tampered with.

The certificate generated in either of the above ways will be posted to the repository and the Subscriber may download the certificate from HKPost's repository at ldap://ldap.hongkongpost.gov.hk.

4.3 The Procedure for Issuing, Checking and Accepting Certificates

a) HKPost will aim to complete the process of an application within the period of time specified in the application form. HKPost will authenticate the identity of each Subscriber and, if and when their identity is authenticated, will notify the Subscriber(s) that the requested certificate is ready to be completed and give details of the electronic interactive process that must be followed to ensure completion. This will usually be done by sending to

the Subscriber(s) an e-Cert Customer Kit which may include a CD-ROM (or alternative storage medium) and PIN mailer (a sealed envelope containing a PIN) and instructions as to how to use them. Where the central key generation service is required, the key pair generation and certificate creation is performed by HKPost on behalf of the Subscriber. During the process, the Subscriber is given the opportunity to check that the contents of the certificate are accurate and true. Upon confirmation to this effect, the system will generate the key pair and create the certificate. The private key and certificate, which are protected by the Subscriber's PIN, will then be stored on a floppy disk or alternative storage medium as mentioned in Section 3.1.7. The floppy disk 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 Subscriber in a secure manner specified on the application form. Proper security controls are in place so that HKPost personnel will not be able to access the Subscriber's private key during the process. Subscribers agree that they are fully accountable for the safe custody of the private key upon receipt of the disk or alternative storage medium and agree that they will be responsible for any consequences under any circumstances for the compromise of the private key. **HKPost will not make or keep a copy of the Subscriber's private key**.

b) When following the interactive procedures for the completion of the certificate outlined in Section 4.3(a) above, the Subscriber(s) will be given the opportunity to **CHECK** to see that **all the information and each representation made by the Subscriber(s) included in the certificate is accurate and true**. Each Subscriber warrants (promises) to HKPost that this check will be done and done properly.

(i) If there is any inaccuracy or untruth in the certificate, the Subscriber(s) **MUST CANCEL** the procedure;

(ii) If (and only if) there is no inaccuracy or untruth in the certificate, Subscriber(s) may continue as directed and permit and consent to the completion of the certificate. By so continuing, Subscriber(s) **ACCEPT** the certificate issued under this CPS.

(iii) In the event of the Subscriber(s)' failure to verify the contents of the certificate or failure to accept the certificate within three months of the date of the Subscriber(s) being sent a notification by HKPost that the certificate is either ready to be verified or ready to be accepted, this Agreement will automatically terminate and Subscriber(s) will not be entitled to a refund of the subscription fee. After the expiry of the aforementioned three months, if the Subscriber(s) wish to apply for an e-Cert certificate, he/she will need to make a fresh application and pay another subscription fee to HKPost pursuant to that application.

By accepting the certificate, the Subscriber acknowledges that the information contained in the certificate is correct. Acceptance confirms and is evidence that the Subscriber agrees to be bound by the terms of this CPS, the certificate application form, and the Subscriber Agreement.

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 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 HKPost 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 an e-Cert has been, or is suspected of having been, compromised (see also Section 2.1.2(h)).

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) Knows or has reasonable cause to believe that the Subscriber whose details appear on the certificate or the Authorised Representative:
    (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;
    (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.

    and where a Subscriber is an Organisation that :
    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 Electronic Transactions Ordinance;
    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 may submit a certificate revocation request to HKPost by fax, lettermail, email or in-person. Based on the revocation request, HKPost will put a "hold" on the certificate, which effectively suspend the validity of the certificate. The certificate will be revoked, which effectively terminates the validity of the certificate permanently, upon receipt of the final confirmation of revocation from the Subscriber. 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 at any of the Post Offices and from the web site at http://www.hongkongpost.gov.hk. HKPost may consider Subscriber's request for resuming the validity of certificates that are in a "hold" status. However, resuming the validity of a certificate that is in a "hold" status 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 "hold" status will not be included the succeeding Certificate Revocation Lists.

The business hours for revocation are as follows:

Monday - Friday	09:00 am - 5:00 pm
Saturday	09:00 am - 12:00 noon
Sunday & Public Holidays	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, HKPost will open at its usual hour 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, HKPost will open at 2:00 pm for any weekday other than a Saturday, Sunday or public holiday

4.4.3 Service Pledge & Certificate Revocation List Update

a) HKPost will exercise reasonable endeavours to see that within 2 working days of (1) HKPost receiving a revocation request from the Subscriber or (2) in the absence of such a request, the decision by HKPost to suspend or revoke the certificate, the suspension or revocation is posted to the Certificate Revocation List. However, a Certificate Revocation List is not published in the directory for access by the public following each certificate revocation. Only when the next Certificate Revocation List is updated and published will it reflect the revoked status of the certificate. Certificate Revocation Lists are published daily and are archived for 7 years.

   For the avoidance of doubt, all Saturdays, Sundays, public holidays and for all weekdays on which a tropical cyclone and rainstorm warning signal is hoisted, are not working days.

   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 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 by HKPost of HKPost's intention to suspend or revoke the certificate. HKPost shall be under no liability to Subscribers 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 could revoke the certificate, or upon making a revocation request or upon being notified by HKPost 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 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 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 who complete the transaction despite such notification.

HKPost shall be under no liability to Relying Parties in respect of the period between HKPost'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 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.

d) The e-Cert Certificate Revocation List (CRL) is updated 3 times daily at 09:45, 14:15 and 23:00 Hong Kong Time (i.e. 01:45, 06:15 and 15:00 Greenwich Mean Time (GMT)). Under normal circumstances, we will publish the latest CRL at "http://www.hongkongpost.gov.hk/crl/eCert.crl" or in the LDAP repository "ldap://ldap.hongkongpost.gov.hk" as soon as possible and within 15 minutes after the update time. HKPost may need to change the above updating and publishing schedule of the e-Cert CRL without prior notice if such changes are considered to be necessary under unforeseeable circumstances. For access to HKPost's repository, please refer to Section 2.5 of this CPS.

e) HKPost's policy concerning the situation where a relying party is temporarily unable to obtain information on revoked certificate is stipulated in Section 2.1.3 (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 processes the revocation action and posts it 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 implement multi-person control on processing audit logs which are 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 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 are created and maintained in case of the loss or destruction of the primary archives.

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 e-Cert root keys and certificates is 10 years. 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 for public access. The original root keys for verification will be kept for a minimum period as specified in Section 4.6.2 in case any signatures signed with the original key might have to be verified later.

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 services This incorporates a tested independent disaster recovery site which is currently located at least 10km from the CA's primary site within the territory of Hong Kong Special Administrative Region. The business continuity plans are reviewed and exercised annually.

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

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

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

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 Director of Information Technology Services and make public announcement if a private key for the issuance of e-Cert certificates under this CPS has been compromised. The compromise of a HKPost private key will result in prompt revocation of the certificates issued under that private key and the issuance of new and replacement certificates.

4.8.3 Key Replacement

In the event of key compromise or disaster recovery where a HKPost's private key for the issuance of e-Cert certificates under this CPS has been compromised or corrupted and cannot be recovered, HKPost will promptly notify the Director of Information Technology Services and make a public announcement as to which certificates have been revoked, and where HKPost's public key is revoked, how the new HKPost public key is provided to Subscribers, and how Subscribers are issued with new certificates.

4.9 CA Termination

In the event that HKPost ceases to operate as a CA, notification to the Director of Information Technology Services 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 a period of 7 years after the date of service termination.

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
HKPost has a CA facility 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 4.8.1)

5.1.8 Protection of Paper Documents
Paper documents and photocopies of identity confirmation documents are maintained by HKPost 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 (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 e-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.

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 follows personnel and management policies that provide reasonable assurance of the trustworthiness and competence of its personnel 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 investigations of personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary) to verify the employee's trustworthiness and competence in accordance with the requirements of this CPS and HKPost's personnel policies. 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 have received the initial training needed to perform their duties. HKPost also provides ongoing training as necessary to enable its personnel to remain current in required skills.

5.3.4 Documentation Supplied To Personnel

HKPost personnel 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 CA keys is implemented through physical security and secure key storage. 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 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 generated the root key pairs for issuing certificates that conform to this CPS. In the case of key generation by Subscribers, Subscribers will be responsible for generating their own key pairs for the certificates that conform to this CPS. **In the case of central key generation by HKPost on behalf of the Subscriber, the system will immediately delete the private key from its system once it is embedded into a floppy disk or alternative storage medium as mentioned in Section 3.1.7. HKPost will not make or keep a copy of the private key**.

6.1.2 Subscriber Public Key Delivery

Other than those key pairs generated under the central key generation by HKPost on behalf of the Subscriber, the Subscriber's public key must be transferred to HKPost using a method designed to ensure that:

- The key is not changed during transit
- The sender possesses the private key that corresponds to the transferred public key (See Section 3.1.7)
- The sender of the public key is the person named in the certificate application

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 e-Cert (Personal) certificates, e-Cert (Organisational) certificates and e-Cert (Server) 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. Keys used in e-Cert (Encipherment) certificates are for the purpose of conducting enciphered electronic communications. (See Section 1.2.3 (d))

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 1.

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 e-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 a Hardware Cryptographic Device which conforms 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 10 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 audit 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 systems. Change control procedures are in place to control and monitor all revisions and enhancements to be made to the components of the HKPost systems.

6.6 Network Security Controls

The HKPost 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 1.

7. CERTIFICATE AND CERTIFICATE REVOCATION LIST PROFILES

7.1 Certificate Profile

Certificates that reference 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 that reference this CPS are issued in the X.509 version 3 format (See Appendix B). A summary of the features of the e-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 for new certificates and upon all holders of existing certificates as those certificates are renewed. HKPost will notify the Director of Information Technology Services any subsequent changes to this CPS as soon as practicable. A copy of this CPS and its predecessors are available for viewing by Subscribers and Relying Parties on the HKPost CA web site at http://www.hongkongpost.gov.hk or in the HKPost repository. Paper copies of this CPS are also available for viewing by Subscribers and Relying Parties at any of Post Offices.

Appendix A - Glossary

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

"Accept a certificate", in relation to a person to whom a certificate is issued, means that the person while having notice of the contents of the certificate

a) authorises the publication of the certificate to one or more persons or in a repository;
b) uses the certificate; or
c) otherwise demonstrates approval of the certificate.

"Addressee" in relation to an electronic record sent by an originator, means the person who is specified by the originator to receive the electronic record but does not include an intermediary.

"Applicant" means a natural or legal person who applies for an e-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.

Certificate or "e-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 a responsible officer of the certification authority issuing it.

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

"Certification Practice Statement (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 (CRL)". A data structure that enumerates public-key certificates (or other kinds of certificates) that have been invalidated by their issuer prior to the time at which they were scheduled to expire.

"Correspond", in relation to private or public keys, means to belong to the same key pair.

"Digital Signature", in relation to an electronic record, means an electronic signature of the signer generated by the transformation of the electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can determine:-

(a) whether the transformation was generated using the private key that corresponds to the signer's public key; and
(b) whether the initial electronic record has been altered since the transformation was generated.

"Electronic Record" means a record generated in digital form by an information system, which can be
(a) transmitted within an information system or from one information system to another; and
(b) stored in an information system or other medium.

"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.

"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 the act of a certification authority of creating a certificate and notifying its contents to the person named or identified in that certificate as the person to whom it is issued.

"Key Pair", in an asymmetric 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.

"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.

"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.

"Rule of law" means
(a) an Ordinance;
(b) a rule of common law or a rule of equity; or
(c) customary law.

"Secure Socket Layer" means an Internet protocol that uses connection-oriented, end-to-end encryption to provide data confidentiality service and data integrity service for application layer traffic between a client (usually a World Wide Web browser) and a server (usually a Web server), and that can optionally provide peer entity authentication between the client and server. The IETF-standardized version of this is the TLS (Transport Layer Security) protocol, specified by RFC 2246.

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

"Subscriber" means a person who has signed a Subscriber Agreement and who-
(a) is named or identified in a certificate as the person to whom the certificate is issued;
(b) has accepted that certificate; and
(c) holds a private key which corresponds to a public key listed in that certificate.
For e-Cert (Organisational), e-Cert (Server) or e-Cert (Encipherment) certificate, both the organisation and the Authorised Representative of the organisation are required to become Subscribers under 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.

"**Verify a Digital Signature**", in relation to a given digital signature, electronic record and public key, means to determine that-

(a) the digital signature was generated using the private key corresponding to the public key listed in a certificate; and
(b) the electronic record has not been altered since its digital signature was generated,

and any reference to a digital signature being verifiable is to be construed accordingly.

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.

Appendix B - Hongkong Post e-Cert Format

		e-Cert (Personal) certificate	e-Cert (Personal/Minor) certificate	e-Cert (Organisational) certificate
Standard Fields				
Version		X.509 V3	X.509 V3	X.509 V3
Serial Number		[generated]	[generated]	[generated]
Signature Algorithm ID		sha1RSA	sha1RSA	sha1RSA
Issuer Name		cn=Hongkong Post e-Cert CA, o=Hongkong Post, c=HK	cn=Hongkong Post e-Cert CA, o=Hongkong Post, c=HK	cn=Hongkong Post e-Cert CA, o=Hongkong Post, c=HK
Validity	**Not Before**	[UTC Time]	[UTC Time]	[UTC Time]
	Not After	[UTC Time]	[UTC Time]	[UTC Time]
Subject Name		cn=[HKID name][1], ea=[email address], ou=[SRN][2], ou=[Renewal Code][3] o=Hongkong Post e-Cert (Personal), c=HK	cn=[HKID name][1], ea=[email address], ou=[SRN][2], ou=[Renewal Code][3] o=Hongkong Post e-Cert (Personal/Minor), c=HK	cn=[name], ea=[email address], ou=[SRN][2], ou=[BRN+CI/CR+Others][4], ou=[Organisation], ou=[Organisation branch/dept], o=Hongkong Post e-Cert (Organisational), c=HK
Subject Public key Info	**Algorithm ID**	RSA	RSA	RSA
	Public Key	[generated and supplied from subscriber's browser during certificate request or generated by Hongkong Post on behalf of the subscriber through the central key generation service][5]	[generated and supplied from subscriber's browser during certificate request or generated by Hongkong Post on behalf of the subscriber through the central key generation service][5]	[generated and supplied from subscriber's browser during certificate request or generated by Hongkong Post on behalf of the subscriber through the central key generation service][5]
Issuer Unique Identifier		Not used	Not used	Not used
Subject unique identifier		Not used	Not used	Not used
Standard Extensions[7]				
Authority Key Identifier	**Issuer**	cn=Hongkong Post Root CA, o=Hongkong Post, c=HK	cn=Hongkong Post Root CA, o=Hongkong Post, c=HK	cn=Hongkong Post Root CA, o=Hongkong Post, c=HK
	Serial Number	[Inherited from issuer]	[Inherited from issuer]	[Inherited from issuer]
Basic Constraints	**Subject Type**	End Entity	End Entity	End Entity
	Path Length Constraint	None	None	None
Key Usage		Digital Signature, Key Encipherment	Digital Signature, Key Encipherment	Digital Signature, Key Encipherment
Subject Alternative Name	**DNSName**	[encrypted(HKID)][6]	[encrypted(HKID)][6]	Not used
	rfc822	[email address]	[email address]	[email address]
Netscape Extensions[7]				
Netscape Cert Type		SSL client, S/MIME	SSL client, S/MIME	SSL client, S/MIME
Netscape SSL Server Name		Not used	Not used	Not used

		e-Cert (Personal) certificate	e-Cert (Personal/Minor) certificate	e-Cert (Organisational) certificate
Netscape Comment		Hongkong Post e-Cert For terms and conditions governing the use of this e-Cert, please see the Subscriber Agreement and CPS both of which can be found at any of our Post Offices. The CPS can also be viewed at http://www.hongkongpost.gov.hk.	Hongkong Post e-Cert For terms and conditions governing the use of this e-Cert, please see the Subscriber Agreement and CPS both of which can be found at any of our Post Offices. The CPS can also be viewed at http://www.hongkongpost.gov.hk.	Hongkong Post e-Cert For terms and conditions governing the use of this e-Cert, please see the Subscriber Agreement and CPS both of which can be found at any of our Post Offices. The CPS can also be viewed at http://www.hongkongpost.gov.hk.

Appendix B

Hongkong Post e-Cert Format

		e-Cert (Server) certificate	e-Cert (Encipherment) certificate
Standard Fields			
Version		X.509 V3	X.509 V3
Serial Number		[generated]	[generated]
Signature Algorithm ID		sha1RSA	sha1RSA
Issuer Name		cn=Hongkong Post e-Cert CA, o=Hongkong Post, c=HK	cn=Hongkong Post e-Cert CA, o=Hongkong Post, c=HK
Validity	**Not Before**	[UTC Time]	[UTC Time]
	Not After	[UTC Time]	[UTC Time]
Subject Name		cn=[URL], ou=[SRN][2], ou=[BRN+CI/CR+Others][4], ou=[Organisation], ou=[Organisation branch/dept], o=Hongkong Post e-Cert (Server), c=HK	cn=[Unit name], ea=[email address], ou=[SRN][2], ou=[BRN+CI/CR+Others][4], ou=[Organisation], ou=[Organisation branch/dept], o=Hongkong Post e-Cert (Encipherment), c=HK
Subject Public key Info	**Algorithm ID**	RSA	RSA
	Public Key	[generated and supplied from subscriber's CSR]	[generated and supplied from subscriber's browser during certificate request or generated by Hongkong Post on behalf of the subscriber through the central key generation service][5]
Issuer Unique Identifier		Not used	Not used
Subject unique identifier		Not used	Not used
Standard Extensions[7]			
Authority Key Identifier	**Issuer**	cn=Hongkong Post Root CA, o=Hongkong Post, c=HK	cn=Hongkong Post Root CA, o=Hongkong Post, c=HK
	Serial Number	[Inherited from issuer]	[Inherited from issuer]
Basic Constraints	**Subject Type**	End Entity	End Entity
	Path Length Constraint	None	None
Key Usage		Key Encipherment	Digital Signature, Key Encipherment
Subject Alternative Name	**DNSName**	Not used	Not used
	rfc822	Not used	[email address]
Netscape Extensions[7]			
Netscape Cert Type		SSL server	SSL client, S/MIME
Netscape SSL Server Name		[URL]	Not used

		e-Cert (Server) certificate	e-Cert (Encipherment) certificate
Netscape Comment		Hongkong Post e-Cert For terms and conditions governing the use of this e-Cert, please see the Subscriber Agreement and CPS both of which can be found at any of our Post Offices. The CPS can also be viewed at http://www.hongkongpost.gov.hk.	Hongkong Post e-Cert This e-Cert is used ONLY (i) to send encrypted electronic messages to the subscriber organisation; (ii) to permit the subscriber organisation to decrypt messages; and (iii) to permit the subscriber organisation to acknowledge receipt of the encrypted message by sending an acknowledgement with a digital signature added to it to confirm the identity of the receiving subscriber organisation. For terms and conditions governing the use of this e-Cert, please see the Subscriber Agreement and CPS both of which can be found at any of our Post Offices. The CPS can also be viewed at http://www.hongkongpost.gov.hk.

Appendix B

Hongkong Post e-Cert Format

Notes:

[1] Name format: Surname (in capital) + Given name, e.g. CHAN Tai Man David

[2] SRN: Subscriber Reference number, 10 decimal digits

[3] If the certificate is a renewed certificate, a renewal code is added in the form of ":Rxx" where xx is a number. If the certificate is issued after its first renewal, the renewal code is ":R01". If the certificate is issued after its second renewal, the renewal code is ":R02", and so on.

[4] Business Registration Number (BRN): 16 digits, Certificate of Incorporation (CI)/ Certificate of Registration (CR): 8 digits, Others: max. 30 characters (blank if null). For HKSAR government departments, BRN and CI/CR are all zeroes, department name in abbreviation (e.g. HKPO for Hongkong Post) is placed in Others. If the certificate is a renewed certificate, a renewal code is added to the "Other" in the form of ":Rxx" where xx is a number. If the certificate is issued after its first renewal, the renewal code is ":R01". If the certificate is issued after its second renewal, the renewal code is ":R02", and so on.

[5] 1024-bit

[6] The subscriber'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 subscriber:-

$$\textbf{cert\_hkid\_hash} = \textit{SHA-1}\ (\ \textit{RSA}_{\textit{privatekey, sha-1}}\ (\ \textbf{hkid\_number}\ )\ )$$

where the *SHA-1 i*s a hash function and *RSA* is the signing function

For key generation by subscribers, **hkid_number** will be signed at the subscriber's browser. For Central Key Generation, hkid_number will be signed during the key generation process at HKPost premises. The signed HKID Number - $\textit{RSA}_{\textit{privatekey, sha-1}}$ **(hkid_number)** – will be passed to the Hongkong Post CA system through a secure channel. Upon verification of subscriber data at CA system side, the CA system will create a hash of the signed HKID number - ***SHA-1*** **(** $\textit{RSA}_{\textit{privatekey, sha-1}}$ **(hkid_number))**. The hash value will then be put into the designated extension field (DNSname) of the certificate being generated.

[7] All Standard Extensions and Netscape Extensions are "Non-critical".

Appendix C - Hongkong Post e-Cert CRL Format (X.509 v.2)

Standard Fields	Sub-fields	Field Content	Remarks
Version		V2	This field describes the version of encoded CRL.
Signature		Sha1RSA	This field contains the algorithm identifier for the algorithm used to sign the CRL.
Issuer		CN=Hongkong Post e-Cert CA 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.
RevokedCertificates	userCertificate	[Certificate Serial Number]	Revoked certificates are listed by their serial numbers.
	revocationDate	[UTC Time]	The date on which the revocation occurred is specified.
	CrlEntryExtensions		
	Reason Code (see Note 2 below)	[Revocation Reason Code]	Reason Code follows each Revoked Certificate standard field. 0= Unspecified 1= Key compromise 2= CA compromise 3= Affiliation changed 4= Superseded 5= Cessation of operation 6= Certificate hold
Standard Extensions			
Authority Key Identifier	Issuer	CN=Hongkong Post Root CA 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	[Serial number of issuer certificate]	This field indicates the serial number of the issuer certificate.
CRL Number		[generated by CA system]	The CRL Number is generated in sequence for each CRL issued by a CA.

Notes :

1. All Standard Extensions are "Non-Critical"

2. The reason code to be included for identifying the reason of revocation may indicate as "0" (i.e. unspecified) since Subscribers need not have or give any particular reason of certificate revocation.

Appendix D - Summary of Hongkong Post e-Cert Features

Features	***e-Cert (Personal) Certificate***	***e-Cert (Organisational) Certificate***	***e-Cert (Server) Certificate***	***e-Cert (Encipherment) Certificate***
Recognized Certificate	Yes	Yes	Yes	Yes
Key pair size	1024-bit RSA	1024-bit RSA	Up to 1024-bit RSA	1024-bit RSA
Key generation software provided by Hongkong Post	Yes	Yes	No	Yes
Key pair generation	By subscriber or by Hongkong Post on behalf of the subscriber through the central key generation service	By subscriber or by Hongkong Post on behalf of the subscriber through the central key generation service	By subscriber	By subscriber or by Hongkong Post on behalf of the subscriber through the central key generation service
Certificate holders	Holders of valid HKID card	Members or employees of registered organisations in Hong Kong	Internet Server Names of registered organisations in Hong Kong	Operational units of registered organisations in Hong Kong
Identity authentication	Face-to-face authentication of the subscriber's identity	Authentication of the identity of the organisation and its Authorised Representative	Authentication of the identity of the domain name, the organisation, and its Authorised Representative	Authentication of the identity of the organisation and its Authorised Representative
Usage of certificate	Digital Signature and Encryption	Digital Signature and Encryption	SSL Encryption	Encryption only
Submission of application	Applicant to submit application in person	Authorised Representative to submit application in person	Authorised Representative to submit application in person	Authorised Representative to submit application in person
Inclusion of subscriber's HKID hash in the certificate	Yes	No	No	No
Unique Subscriber Reference Number assigned to the certificate	Yes	Yes	Yes	Yes
Inclusion of subscriber's Business Registration/Company Registration Number (if any) in the certificate	No	Yes	Yes	Yes
Inclusion of subscriber's details	• Subscriber Name • Subscriber Email address	• Subscriber Name • Subscriber Email address • Subscriber Organisation	• Subscriber Server Name • Subscriber Organisation Name	• Subscriber Organisation Unit Name • Subscriber Organisation

Features	***e-Cert (Personal) Certificate***	***e-Cert (Organisational) Certificate***	***e-Cert (Server) Certificate***	***e-Cert (Encipherment) Certificate***
		Name		Name • Subscriber Email address
Subscription Fees (see also Section 2.4 of this CPS)	$150 per certificate per year (Renewal :- $50 per certificate per year)	Administration Fee $150 per application, $150 per certificate per year	$2500 per certificate per year(administration fee inclusive)	Administration Fee $150 per application, $150 per certificate per year
Certificate Validity	One Year	One Year	One Year	One Year
Reliance Limit	HK$500,000	HK$500,000	HK$500,000	HK$250,000