THE CERTIFICATION PRACTICE STATEMENT

OF

THE POSTMASTER GENERAL

As

A Recognized Certification Authority under the Electronic Transactions Ordinance

for

Hongkong Post e-Cert (Personal) for Smart ID Card

Date : 23 June 2003

Table of Contents

PREAMBLE

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

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

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

Under the Ordinance, the Postmaster General is a Recognized Certification Authority ("CA") for the purposes of the Ordinance and the PKI. Under the Ordinance the Postmaster General may perform the functions and provide the services of a CA by the officers of the Hong Kong Post Office. The Postmaster General has decided so to perform his functions, and he is therefore referred for the purposes of this document as **HKPost**.

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. The e-Cert (Personal) certificates issued under this CPS are referred to as "certificates" or "e-Certs" in this CPS.

The Registration of Persons (Amendment) Ordinance provides for the issue of a new smart ID card with multi-application capacity ("Smart ID Card") by the Immigration Department ("ImmD") of the Government of the Hong Kong Special Administrative Region. The inclusion of an e-Cert issued by HKPost in the chip of a Smart ID Card is provided under Schedule 5 of the Registration of Persons (Amendment) Ordinance. On this basis, HKPost issues e-Cert (Personal) certificates to individual Smart ID Cardholders, and embeds the e-Certs onto the Smart ID Cards.

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 (Personal) format
Appendix C contains a Hongkong Post e-Cert CRL format
Appendix D contains a summary of Hongkong Post e-Cert (Personal) 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 e-Cert (Personal) certificates which can be embedded onto the Smart ID Cards.

The Internet Assigned Numbers Authority ("IANA") has assigned the Private Enterprise Number 16030 to HKPost. For identification purpose, this CPS bears an Object Identifier ("OID") "1.3.6.1.4.1.16030.1.1.1" (see description of the field "Certificate Policies" in Appendix B).

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

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. HKPost has designated the e-Cert (Personal) certificate issued under this CPS as Recognized Certificate. 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 accepted Recognized Certificates. Recognized Certificates 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 (Personal) 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

Upon the issuance of a certificate signed by HKPost and acceptance of the certificate by the Subscriber, HKPost will then 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 Agreement 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 Agreement 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 who have been issued an e-Cert. Relying Parties are entities that rely on an e-Cert in a transaction. Applicants and Subscribers who rely on an e-Cert of another Subscriber 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.**

1.2.2.1 Warranties and Representations by Applicants and Subscribers

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

a) No person other than the Subscriber of the certificates 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 is the Digital Signature of the Subscriber.
c) All Information and representations made by the Subscriber included in the certificate are true.
d) The certificate will be used exclusively for authorised and legal purposes.
e) All Information supplied in the certificate application process does not infringe or violate in any way the trademarks, service marks, trade name, company name, or any other intellectual property rights of any third party.

1.2.3 Classes of Subscribers

HKPost issues certificates under this CPS only to Applicants whose application for a certificate has been approved by HKPost and who have signed or confirmed their acceptance of a Subscriber Agreement in the appropriate form. e-Cert (Personal) certificates are issued under this CPS and the Subscriber Agreement to individuals who have a HKID Card. These certificates may be used to perform commercial operations. e-Cert (Personal) certificates may be issued to persons under 18 who have a HKID Card (see also Section 3.1.1.2)..

1.2.4 Certificate Lifespan

Certificates issued under this CPS to new Applicants are valid for THREE (3) years. Certificates issued under this CPS as a result of certificate renewal may be valid for more than THREE (3) years but no more than THREE (3) years and ONE (1) month (see Section 3.3). The validity period of an e-Cert is specified in the certificate itself. Format of certificates issued under this CPS is in **Appendix B**.

1.2.5 Application at HKPost Premises

All initial applications and applications following the revocation or expiration of an e-Cert will require the applicants to submit their applications as described in sections 3.1 and 4.1.

1.3 Contact Details

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

1.4 Complaints 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 Certificates that have been accepted by the Subscriber. In accordance with this CPS, HKPost has the obligation to:-

a) issue and publish certificates in a timely manner (see Section 2.5);
b) notify Applicants of the approval or rejection of their applications (see Section 4.1);
c) revoke certificates and publish Certification Revocation Lists in a timely manner (see Section 4.4); and
d) 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) Agreeing that the certificate and key pair are generated by HKPost in a Trustworthy System and environment within HKPost's premises on behalf of the Subscriber**.**
b) Completing the application procedures properly and signing, or confirming acceptance of, a Subscriber Agreement in the appropriate form and performing the obligations placed upon them by that Agreement, and ensuring accuracy of representations in certificate application.
c) Accurately following the procedures specified in this CPS as to the completion of certificates.
d) Acknowledging that they are undertaking an obligation to protect the confidentiality (i.e. keep it secret) and the integrity of their private key using reasonable precautions to prevent its loss, disclosure, or unauthorised use.
e) 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).
f) Notifying HKPost immediately from time to time of any change in the Information in the certificate provided by the Subscriber.
g) 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.
h) Agreeing that by having issued or accepting a certificate they warrant (promise) to HKPost and represent to all Relying Parties that during the operational period of the certificate, the facts stated in Section 1.2.2.1 above are and will remain true.
i) Not using a certificate in a transaction on becoming aware of any ground upon which HKPost could suspend or revoke it under the terms of the CPS, or after the Subscriber has made a

revocation request or been notified by HKPost of HKPost's intention to suspend or revoke the certificate under the terms of this CPS.

j) Upon becoming so aware of any ground upon which HKPost could suspend or revoke the certificate, or upon the Subscriber making a revocation request or upon being notified by HKPost of its intention to suspend or 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 suspended or revoked (either by HKPost or at the Applicant's or 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.

k) Agreeing to forfeit the use of any private keys embedded on the Subscriber's HKID Card in case the Subscriber's HKID Card is lost, destroyed, defaced or damaged, or surrendered to or invalidated or seized by the Immigration Department or other law enforcement agencies under the laws of the Hong Kong SAR, and that HKPost and the Government of the Hong Kong SAR shall be under no liability to the Applicant or Subscriber in respect of any such events. The Applicant/Subscriber may request HKPost to revoke the e-Cert embedded on the HKID Card in accordance with the procedures stipulated in Section 4.4.2.

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 Agreement 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.

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, a Subscriber Agreement is not a contract for the supply of goods of any description or at all. Any and all certificates issued pursuant to it remain the property of and in the possession and control of HKPost and no right, title or interest in the certificates is transferred to the Subscriber, who merely has the right to 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. HKPost agrees to transfer, free of charge, those articles into possession of Applicants or Subscribers for the limited purposes set out in this CPS, nonetheless HKPost will exercise reasonable care to see that the same is fit for the purposes of completing and accepting a certificate as set out in this CPS, and if it is not, then HKPost's liability shall be as set out in sections 2.2.3- 2.2.4 below. In addition, the e-Cert Customer Kit 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 e-Cert Customer Kit.

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 Agreement or the issue by HKPost of certificates under the PKI. Accordingly, each Applicant, Subscriber and Relying Party must agree that it is

reasonable for HKPost to limit its liabilities as set out in the Subscriber Agreement and in this CPS.

2.2.3.2 Limitation on Types of Recoverable Loss

In the event of HKPost's breach of :-

a) the Subscriber Agreement; or
b) any duty of care; and in particular its duty under the Subscriber Agreement 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 :-**

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

2.2.3.3 HK$ 200,000 Limit for e-Cert (Personal) Certificates
Subject to the exceptions that appear below, in the event of HKPost's breach of :-

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

the liability of HKPost to any Subscriber and any Relying Party, whether as Subscriber or Relying Party as defined by the CPS or in any other capacity at all, is limited to, and shall not under any circumstances exceed, HK$200,000 in respect of one e-Cert (Personal) certificate, or HK$0 (zero) in respect of one e-Cert (Personal) certificate issued to a person under 18.

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 Agreement, 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 Certificate Notices, Limitations and Reliance Limit

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

> *"The Postmaster General acting by the officers of the Hong Kong Post Office has issued this certificate as a recognized CA under the Electronic Transactions Ordinance upon the terms and conditions set out in the Postmaster General's Certification Practice Statement (CPS) that applies to this certificate.*
>
> *Accordingly, any person, before relying upon this certificate should read the CPS 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; and

d) Performing all appropriate certificate path 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 $200,000 if this certificate is an e-Cert (Personal) certificate, or HK$0 if this certificate is an e-Cert (Personal) certificate issued to a person under 18, in respect of proved loss caused by reasonable reliance upon such inaccurate or misleading matters in this certificate where such losses are not and do not include (1) any direct or indirect loss of profits or revenue, loss or injury to reputation or goodwill, loss of any opportunity or chance, loss of projects, or the loss or loss of use of any data, equipment or software or (2) any indirect, consequential or incidental loss or damage even if, in respect of the latter, HKPost has been advised of the likelihood of such loss or damage in advance. The applicable Reliance Limit that applies to this certificate under the Ordinance in these circumstances is HK $200,000 if this certificate is an e-Cert (Personal) certificate, or HK$0 if this certificate is an e-Cert (Personal) certificate issued to a person under 18, 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.

<u>Time Limit For Making Claims</u>
Any Relying Party who wishes to make any legal claim upon the Postmaster General arising out of or in any way connected with the issuance, 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") provided to the Applicants or Subscribers under this CPS (as applicable) 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. For the avoidance of doubt, the Smart ID Card is issued by the Immigration Department and is NOT provided by HKPost under this CPS.

2.2.4.2 Notwithstanding the limitation of HKPost's liability set out above, if, after acceptance of the certificate, a Subscriber finds that, because of any error in the Private Key or Public Key of the certificate, no transactions contemplated by the PKI can be completed properly or at all, and that Subscriber notifies 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 paid. If the Subscriber waits longer than 3 months after acceptance before notifying HKPost of any such error, the fee paid will not be refunded as of right, but only at the discretion of HKPost.

2.2.5 Assignment by Subscriber

Subscribers shall not assign their rights under Subscriber Agreement or certificates. Any attempted assignment shall be void.

2.2.6 Authority to Make Representations

Except expressly authorized by HKPost, 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 Agreement 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, Relying Parties and HKPost 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 potential or actual liabilities and claims against Reliance Limit on the certificates.

2.3 Interpretation and Enforcement (Governing Law)

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

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

2.3.3 Dispute Resolution Procedures
The decisions of HKPost pertaining to matters within the scope of this CPS are final. Any claims should be submitted to HKPost at the following address:

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

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

2.4 Subscription Fees

e-Cert (Personal) certificates (for both new and renewal application) are available at the cost of HK$50 per certificate per year (Subscription Fee). Hongkong Post will waive the first year's costs of a certificate so that each of the Smart ID Card holders will be entitled to free use of the first certificate embedded on the Smart ID Card for the first year. The Subscription Fee shall be paid before the commencement of each subscription period unless waived (in respect of the first year) by HKPost. HKPost reserves its absolute right to review and determine the Subscription Fee from time to time and will notify the Subscribers and the public at the HKPost web Site http://www.hongkongpost.gov.hk.

2.5 Publication and Repository

HKPost maintains a Repository that contains a list of accepted certificates issued under this CPS, the current certificate revocation list, the HKPost Public Key, a copy of this CPS, and other Information related to 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 receipt of the Subscriber's confirmation of acceptance of the e-Cert. The HKPost Repository can be accessed at URLs as follows:-

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

2.5.1 Certificate Repository Controls

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

2.5.2 Certificate Repository Access Requirements

Only 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 acceptance of each certificate by the Subscriber and any other applicable events such as revocation of certificates or other CA disclosure records.

2.6 Compliance Assessment

Compliance assessments 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

HKPost will ensure that the restrictions in this subsection will be adhered to by itself 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 the release of compiled data which is not traceable to an individual Subscriber) unless required by a court-issued subpoena or order, or when otherwise required by the laws of Hong Kong SAR.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Application

Save in the case of Applicants who are holders of valid e-Cert (Personal) 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. In the case of Applicants who are holders of valid e-Cert (Personal) certificates, their attendance is not required, but their valid Digital Signatures supported by their e-Cert (Personal) certificates are required as proof of identity.

All Applicants for e-Certs shall submit a completed application form and Subscriber Agreement to HKPost. Following approval of the application, HKPost prepares an e-Cert and notifies the Applicant of how the certificate may be issued and accepted.

3.1.1 Types of Names

3.1.1.1 e-Cert (Personal) certificates

Subscribers for e-Cert (Personal) certificates are identified in a certificate with a Subject Name consisting of:

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

3.1.1.2 e-Cert (Personal) certificates issued to Subscribers who are under 18

Such Subscribers are identified in the certificate as above. The Subscriber who is under 18 at the time of submitting the e-Cert application forms are issued an e-Cert to be displayed as "e-Cert (Personal/Minor)" (see **Appendix B**) to indicate that the Subscriber is under 18 at the time of submitting the e-Cert application form.

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 Subject Name shall be unambiguous and unique to a Subscriber. However, this CPS does not require that a specific component or element of a name be unique or unambiguous by itself.

3.1.5 Name Claim Dispute Resolution Procedure

The decisions of HKPost in matters concerning name disputes are discretionary and final.

3.1.6 Infringement and Violation of Trademarks

Applicants and Subscribers warrant (promise) to HKPost and represent to 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

HKPost carry 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 are delivered to the Applicant in a secure manner stipulated in Section 4.1.2, 4.2.3 and 4.3.2 below.

3.1.8 Authentication of Individual Identity

Confirmation of the identity of each individual Applicant will be accomplished through one of the following processes:-

a) Each Applicant for a certificate shall 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 review and certify the application package, and forward the application to HKPost CA Centre for processing.
b) Each Applicant for a certificate shall present his valid Digital Signature supported by a valid e-Cert (Personal) certificate.

3.2 Subscription Renewal

3.2.1 HKPost will issue subscription renewal notice in the form of emails or letter mail to the Subscribers within one (1) month prior to the expiry of the subscription. The e-Certs issued on Smart ID Cards are physically valid for three years while the Smart ID Card holders are offered one-year free use. The subscription of e-Cert service can be renewed before expiry of the one-year free e-Cert service at the request of the Subscriber and the discretion of HKPost. HKPost will not perform renewal of subscription of expired, suspended or revoked certificates.

3.2.2 Subscribers do not need to visit HKPost service counters to upload another e-Cert onto their Smart ID Cards during the three-year validity period. If a Subscriber does not pay the subscription fee before the one-year free service expires, his e-Cert may be revoked upon expiry of subscription. He may leave the e-Cert on the Smart ID Card or go to one of the designated Post Offices to have his e-Cert removed from the Smart ID Card.

3.2.3 Subscription of an e-Cert (Personal) certificate may be renewed without going through the process of an authentication of the identity of the Subscriber which is required when a new certificate application is made. To apply for subscription renewal, the Subscriber may either submit the subscription renewal application through electronic means or submit a completed and signed subscription renewal application form to HKPost. Details of the subscription renewal application are available at both post offices and HKPost's web site at http://www.hongkongpost.gov.hk. Upon subscription renewal, the Subscriber's e-Cert and key pair will continue to be valid and generation of new key pair of the Subscriber will not be required. Upon subscription 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.

3.3 Certificate Renewal

3.3.1 HKPost will issue renewal notice in the form of emails or letter mail to the Subscribers within one (1) month prior to the expiry of the certificates. 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. At the discretion of HKPost, the new certificate to be issued to the Subscriber may be valid as from the date the certificate is generated and expired on the date that is three (3) years after the expiry date of the certificate being renewed. Accordingly, the new certificate may have a validity period of more than three years but no more than three years and one month.

3.3.2 An e-Cert (Personal) certificate may be renewed without going through the process of an 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 certificate renewal, a new key pair of the Subscriber will be generated through HKPost's central key generation service by HKPost's personnel. Upon certificate 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

4.1.1 Application Processing

4.1.1.1 Citizens who have not been issued the Smart ID Card may apply to embed an e-Cert on their Smart ID Card (see Section 4.2) by submitting application forms :-

a) in advance to HKPost in person at HKPost service counters, by post, by fax or through the Internet before visiting Immigration Department's ("ImmD") Smart ID Card Centres ("SIDCCs") for ID card replacement; or

b) at the HKPost service counters located at SIDCCs at the time when they replace their ID card.

4.1.1.2 Citizens who have been issued the Smart ID Card but have not applied for an e-Cert on the Smart ID Card may apply to embed an e-Cert on their Smart ID Card (see Section 4.3) by submitting application forms at designated HKPost service counters.

4.1.2 Back-up Copy of e-Cert and Private Key

4.1.2.1 The e-Cert and the Private Key embedded on the Smart ID Card shall not be recovered in case the card is lost or damaged. Accordingly, the Applicant is provided with an option to have a backup copy of his e-Cert and Private Key embedded on the Smart ID Card on a floppy disk or alternative storage medium at a charge specified on the application form. The Applicant may, at the time of submitting an application form, opt for a backup e-Cert and Private Key.

4.1.2.2 If the Applicant has opted for a back-up copy of e-Cert, the Private Key and e-Cert, which are protected by the Applicant's PIN, will then be stored on a floppy disk or alternative storage medium. 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 Applicant in a manner specified on the application form.

4.1.2.3 Applicants 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.

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

4.1.3 Identity Verification

4.1.3.1 The Applicant is required to present his HKID Card for identity verification conducted by HKPost staff at HKPost service counters. Upon satisfactory completion of the identity verification process, an e-Cert PIN envelope will be delivered to the Applicant.

4.1.3.2 Each of the e-Certs embedded onto the Smart ID Cards will be protected by individual PINs. The PINs will be distributed to the e-Cert Applicants separately in the form of sealed PIN envelopes. The e-Cert PIN will be required for any subsequent use of the e-Cert in order to prevent unauthorized access to the e-Cert.

4.1.4 HKPost will notify the Applicant of approval of an application by email or letter mail. 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 of rejection of his/her application.

4.2 Issuing and Embedding e-Cert on Smart ID Card through Immigration Department

4.2.1 For applications submitted at locations described in Section 4.1.1.1 above, HKPost will issue an embedded e-Cert onto the Applicant's Smart ID Card, through the process stipulated in this Section 4.2, so that the Applicants will be able to collect their Smart ID Card from the Immigration Department ("ImmD") with their e-Certs already embedded.

4.2.2 Validation Process

4.2.2.1 A data validation process will be carried out by the computer systems of ImmD and HKPost on a daily basis and as follows-

a) the data of citizens who have applied for the e-Cert (Applicants) will be kept securely in a database developed and managed by HKPost;

b) HKPost's system will be programmed to compile on a daily basis an "opt-in list" containing the ID number and English name of Applicants belonging to the group gazetted for card replacement at the time;

c) HKPost's system will send the opt-in list to ImmD's system for validation on a daily basis through a secure communication link with end-to-end encryption in place;

d) ImmD's system will, on the basis of the ID number of the e-Cert Applicants in the opt-in list, ascertain whether the e-Cert Applicants have registered for ID card replacement and then return to HKPost's system a Validation Result List containing the status of the Applicants ("validated" and "non-validated"). ImmD will not keep copies of the opt-in lists or the validation results;; and

e) The data transfer between ImmD's and HKPost's systems will be conducted through a secure communication link with end-to-end encryption in place.

4.2.2.2 The above validation process will not constitute a "matching procedure"[1] under the Personal Data (Privacy) Ordinance (PDPO), Cap. 486. The purpose of the validation process is to ensure that the e-Cert Applicant is the person who registers for ID card replacement so that HKPost can proceed to generate the e-Cert for the Applicant and send it to ImmD for embedding onto the corresponding Smart ID Cards. The process is not for, and will not serve, the purpose of enabling HKPost to take any "adverse action"[2] against the e-Cert Applicants (as data subjects). The validation process will not deprive citizens of the opportunity to enjoy one year's free use of e-Cert embedded on the Smart ID Card. HKPost will follow up on those non-validated cases so that eligible e-Cert Applicants will be able to have their e-Certs embedded onto their Smart ID Cards.

4.2.3 Generating and Embedding e-Cert on Smart ID Card

4.2.3.1 Following the validation process, HKPost will generate e-Certs (including the associated key pairs) for the validated cases and send the e-Certs to ImmD for embedding onto the Smart ID Cards of the respective Applicants. The key pair generation is performed by HKPost on behalf of the Applicant and certificate creation is performed by HKPost. This is done in a Trustworthy System and environment within HKPost's premises to ensure that the Private Key will not be tampered with.

4.2.3.2 The workflow for embedding e-Certs on Smart ID Cards is as follows -

a) HKPost will send to ImmD the e-Certs and Private Keys, which are protected by e-Cert PINs assigned to respective Applicants (see also Section 4.2.2.2) and in an encrypted form, through a secure channel with end-to-end encryption mechanism in place. The encrypted e-Certs and Private Keys will be kept in a secure system at ImmD for embedding onto the Smart ID Cards;

b) ImmD's system will embed individual encrypted e-Certs and Private Keys onto the corresponding Smart ID Cards; and

c) the encrypted e-Certs and Private Keys will be purged from ImmD's database;

4.2.4 Acceptance of e-Cert

4.2.4.1 HKPost will provide opportunities for the Applicants to confirm acceptance of their e-Certs upon collection of the new Smart ID Cards from ImmD. Applicants agree that they are fully accountable for the safe custody of the Private Key

[1] "Matching procedure", as defined under the PDPO, means any procedure whereby personal data collected for one or more purposes in respect of 10 or more data subjects are compared (except by manual means) with personal data collected for any other purpose in respect of those data subjects where the comparison-

(a) is (whether in whole or in part) for the purpose of producing or verifying data that; or
(b) produces or verifies data in respect of which it is reasonable to believe that it is practicable that the data,

may be used (whether immediately or at any subsequent time) for the purpose of taking adverse action against any of those data subjects.

[2] "Adverse action", in relation to an individual, as defined under the PDPO, means any action that may adversely affect the individual's rights, benefits, privileges, obligations or interests (including legitimate expectations).

embedded on the Smart ID Card upon receipt of the Smart ID Card and agree that they will be responsible for any consequences under any circumstances for the compromise of the Private Key. The e-Cert acceptance can be done at the HKPost web site through the steps mentioned in Section 4.2.4.2, or at the HKPost service counters through the steps mentioned in Section 4.2.4.3.

4.2.4.2 Applicants may perform e-Cert acceptance at the designated HKPost web page through the Internet as follows:-

a) the Applicant inputs his personal information at the web page;

b) if the data input by the Applicant match the Applicant's data kept by HKPost's system, content of the e-Cert issued to the Applicant will be displayed for the Applicant's verification;

c) the applicant may confirm acceptance of his e-Cert (see also Section 4.2.4.4); and

d) the data of the Applicant's acceptance of the e-Cert will be transferred back to the HKPost system.

4.2.4.3 The Applicants may perform e-Cert acceptance at the HKPost service counters as follows:-

a) insert the Smart ID Card into the smart card reader of the computer installed at the counter;

b) content of the e-Cert embedded on the Smart ID Card will be displayed for the Applicant's verification;

c) the Applicant may confirm acceptance of his e-Cert (see also Section 4.2.4.4); and

d) the data of the Applicant's acceptance of the e-Cert will be transferred back to the HKPost system.

4.2.4.4 In respect of the processes mentioned in 4.2.4.2(c) and 4.2.4.3(c) above, the Applicant may confirm **not** to accept the e-Cert and request revocation of the e-Cert. He may leave the un-accepted e-Cert on the Smart ID Card or go to one of the designated Post Offices to have it removed.

4.2.5 Publication of e-Cert

Upon receipt of the Subscriber's acceptance of his/her e-Cert, HKPost's system will publish, as stipulated under the Ordinance, the accepted e-Cert in a Repository, which is maintained by HKPost (see Section 2.5). Un-accepted e-Certs will not be posted to the Repository.

4.3 Embedding e-Cert onto Smart ID Cards at HKPost Service Counters

4.3.1 For citizens who decide to opt for the e-Cert after their Smart ID Cards are issued and those "non-validated" cases described in Section 4.2.2 above, they may complete the

application and embedding e-Cert onto the Smart ID Cards at designated HKPost service counters. The list of designated HKPost service counters is published at the HKPost web site at www.hongkongpost.gov.hk.

4.3.2 For citizens who decide to opt for the e-Cert after their Smart ID Cards are issued, they may complete their applications and embed their e-Certs on their Smart ID Cards over the designated HKPost service counters through the following steps:-

a) The Applicant submits the application, completes identity verification and collects the PIN envelope in accordance with the process described in Section 4.1.1.2, 4.1.2 and 4.1.3.

b) HKPost's staff will capture the Applicant's data provided on the application form at the terminal installed at the counter for the generation of the Applicant's e-Cert.

c) The content of the e-Cert generated will be displayed on the screen for the Applicant's verification.

d) The Applicant may confirm acceptance of his e-Cert (see also Section 4.2.4). The data of the Applicant's acceptance will be transferred back to the HKPost CA system.

e) If the Applicant accepts the e-Cert, the Applicant's Smart ID Card will be inserted into a card reader and the corresponding e-Cert and Private Key will be retrieved from the back-end secure system and then loaded onto the Smart ID Card through a secure mechanism. The e-Cert and Private key embedded on the Smart ID Card will be protected by the e-Cert PIN inside the sealed PIN envelope delivered to the Applicant. If the Applicant rejects the e-Cert, no e-Cert and Private Key will be loaded onto the Smart ID Card.

f) After completing the above process, the Smart ID Card will be returned to the Applicant immediately;

g) The accepted e-Cert will then be published in a Repository.

4.3.3 For those "non-validated" Applicants described in Section 4.2.2 above who have submitted an application, completed identity verification and collected a PIN envelope, they may have their e-Certs embedded onto their Smart ID Cards through the following steps:-

a) The Applicant presents his Smart ID Card for HKPost's staff to verify the Applicant's application status through the terminal installed at the counter.

b) If the Applicant, based on the Applicant's record in the HKPost system, is confirmed to have submitted an application, completed identity verification and collected a PIN envelope, HKPost's staff will arrange to generate the Applicant's e-Cert by the HKPost system through the terminal installed at the counter.

c) The content of the e-Cert generated will be displayed on the screen for the Applicant's verification.

d) The Applicant may confirm acceptance of his e-Cert (see also Section 4.2.4). The data of the Applicant's acceptance of the e-Cert will be transferred back to the HKPost CA system.

e) If the Applicant accepts the e-Cert, the Applicant's Smart ID Card will be inserted into a card reader and the corresponding e-Cert and Private Key will be retrieved from the back-end secure system and then loaded onto the Smart ID Card through a secure mechanism. The e-Cert and Private Key embedded on the Smart ID Card will be protected by the e-Cert PIN inside the sealed PIN envelope delivered to the Applicant. If the Applicant rejects the e-Cert, no e-Cert and Private key will be loaded onto the Smart ID Card.

f) After completing the above process, the Smart ID Card will be returned to the Applicant immediately;

g) The accepted e-Cert will then be published in a Repository.

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 certificates in the event of compromise of the HKPost Private Keys (see Section 4.8.2).

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

Each Subscriber MUST apply to 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(g)).

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 :
    (i) Is dead or has died;

(ii) Is or has become an undischarged bankrupt or has entered into a composition or scheme of arrangement or a voluntary arrangement within the meaning of the Bankruptcy Ordinance (Cap. 6) within 5 years preceding the date of revocation; or

(iii) Has been convicted in Hong Kong or elsewhere of an offence for which it was necessary to find that the person acted fraudulently, corruptly or dishonestly or committed an offence under the Electronic Transactions Ordinance; or

g) Determines that the Subscriber has failed to pay the subscription fee (see Section 3.2.2).

4.4.2 Revocation Request Procedure

A Subscriber may submit a certificate revocation request to HKPost through a designated web page on the HKPost web site at http://www.hongkongpost.gov.hk, by fax, letter mail, email or in-person. Based on the revocation request, HKPost will suspend the validity of the certificate. The certificate will be revoked, which terminates the validity of the certificate permanently, upon receipt of the final confirmation of revocation from the Subscriber. Such final confirmation of revocation can be an email digitally signed by the Subscriber's Private Key, an original letter signed by the Subscriber or a Request for Certificate Revocation Form signed by the Subscriber. If no final confirmation of revocation is received from the Subscriber, the validity of the certificate will remain suspended and will be included in the Certificate Revocation List (CRL) until the certificate expires. The Request for Certificate Revocation Form can be obtained from the web site at http://www.hongkongpost.gov.hk. HKPost may consider Subscriber's request for resuming the validity of certificates that are suspended. However, resuming the validity of a certificate that is suspended is only at the discretion of HKPost.

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

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 ensure 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 of this sub-section, 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 transactions in the period between HKPost's decision to suspend or revoke a certificate (either in response to a request or otherwise) and the appearance of the suspension or revocation status 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 and published in accordance with the schedule and format specified in **Appendix C**.

e) HKPost's policy concerning the situation where a relying party is temporarily unable to obtain Information on revoked certificate is stipulated in Section 2.1.3 (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 posts the suspension/revocation status to the Certificate Revocation List.

4.5 Computer Security Audit Procedures

4.5.1 Types of Events Recorded

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

- Suspicious network activity
- Repeated failed access attempts
- Events related to equipment and software installation, modification, and configuration of the CA operation
- Privileged accesses to all CA components
- Regular certificate management operations including:-
  - Certificate revocation and suspension requests
  - Actual issuance, revocation and suspension of certificates
  - Certificate renewals
  - Updates to repositories
  - CRL generation and posting
  - CA Key rollover
  - Backups
  - Emergency key recoveries

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

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

4.5.4 Protection of Audit Logs
HKPost 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 will be created and maintained when necessary

4.6.5 Timestamping

Archived Information is marked with the date at which the archive item was created. HKPost utilizes controls to prevent the unauthorized manipulation of the system clocks.

4.7 Key Changeover

The lifespan of the HKPost CA and e-Cert root keys and certificates created by HKPost for the purpose of certifying certificates issued under this CPS is no more than 20 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 assessment 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 Applicants/Subscribers are generated through a procedure such that the Private Key cannot be accessed by anyone other than the authorised user of the Private Key unless there is some compromise of the procedure by the authorised user. HKPost generates the root key pairs for issuing certificates that conform to this CPS. In case of central key generation by HKPost on behalf of the Applicants, the Applicants' Private Keys will be purged from the HKPost system upon completion of delivery of the e-Certs and Private Keys to the Applicants.

6.1.2 Subscriber Public Key Delivery

Key pairs will be generated under the central key generation by HKPost on behalf of the Applicant/Subscriber.

6.1.3 Public Key Delivery to Subscriber

The Public Key of each HKPost key pairs 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 may be used for Digital Signatures and conducting enciphered electronic communications. HKPost Root Key (the key used to create or issue certificates that conform to this CPS) is used only for signing (a) certificates and (b) Certificate Revocation Lists.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

HKPost Private Keys are created in a crypto module validated to al least FIPS 140-1 Level 3.

6.2.2 Private Key Multi-Person Control

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

6.2.3 Private Key Escrow

No over-all key escrow process is planned for HKPost Private Keys and Subscribers' Private Keys in the 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 devices 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 CA root keys will be used for no more than 20 years (see also Section 4.7). 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 2.

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 Subscribers 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 Applicants, Subscribers and Relying Parties on the HKPost CA web site at http://www.hongkongpost.gov.hk.

Appendix A - Glossary

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

"Applicant" means a natural or legal person who has applied 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" or **"CA"** means a person who issues a certificate to a person (who may be another Certification Authority).

"Certification Practice Statement" or **"CPS"** means a statement issued by a Certification Authority to specify the practices and standards that the Certification Authority employs in issuing certificates.

"Certificate Revocation List" or **"CRL""** means a data structure that enumerates public-key certificates (or other kinds of certificates) that have been invalidated by their issuer prior to the 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.

“HKID Card” means the Hong Kong Identity Card, including the Smart ID Card, issued by the Immigration Department of the Hong Kong Special Administrative Region under the Registration of Persons (Amendment) Ordinance.

"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.

"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.

"Smart ID Card" means the HKID Card onto which an e-Cert may be embedded.

"Subscriber" means a person who:-

(i) is named or identified in a certificate as the person to whom the certificate is issued;
(ii) has accepted that certificate; and
(iii) holds a Private Key which corresponds to a Public Key listed in that certificate.

"Trustworthy System" means computer hardware, software and procedures that-

(a) are reasonably secure from intrusion and misuse;
(b) are at a reasonable level in respect of availability, reliability and ensuring a correct mode of operations for a reasonable period of time;
(c) are reasonably suitable for performing their intended function; and
(d) adhere to generally accepted security principles.

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

Appendix B - Hongkong Post e-Cert Format

		Hongkong Post e-Cert (Personal) certificates	Hongkong Post e-Cert (Personal) certificates issued to persons under 18
Standard fields			
Version		X.509 v3	
Serial number		[Set by HKPost CA system]	
Signature algorithm ID		sha1RSA	
Issuer name		cn=Hongkong Post e-Cert CA 1, o=Hongkong Post, c=HK	
Validity period	**Not before**	[UTC time set by HKPost CA system]	
	Not after	[UTC time set by HKPost CA system]	
Subject name		cn=[HKID name] (Note 1) e=[email address] (Note 2) ou=[SRN] (Note 3) o=Hongkong Post e-Cert (Personal) c=HK	cn=[HKID name] (Note 1) e=[email address] (Note 2) ou=[SRN] (Note 3) o=Hongkong Post e-Cert (Personal/Minor) (Note 4) c=HK
Subject public key info		Algorithm ID: RSA Public Key: 1024-bit key size	
Issuer unique identifier		Not used	
Subject unique identifier		Not used	
Standard extension (Note 5)			
Authority key identifier	**Issuer**	cn=Hongkong Post Root CA 1, o=Hongkong Post, c=HK	
	Serial number	[Inherited from Issuer]	
Key usage		Non-repudiation, Digital Signature, Key Encipherment **This field will be set Critical.**	
Certificate policies		PolicyIdentifier = 1.3.6.1.4.1.16030.1.1.1 (Note 6) PolicyQualifierID = CPS Qualifier = www.hongkongpost.gov.hk	
Subject alternative name	**DNS**	encrypted(HKID) (Note 7)	
	rfc822	[Applicant's email address] (Note 2)	
Issuer alternate name		Not used	
Basic constraint	**Subject type**	End Entity	
	Path length constraint	None	
Extended key usage		Not used	
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 8)	
Netscape extension (Note 5)			
Netscape cert type		SSL Client, S/MIME	

		Hongkong Post e-Cert (Personal) certificates	Hongkong Post e-Cert (Personal) certificates issued to persons under 18
Netscape SSL server name		Not used	
Netscape comment		Not used	

Note

1. Applicant name format: Surname (in capital) + Given name (e.g. CHAN Tai Man David).
2. Applicant's email address (optional)
3. SRN: 10-digit Subscriber Reference Number
4. "e-Cert (Personal/Minor)" indicates that the Applicant is under 18 at the time of submitting the e-Cert application form (see section 3.1.1.2 of this CPS).
5. All standard extensions and Netscape extensions are set as "non-critical" unless otherwise specified.
6. The Internet Assigned Numbers Authority (IANA) has assigned the Private Enterprise Number 16030 to HKPost. For identification purpose, this CPS bears an Object Identifier (OID) "1.3.6.1.4.1.16030.1.1.1".
7. The Applicant's HKID number (**hkid_number** - including the check digit) will be stored in the certificate in the form of a hash value of the HKID number (**cert_hkid_hash**) which has been signed by the Private Key of the Applicant:-

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

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

   With Central Key Generation, hkid_number will be signed during the key generation process at HKPost premises and the CA system will create a hash of the signed HKID number - ***SHA-1*** **(** $RSA_{privatekey,\ sha\text{-}1}$ **(hkid_number))**. The hash value will then be put into the designated extension field of the certificate being generated.
8. URL of CRL Distribution Point is http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL1_<xxxxx>.crl, where <xxxxx> is a string of five alphanumeric characters generated by the CA system. HKPost CA publishes a number of partitioned CRLs. If a certificate is suspended or revoked, its information will be published in the partitioned CRL at the URL specified in this CRL Distribution Point field.

Appendix C - Hongkong Post e-Cert Certificate Revocation Lists (CRLs)

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

a) **Partitioned CRLs** that contain Information of suspended or revoked certificates in groups. Each of the partitioned CRLs is available for public access at a location (URL) specified in the "CRL Distribution Points" field of each certificate issued. The URL is in the form of http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL1_<xxxxx>.crl, where <xxxxx> is a string of five alphanumeric characters generated by the CA system.

b) **Full CRL** that contains Information of all suspended or revoked certificates. The Full CRL is available at :-

http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL1.crl; or
ldap://ldap1.hongkongpost.gov.hk (port 389, cn=Hongkong Post e-Cert CA 1 CRL1, o=Hongkong Post, c=HK);

Under normal circumstances, HKPost will publish the latest CRL as soon as possible after the update time. HKPost may need to change the above updating and publishing schedule of the e-Cert CRL without prior notice if such changes are considered to be necessary under unforeseeable circumstances.

Format of Partitioned and Full CRL :-

Standard Fields	Sub-fields	Field Contents of Partitioned CRL	Field Contents of Full CRL	Remarks
Version		v2		This field describes the version of encoded CRL as X.509 v2.
Signature algorithm ID		sha1RSA		This field contains the algorithm identifier for the algorithm used to sign the CRL.
Issuer name		cn=Hongkong Post e-Cert CA 1, o=Hongkong Post, c=HK		This field identifies the entity who has signed and issued the CRL.
This update		[UTC time]		"This Update" indicates the date the CRL was generated.
Next update		[UTC time]		"Next Update" contains the date by which the next CRL will be issued, but it will not be issued any later than the indicated date. Notwithstanding this, the CRL is updated and issued on a daily basis as stated in the CPS.
Revoked certificates	User certificate	[Certificate Serial Number]		Revoked certificates are listed by their serial numbers.
	Revocation date	[UTC time]		The date on which the revocation occurred is specified.
	CRL entry extensions			
	Reason code	[Revocation Reason Code]		(Note 1)
Standard extension	(Note 2)			

Standard Fields	Sub-fields	Field Contents of Partitioned CRL	Field Contents of Full CRL	Remarks
Authority key identifier	Issuer	cn=Hongkong Post Root CA 1 o=Hongkong Post c=HK		This field provides a means of identifying the public key corresponding to the private key used to sign a CRL.
	Serial number	[Inherited from Issuer]		This field indicates the serial number of the issuer certificate.
CRL number		[Generated by CA system – each partitioned CRL has its own sequence]		The CRL Number is generated in sequence for each CRL issued by a CA.
Issuer distribution point		[DER Encoded CRL Distribution Point] This field will be set Critical.	Not used	This filed is used for Partitioned CRLs only.

Note

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

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

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

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

Appendix D - Summary of Hongkong Post e-Cert Features

Features	***e-Cert (Personal) Certificates***	***e-Cert (Personal) Certificates issued to persons under 18***
Subscribers	Holders of valid HKID Card who are 18 or above at the time of submitting an application	Holders of valid HKID Card who are under 18 at the time of submitting an application
Reliance Limit	HK$200,000	HK$0
Recognized Certificate	Yes	
Key pair size	1024-bit RSA	
Key pair generation	By Hongkong Post on behalf of the Subscriber through the central key generation service.	
Identity verification	Face-to-face authentication of the Applicant's identity; or by Digital Signature of the Applicant's valid e-Cert (Personal).	
Usage of certificate	Digital Signature and Encryption	
Subscriber's information included in the certificate	▪ English name as appeared on the HKID Card; ▪ HKID number encrypted as a hash value; ▪ Email address; and ▪ Subscriber Reference Number (SRN) generated by the HKPost system	
Subscription Fees (see also Section 2.4 of this CPS)	$50 per certificate (both new and renewal application) per year	
Certificate Validity	Three Years (Note 1)	

Note

1. Certificates issued under the certificate renewal process may have a validity period of more than 3 years, but no more than 3 years and 1 month (see Sections 1.2.4 and 3.3 of this CPS).